

# **Annex 1.**



## **New gTLD Application Submitted to ICANN by: Vistaprint Limited**

**String: webs**

**Originally Posted: 13 June 2012**

**Application ID: 1-1033-22687**

### **Applicant Information**

#### **1. Full legal name**

Vistaprint Limited

#### **2. Address of the principal place of business**

Contact Information Redacted

#### **3. Phone number**

Contact Information Redacted

#### **4. Fax number**

Contact Information Redacted

## 5. If applicable, website or URL

<http://www.vistaprint.com>

## Primary Contact

### 6(a). Name

Mr. David Barron

### 6(b). Title

Vice President and Senior IP Counsel

### 6(c). Address

### 6(d). Phone Number

Contact Information Redacted

### 6(e). Fax Number

Contact Information Redacted

### 6(f). Email Address

Contact Information Redacted

## Secondary Contact

### 7(a). Name

Ms. Victoria Clifford

**7(b). Title**

Intellectual Property Paralegal

**7(c). Address****7(d). Phone Number**

Contact Information Redacted

**7(e). Fax Number**

Contact Information Redacted

**7(f). Email Address**

Contact Information Redacted

**Proof of Legal Establishment****8(a). Legal form of the Applicant**

Limited company (corporation)

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

Bermuda

The companies act 1981

Memorandum of association of company limited by shares (Section 7 (1) and (2) )

<http://www.bermulalaws.bm/Laws/Consolidated%20Laws/Companies%20Act%201981.pdf>

**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.**

Vistaprint N.V. (NASDAQ:VPRT)

**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**

Ernst Jan Teunissen	Director
Lawrence Adam Gold	Director

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

Ernst Jan Teunissen	President
Lawrence Adam Gold	Senior Vice President

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

Vistaprint N.V.	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.**

webs

**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.**

A number of operational and rendering issues may arise with the delegation, and subsequent operation and use of a new TLD. Some of these issues may be experienced just by the users of one or two particular TLDs, due to the nature or composition of the string itself; whereas other issues (such as software support) may be experienced across all new TLDs.

Evaluation of the potential operational and rendering issues for the .WEBS TLD was delegated to ARI. ARI is experienced with:

- The operational issues of operating TLDs
- TLDs that offer registrations at the third level (eg .com.au, .net.au) and below
- The rendering and operational issues surrounding the introduction of IDNs

ARI has executed a suite of tests to evaluate any issues arising from the use of the TLD string. ARI configured a test environment that consisted of DNS software, web server software, and an email server configured for sample domains in the .WEBS TLD. Where possible, ARI attempted to test many equivalent applications, however the number of and different versions of applications means that testing was limited to the most common environments.

The tests executed by ARI indicate that the .WEBS TLD is subject to the same issues already experienced by TLDs in the root, which are neither new nor unique. A summary of these common issues is provided below.

- Some applications make assumptions about known valid TLDs and fail to recognize new TLDs
- Some Non-IDN aware applications require the user to provide input in A-labels
- Some IDN aware applications present the user with the domain name using A-labels instead of U-labels
- Some IDN aware applications fail to render IRIs in a manner consistent with user expectations.

To mitigate these issues, ARI will work with the Applicant to ensure that maintainers of applications are made aware of the delegation and operation of the .WEBS TLD. When relevant, the Applicant and ARI will refer the maintainers to the verification code produced by ICANN in the area for Universal Acceptance of All Top Level Domains such that operational issues can be mitigated for other TLDs.

The Applicant and ARI will work with maintainers of applications to provide subject matter knowledge where required, and provide directions to the tools provided by third parties such as the International Components for Unicode project and other groups, that can assist the application maintainer in adding the required support. User education may be required enabling users to configure their applications for correct functioning of this TLD. An informational section on the TLD website will be considered to address questions raised by the Internet community.

The steps ARI will take to mitigate these issues are more than adequate. Thus, we do not believe the .WEBS TLD raises stability concerns and there is no reason that it should be denied on an operational and rendering issues bases.

## 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.

The Applicant, Vistaprint Limited, is the Intellectual Property holding company of the publicly traded company, Vistaprint NV, a large online supplier of printed and promotional material as well as marketing services to micro businesses and consumers. It offers business and consumer marketing and identity products and services worldwide. Vistaprint Limited and its subsidiaries also operate the WEBS and VISTAPRINT websites (webs.com, vistaprint.com and others) and benefits from online transactions with customers. Through its subsidiaries, the Applicant also provides hosting and other Internet related services. This is done in particular through the WEBS website, accessible through webs.com

According to the Applicant, the purpose of the TLD is manifold, as will be further explained below:

- i. Securing, protecting and operating one of the Applicant's business lines ("WEBS") to the benefit of its stakeholders, referred to below and in particular, members of the WEBS community;
- ii. Reflect and operate Applicant's "WEBS" business at the top level of the DNS' hierarchy;
- iii. Provide stakeholders of the Applicant, including subsidiaries, and their respective suppliers, customers, sponsorships, and their respective directors, officers, employees, with a recognizable and trusted location on the Internet;
- iv. Provide such stakeholders with a secure and safe Internet environment that is mainly or even fully under the control of the Applicant and its stakeholders.

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

- i. WEBS is displayed by Applicant on its web site, webs.com. Through the WEBS community, Applicant has gained international exposure in hosting services and website related services. The proposed gTLD aims at consolidating the reputation of Applicant's WEBS services and the community it represents;
- ii. From the Applicant's perspective, .WEBS will 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 .WEBS top-level domain will be unambiguous as regards the identity of the Registry Operator. Furthermore, it will be clear that the services offered under the .WEBS space were made possible thanks to the products and services offered by and for the Webs community;
- iii. As mentioned in the vision / mission statement before, some of the key reasons why Applicant is applying for .WEBS are:
  1. Marketing and branding: reflect the Applicant's WEBS business at the



top-level of the DNS' hierarchy,

2. Safety and security, given the fact that the TLD and most if not all of the domain names registered therein will be completely or at least partially under the control of the Registry Operator;

3. Affiliation between WEBS and the various product brands registered and/or used by the Applicant and/or its subsidiaries in their day-to-day business;

iv. The Applicant intends to implement the following policies and procedures with respect to the registration of domain names in the .WEBS top-level domain include but are not limited to:

1. Reservation of domain names in the name of the Applicant. These names include:

a) descriptive names, referring to the actual day-to-day business activities of the Applicant and/or its subsidiaries;

b) descriptive names, referring to the internal departments of the Applicant;

c) descriptive names, referring to the subsidiaries of the Applicant;

d) product and service brands promoted by the Applicant and/or its subsidiaries now and in the future;

e) etc.

2. Launch of the TLD:

a) Sunrise: allow physical persons, organizations and entities that meet the eligibility requirements in force at that point in time to choose the domain names that are identical to their trademarks;

b) 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.

c) 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 Applicant for the TLD (Vistaprint Limited). In any case, the Applicant reserves the right to impose additional and other restrictions from time to time at its sole discretion;

v. The Applicant currently has privacy and data protection policies in place in relation to the services it offers. The Applicant is committed to implement similar privacy policies in relation to the use of the TLD. The privacy policy that is currently in place in relation to services offered in connection with WEBS is accessible on <http://www.webs.com/privacy.htm>. At the time of submitting this application, this privacy policy is as follows:

"Webs is a website building and hosting service provided at <http://www.webs.com> and <http://www.freewebs.com> and its directly associated domains, widgets, tools, services and applications that are operated by Webs, Inc. (collectively, "Webs" or "Services"). Your privacy on the Internet is very important to us. We strive to make your online experience satisfying and safe.

This "Privacy Policy" explains what information we gather from our users and how we use it. By using or accessing our Services, you are accepting the practices described in this Privacy Policy. (Capitalized terms not defined herein have the meaning set forth in our Terms of Service).

Webs is not intended for children under 13 years of age. Consistent with the Federal Children's Online Privacy Protection Act of 1998 ("COPPA"), we will never knowingly gather or use personally identifiable information from anyone under the age of 13, and we do not allow anyone under the age of 13 to register on Webs.

What information does Webs gather?

Webs gathers and stores three types of information about users that are subject to our Privacy Policy:

Information users provide to us:

These are voluntary submissions made when creating an account on Webs or through your use of the Services, such as your name, date of birth, location and email address provided during registration, Content posted, or payment information provided during purchases. Please understand that when you sign into Webs or post Content, your information is not anonymous to us.

Information we collect when you interact with Webs:

We keep track of the actions you take on Webs, such as adding a friend, adding an application, or posting Content. Also, when you access our Services, we may collect information about your access method (such as hardware and software attributes), location, IP address, and pages you visit. In addition, we store certain information from your browser using "cookies". (For more on cookies, please see the section "What are cookies?")

Information we receive from third parties:

We do not own or operate the third-party applications, user websites and other services offered that you may use or interact with through Webs (collectively, "Webs-enhanced" applications, websites and services). Whenever you visit, use or interact with a Webs-enhanced application, website or service, we will receive information from them, including information about actions you take and Content you post on that application, website or service.

Why does Webs gather information about me?

Webs collects information in order to provide a safe, efficient and customized experience. This information allows us to better tailor our content to users' needs and to help us better understand the demographics of our audience. Webs may use some of this information for contacting you, customizing the content and advertising you view, improving our services, conducting research, and providing anonymous reporting for clients. We only collect personally identifiable information from you because you are voluntarily submitting the information to us in order to enjoy certain Services.

How will Websites and Applications on Webs treat my information?

As mentioned above, we do not own or operate Webs-enhanced applications, websites and services. We take steps to ensure that providers of Webs-enhanced applications, websites and services use information that you share on Webs in a manner consistent with your privacy settings and the terms of this Privacy Policy, but we cannot guarantee that they will follow our rules. Please take the time to familiarize yourself with the privacy settings of your account, as well as the settings and policies of the applications, websites and services that you visit, add or use on Webs. Here are some specific things to remember:

By visiting or becoming a Member of a Website on Webs, the Content and information you provide during the registration process (including your email address) and other interactions with the Website may be accessed by the Website Creator and their authorized representatives and administrators, as well as any Application Developer whose Applications run on that Website.

By adding or using an Application or a service provided by one of our affiliates or business partners, the information you provide in the interactions with that Application or service may be accessed by the respective Application Developer, affiliate or business partner and their authorized representatives.

Although certain categories of profile information (such as your birthday) have privacy settings, others (such as your name, gender, profile photo, geographic region, list of friends, list of websites you have joined) are considered publicly available and have no privacy settings associated with them.

Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere to the extent it has been shared with others, it was otherwise distributed pursuant to your privacy settings or privacy settings of the Website(s) or Application(s) you used, or it was copied or stored by other users.

Certain types of communications you send to other users cannot be removed, such as messages.

When you post information on a Website, that information is subject to that Website's privacy settings and privacy policy, which may change from time to time.

Publicly available information may be accessed by everyone on the Internet, including third-party search engines that may index, cache and store that information.

You should always review the policies of third party websites, applications and services to make sure you are comfortable with the ways in which they use information you share with them. Any information you share with them is at your own risk. If you find an application, website or service that violates our rules, you should report the violation to us using this automated form, and we reserve the right to take action as we deem appropriate without assuming any obligation or liability to do so.

What are cookies?

Webs may place a text file called a "cookie" in the browser files of your computer. These cookies help us make Webs easier to use, to make our advertising better, and to protect both you and Webs. For example, a cookie may be used to store or "remember" your Member login information (but not your password) so that you are not required to manually log into the site at every visit. You can remove or block cookies using the settings in your browser, but in some cases that may impact your ability to use some of our Services.

Our advertisers and partners may also set cookies through our Services. For more information, please see the section "What about third party advertisers and links?"

What about third party advertisers and links?

In the course of serving advertisements on Webs, a third-party advertiser may place or recognize a unique cookie on your browser. Additionally, some links from Webs may lead to websites operated by other companies. While these websites and advertisements may be co-branded with our name or logo, they are not operated or maintained by us. We do not control these cookies and users of Webs Services should check the privacy policy of the relevant advertiser to understand whether and how it uses cookies. Webs is not responsible for websites operated by third parties that are linked to by any of our sites.

Ads appearing on this website, Webs, and sites hosted by Webs may be delivered to you by Google Ad Manager, DoubleClick, or other advertising partners. Information about your visits to this site, such as the number of times you have viewed an ad (but not your name, address or other personal information), is used to serve ads to you. For more information about these partners, their cookies, and how to "opt-out," please follow the links below.

Network Advertising Initiative (NAI)

Google Ad Manager

DoubleClick

How secure is my information?

Webs uses commercially reasonable physical, electronic, and procedural measures to safeguard personally identifiable information in our possession against loss, theft and unauthorized use, disclosure or modification. We limit access to personal information about you to employees whom we believe reasonably need that information to provide support, products, or services to you or to fulfill their roles within our organization.

Although we have established and maintain security procedures to protect your personally identifiable information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information. We cannot guarantee that only authorized

persons will view your information. We cannot ensure that information you share on Webs will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Webs. You can reduce these risks by using common sense security practices such as choosing a strong password, using different passwords for different services, and using up-to-date antivirus software.

Please report any security violations to us on this automated form.

How private is the Content I upload?

Any Content uploaded or created using our Services and posted on a Website are by default hosted for the public and are thus publicly accessible unless explicitly protected by the Website Creator's optional password protection setting.

Please note that even if you do not publish links to Content or submit links to a search engine, individuals or search engines may discover and link to your Content by data-mining, guessing the address, spidering sites, or other methods. If you are concerned about the privacy or confidentiality of Content that you produce, please take all appropriate steps to ensure that sensitive materials are password-protected. Webs makes no guarantee as to the reliability or security of the password protection feature.

What control do I have over my information?

As a registered member, you may modify or update your personal account information at any time by logging into your account and (a) accessing the Settings area for each Website you have created, and (b) accessing the Manage Profile area for each Website you have joined by clicking on the corresponding Edit Profile link on your Dashboard page. You may also remove the Website(s) you may have created on Webs at any time by logging into your account and clicking on the corresponding "Delete Site" link on your Dashboard page. Should you desire to do so, you may also delete and close your Webs account at any time by contacting our support team. Note that removed or deleted information may persist in backup copies for a reasonable period of time.

How is information shared?

Webs will not share your personally identifiable information with others except as described herein with regards to sharing with Webs-enhanced applications, websites and services and in limited circumstances where we believe such sharing is reasonably necessary to offer the Services, legally required, or permitted by you. For example, we may provide information to service providers to help us bring you the services we offer. Specifically, we may use third parties to facilitate our business, such as to host the Services at a co-location facility for servers, to register your domain name, to send out email updates about Webs, to provide you with email functionality for your domain, to remove repetitive information from our user lists, to process payments for products or services, or to provide search results or links (including sponsored links). In connection with these offerings and business operations, our service providers may have access to your personal information for use for a limited time.

Where we utilize third parties for the processing of any personal information, we implement reasonable contractual and technical protections limiting the use of that information to the Webs-specified purposes. We may store personal information in locations outside the direct control of Webs (for instance, on servers or databases co-located with hosting providers).

Except as otherwise described in this Privacy Policy, we will not disclose personal information to any third party unless we believe that disclosure is necessary: (1) to conform to legal requirements or to respond to a subpoena, search warrant or other legal process received by Webs, whether or not a response is required by applicable law; (2) to enforce the Webs Terms of Service or to protect our rights; or (3) to protect the safety or rights of members of the public or users of the Services. Webs reserves the right to

transfer personal information to a successor in interest that acquires rights to that information as a result of the sale of Webs or substantially all of its assets to that successor in interest. We may also transfer such information in the course of corporate divestitures, mergers, or dissolution.

How am I notified of changes to this Privacy Policy

We may change this Privacy Policy pursuant to the procedures outlined in our Terms of Service. Unless stated otherwise, our current Privacy Policy applies to all information we have about you and your account. If we make changes to this Privacy Policy we will notify you by publication here.

Who can I contact about this Privacy Policy?

To submit an inquiry about our Privacy Policy, please contact our support department.

[Last updated: February 19, 2010]"

vi. The Applicant is part of a multinational organization that has been established in 1995. In December 2011, the Applicant acquired Webs, Inc., which has continuously been trading as WEBS since 2005 and under the webs.com domain name since 2005. Since its establishment, it has developed an important reputation in printing and Internet services. Therefore, the Applicant has different ways in order to make existing and future clients, visitors and stakeholders aware of the use and possibly the (gradual) move from the group's webs.com domain name to the .WEBS TLD, including but not limited to:

1. Internet advertising campaigns;
2. having Internet traffic to its key domain names resolving into domain names registered in the .WEBS TLD;
3. email marketing campaigns; etc.

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

i. The Applicant will organize the registry operation for the .WEBS TLD in such a manner that it will minimize the likelihood of having multiple applications for a particular domain name. This can be achieved in one of the following ways:

1. Given the fact that, at least prior to the launch of the .WEBS top-level domain, the Applicant / Registry Operator will reserve, delegate and use a large number of domain names that are directly or indirectly relevant to Applicant's business in its own name. Since quite a number of these domain names will 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 will 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 .WEBS top-level domain;

3. The Registry Operator may give existing (paying) customers a right of first offer or first refusal for the registration of certain types of domain names and/or during one or more specific launch phases. The duration and/or nature of the customer relationship may be used as a criteria to solve contention when multiple applications for a particular domain name occur;

4. 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.

ii. Given the Applicant's activity as an innovative web hosting provider at a limited cost, the Applicant intends to make the .WEBS top-level domain

available to qualifying domain name registrants at a limited cost or at no cost as part of a web hosting or other service package. As the Applicant will be less dependent on the service offerings of existing registries, the pricing of the Applicant's services will depend less on the pricing of the service offerings from those registries. The per domain name price to be paid by the Applicant for a web hosting service, inclusive of a domain name, is likely to be lower. This may result in a better price offering to Internet users for the Applicant's value added services. The Internet user and the Internet community would benefit from the Applicant being able to reduce costs, as this may result in better pricing and/or more room for investing in customer service, in innovative Internet solutions, etc. It must be noted that this does not preclude the Applicant / Registry Operator to charge higher fees for the registration of domain names under the .WEBS TLD at its discretion, e.g., as part of premium packages or for certain categories of clients and customers. The fact that some may be willing to pay more for the registration of particular domain names would again be beneficial for other potential domain name registrants in the .WEBS TLD.

iii. The Applicant / Registry Operator may at its discretion make contractual commitments to increase or decrease the fees for the registration of domain names under the .WEBS TLD.

## Community-based Designation

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

Yes

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

The Applicant is committing to serve the 'WEBS' community. The 'WEBS' community was created in late 2005 by Freewebs, now called Webs, Inc. Webs, Inc. presently is a subsidiary of the Applicant.

In August 2006, Business Wire reported on this stating that "new Freewebs tools and features put the 'We' in Web for world's largest Web Publisher; import tools, profile pages and ratings & comments help enhance online experience, engage website fvisitors and create a single web presence for millions of users" (Document 20.a.1). Since 2006, the Applicant started by giving its users the option to publish their myWebs profile as a page on their website, making it accessible and searchable to all Freewebs - and later on Webs - visitors. The Applicant invested in creating the tools necessary for its members to simply create their Web presence and share their passions with the world.

Since its inception, the name of the community was 'WEBS'. This is shown by the mention of 'myWebs' and the mention of the name 'Webs' as such to refer to the blog that was used by the community to communicate with each other to share Webs experiences (see Document 20.a.2 - additional examples of community-engaging entries are available upon request). In 2008 this resulted in the rebranding of the company name from Freewebs into Webs. The community only became stronger and the aim was to have visitors to become active participants. The Applicant, through the Webs platform lets site owners create community-driven sites that visitors can join as members. By giving site members the ability to comment on photos, post to a blog, add to a site calendar, and more, a site becomes more of a living, breathing entity and a reflection of the Webs

community.

The myWebs service had 223,039 different members with 488,064 memberships to 84,226 groups. Every month more than 3.9 million of websites from the Webs community are visited by over 25 million unique visitors. Between late 2005 and early 2010, the Webs blog was branched between a blog for free users and a blog for paid users. Both blogs were actively used. Today Webs, Inc. provides community-powered support for Webs through <http://support.webs.com/webs>. Members of the Webs community support each other and share experiences through this portal. Furthermore, the Webs community members also communicate with each other on Twitter and Facebook. Webs on Facebook has 85,990 people expressing that they like Webs (see Document 20.a.3).

The Webs community has members worldwide, with active websites in North America, Europe, Asia-Pacific and other parts of the world. More information about the geographic diversity of the Webs Community is provided in Document 20.a.4. The Applicant is prepared to provide more information on the size and geographic extent of the community in the event of a community priority evaluation, insofar this information is kept confidential.

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

The Applicant is directly related to the WEBS Community since December 2011, when it acquired Webs, Inc. as a subsidiary.

Webs, Inc. (called Freewebs at the time) started the Community initiative by investing in online tools through which Webs members could share their experiences and comment. Through its subsidiary, Webs, Inc. the Applicant provides community members with useful information on improving their Webs experiences, through blogs, services, example sites, providing platforms on which the community can interact, etc.

Through its subsidiaries Vistaprint Netherlands B.V. and Webs, Inc. (to which the former is affiliated), the Applicant provides community members also with policies and terms of use of the different products and services, laying down rules and terms of conduct to be accepted by members of the WEBS community. These policies and terms of use also explain the contractual relationship and the way in which the Applicant's subsidiaries are accountable to the community.

As shown by Document 20.f, the application for the .WEBS community is endorsed by the co-founders of the Webs community themselves. The co-founders of the Webs Community are still active in Webs.com and driving the Webs Community. The co-founders are prepared to provide additional information, should this be required.

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

According to the Applicant the community-based purpose of the applied-for gTLD is to provide members of the Webs community with a clear identifier for their community. This will bring a high degree of recognition and specialization to the currently existing name space, as it will be clear that the services offered under the .WEBS space were made possible thanks to the products and services offered by and for the Webs community.

The registration of domain names is likely to be reserved to the Applicant and/or its subsidiaries in the first place. This should allow the Applicant to

build awareness amongst the members of the Webs community and the Internet community at large that the .WEBS gTLD exists, that the domain names registered under .WEBS and the content provided on the websites to which those domain names point are managed by the Applicant and/or its subsidiaries. Afterwards, registration may be granted to other members of the Webs community.

Such members of the Webs community can be identified as users of services offered by Vistaprint Netherlands B.V. Webs, Inc. such as websites, toolbars, widgets, or other distribution channels and any other features, content, services or applications offered by Webs, Inc. or by third party paid service providers, and that register or have registered on one of the websites on which such services are offered by Vistaprint Netherlands B.V. and/or Webs, Inc.

Together with the Applicant and/or its subsidiaries, these members of the Webs community will be the intended end-users of the .WEBS TLD, as it is intended that these community members will be using and building the services offered under the .WEBS TLD.

The Applicant intends to use the TLD for the following activities it has already carried out:

- provision of website building tools
- development of website building tools in cooperation with the Webs community
- provision of professional templates and business applications
- provision of hosting services
- interaction with the Webs community
- etc.

The Applicant intends to continue carrying out these activities in service of the community-based purpose of the .WEBS TLD.

The fact that the Applicant, through its subsidiaries, has continuously provided hosting services and innovative website building tools with growing success and growing interest of the Webs community shows the lasting nature of the Applicant's community-based purpose of the applied-for TLD. Furthermore, the fact that this initiative is sponsored by the Applicant at the highest level of the organization shows the Applicant's commitment to make this initiative long-lasting.

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

There is a clear relationship between the applied-for .WEBS gTLD string and the community identified in the answer to question 20(a) above.

The .WEBS gTLD is identical to the established name of the community. Hence there is a clear relationship to the established name of the community.

The .WEBS gTLD will also allow members of the Webs community to show their relationship to the community more clearly. Whereas community members previously made profiles under the myWebs identifier to show their relationship to the community, it will become possible for Webs community members to also show their relationship to the community through the use of the .WEBS gTLD.

"WEBS," in the context of Applicant's and the Community's usage, is not a dictionary word. Therefore, Applicant is of the opinion that "WEBS," as Applicant uses it, has no relevant connotations beyond the community, as opposed to the generic term "WEB," which refers to the World Wide Web. In the context of the Internet, people refer to "the Web," but not to the plural term "Webs."



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

The Applicant intends to use a coherent set of registration policies in support of the community-based purpose of the .WEBS gTLD.

The Applicant plans to limit the eligibility to register second-level names in the gTLD to members of the WEBS community, impose restrictions on the second-level names that may be registered in the .WEBS gTLD as well as on the content and use. Finally, the Applicant intends to implement enforcement measures (with appeal mechanisms) to ensure the compliance with the rules and restrictions.

### Eligibility

At least during the initial months or even years following the delegation of the .WEBS gTLD to the Applicant, 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."

This should allow the Applicant to build awareness amongst the members of the Webs community and the Internet community at large that the .WEBS gTLD exists, that the domain names registered under .WEBS and the content provided on the websites to which those domain names point are managed by the Applicant and/or its subsidiaries. Also this would not limit the Applicant from allowing other members of the Webs community to use domain names managed by the Applicant and/or its subsidiaries.

At a later stage, in addition to the Applicant and/or its subsidiaries, members of the Webs community will possibly be entitled to register domain names in .WEBS. That is to say, one of the main eligibility criteria will be that the interested party wishing to register a domain name in the .WEBS TLD is either a member of the Applicant or has a sufficiently close link to the Webs community.

In any event, the Applicant reserves the right to change or restrict any policies, procedures and practices at any point in time if it is of the opinion that there would be a risk that the reputation of the Applicant's WEBS business would be damaged.

The eligibility to register domain names would in any event be limited to the Applicant, its members and subsidiaries and other members of the Webs community.

Such members of the Webs community can be identified as users of services offered by Vistaprint Netherlands B.V. Webs, Inc. such as websites, toolbars, widgets, or other distribution channels and any other features, content, services or applications offered by Webs, Inc. or by third party paid service providers, and that register or have registered on one of the websites on which such services are offered by Vistaprint Netherlands B.V. and/or Webs, Inc. Registration of domain names in the .WEBS TLD would be reserved to members of the Webs community who represent that they are fully able and competent to enter into the terms, conditions, obligations and warranties set forth in the policies, procedures and practices applicable in that point in time.

Members of the Webs community will need to make representations and warranties

similar to the following: that (a) all registration information they submit is truthful and accurate; (b) they will maintain the accuracy of such information; (c) they are 13 years of age and older; and (d) their use of the services offered by the Registry Operator or its affiliates does not violate any applicable law or regulation.

#### Name selection

The registration of domain names that could directly or indirectly damage, impair or disrupt the reputation and/or activities of the Applicant, the integrity of any of the brands and/or any of the trademarks from the Applicant and/or its subsidiaries will not be allowed. Registrants will also need to represent and warrant that the registration of domain names complies with all applicable laws and does not infringe upon or otherwise violates the rights of any third party.

Moreover, the Applicant will possibly draw up a list of reserved names which will not be available for registration and also put possibly special provisions in place for geographic names (see the Applicant's answer to Question 22 below), The Applicant will however reserve the right to allocate to and register a domain name mentioned on the list of reserved names in the name of a party indicated by the Applicant.

#### Content and use restrictions

The Applicant will in any case require that all content and use offered under the .WEBS TLD complies with all applicable laws, including, but not limited to, trademark laws, criminal laws, data protection laws etc. To that end, the Applicant will likely require applicants for a second-level domain name registration to warrant that:

- to their knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party;
- the applicant is not submitting the domain name registration request and, upon registration, will not use the domain name for an unlawful purpose, contrary to public policy or morality, for offensive purposes, to mislead the public and/or contrary to good and fair business practices; and
- it will not knowingly use the domain name in violation of any applicable laws or regulations, including third party interests; and
- it will keep the WHOIS information related to the domain name accurate and up-to-date at all times, both with its accredited registrar and the Applicant and/or its affiliates.

Furthermore, the Applicant will likely require applicants for a second-level domain name to choose carefully the content they post on any website and that they provide to other users: Community members shall not be allowed to use the services provided through the .WEBS TLD to post, disseminate or communicate any obscene, lewd, excessively violent, harassing, sexually explicit or otherwise objectionable subject matter.

The Applicant reserves the right to change or restrict any policies, procedures and practices at any point in time if it is of the opinion that there would be a risk that the reputation of the WEBS business would be damaged by the content or use made by a registrant of a second-level domain name in the .WEBS TLD.

#### Enforcement

Community members that become aware of any third party violation of the terms and conditions applicable at that time will likely be invited and may be obliged to report this to the Applicant or its designee, who may, at its sole discretion delete any content and revoke, temporarily or permanently suspend, delete or cancel at any time the registration of domain names in the .WEBS TLD. The Applicant also reserves the right to revoke, temporarily or permanently suspend, delete or cancel at any time the registration of domain names in the .WEBS TLD, when the registration or use of the domain name is in violation

of the terms and conditions applicable at the time. This will possibly include the right to revoke, temporarily or permanently suspend, delete or cancel the registration of a domain name, if it is suspected that the domain name is registered or used by persons under 13 years of age.

The Applicant may also implement technical and operational measures to monitor the compliance with the applicable registration policies.

The Applicant will make sure that there are alternative dispute procedures in place to ensure that complaints in relation to the registration and use of a domain name are in place. This shall include procedures to challenge decisions from the Applicant or its designee to revoke, temporarily or permanently suspend, delete or cancel the registration of a domain name.

## **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 multinational organization which holds interests in printing and other services worldwide, it has a vested interest in giving its visitors, clients and business partners a clear and predictable naming scheme in the .WEBS TLD. Since visitors and clients may mainly be looking for offers and activities organized by local branches and subsidiaries 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 or its Affiliates, 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 activities in printing, business and consumer marketing and identity products and services, and possibly other markets; and
- in order to directly and indirectly promote local commercial activity 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.

As mentioned in response to Question 18 (b) above, the Applicant is a large online supplier of printed and promotional material as well as marketing services to micro businesses and consumers. In connection to its business, the Applicant has a substantial experience and expertise in managing complex information technology infrastructures, hereby relying on in-house and external resources.

However, the Applicant has no in-depth experience in managing a domain name registry system and it would require too many efforts for the Applicant to develop a system itself that complies with the specific technical requirements imposed upon new gTLD registries. Therefore, the Applicant has decided to rely on ARI Registry Services ("ARI" - see [www.ariservices.com](http://www.ariservices.com)) and NetNames to provide a full suite of services in relation to the deployment and operation of its applied-for .WEBS TLD. It has been agreed between the Applicant and ARI that ARI will perform the back-end registry services for the .WEBS registry.

The response to this question describes the registry services for the .WEBS TLD as will be provided by ARI, in the name and on behalf of the Applicant. These registry services are referred to as ARI's Managed TLD Registry Service. When, throughout the responses to questions #23 to #44, it is stated that ARI will perform certain services or comply with certain standards or processes, ARI will do this in the name and on behalf of the Applicant, who itself is committed to comply with these standards or processes towards ICANN. Where use is made of the first person plural, reference is made to ARI, as the answer to this question is provided directly by ARI, the back-end provider of registry services for the applied-for .WEBS TLD (also referred to as 'this TLD').

It goes without saying that each and every service offered under the .WEBS gTLD will be provided under the authority and responsibility of the Applicant.

#### 1 INTRODUCTION

ARI's Managed TLD Registry Service is a complete offering, providing all of the required registry services. What follows is a description of each of those services.

#### 2 REGISTRY SERVICES

The following sections describe the registry services provided. Each of these services has, where required, been designed to take into account the requirements of consensus policies as documented here:

[<http://www.icann.org/en/resources/Registrars/consensus-policies>]

At the time of delegation into the root this TLD will not be offering any unique Registry services.

## 2.1 Receipt of Data from Registrars

The day-to-day functions of the registry, as perceived by Internet users, involves the receipt of data from Registrars and making the necessary changes to the SRS database. Functionality such as the creation, renewal and deletion of domains by Registrars, on behalf of registrants, is provided by two separate systems:

- An open protocol-based provisioning system commonly used by Registrars with automated domain management functionality within their own systems.
- A dedicated website providing the same functionality for user interaction. Registrants (or prospective registrants) who wish to manage their existing domains or credentials, register new domains or delete their domains will have their requests carried out by Registrars using one of the two systems described below.

ARI operates Extensible Provisioning Protocol (EPP) server software and distributes applicable toolkits to facilitate the receipt of data from Registrars in a common format. EPP offers a common protocol for Registrars to interact with SRS data and is favoured for automating such interaction in the Registrar's systems. In addition to the EPP server, Registrars have the ability to use a web-based management interface (SRS Web Interface), which provides functions equivalent to the EPP server functionality.

### 2.1.1 EPP

The EPP software allows Registrars to communicate with the SRS using a standard protocol. The EPP server software is compliant with all appropriate RFCs and will be updated to comply with any relevant new RFCs or other new standards, as and when they are finalised. All standard EPP operations on SRS objects are supported.

Specifically, the EPP service complies with the following standards:

- RFC 5730 Extensible Provisioning Protocol (EPP).
- RFC 5731 Extensible Provisioning Protocol (EPP) Domain Name Mapping.
- RFC 5732 Extensible Provisioning Protocol (EPP) Host Mapping.
- RFC 5733 Extensible Provisioning Protocol (EPP) Contact Mapping.
- RFC 5734 Extensible Provisioning Protocol (EPP) Transport over TCP.
- RFC 5910 Domain Name System (DNS) Security Extensions for the Extensible Provisioning Protocol (EPP).
- RFC 3915 Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (EPP).
- Extensions to ARI's EPP service comply with RFC 3735 Guidelines for Extending the Extensible Provisioning Protocol (EPP).

#### 2.1.1.1 Security for EPP Service

To avoid abuse and to mitigate potential fraudulent operations, the EPP server software uses a number of security mechanisms that restrict the source of incoming connections and prescribe the authentication and authorisation of the client. Connections are further managed by command rate limiting and are restricted to only a certain number for each Registrar, to help reduce unwanted fraudulent and other activities. Additionally, secure communication to the EPP interface is required, lowering the likelihood of the authentication mechanisms being compromised.

The EPP server has restrictions on the operations it is permitted to make to the data within the registry database. Except as allowed by the EPP protocol, the EPP server cannot update the credentials used by Registrars for access to the SRS. These credentials include those used by Registrars to login to ARI's SRS Web Interface and the EPP service.

Secure communication to the EPP server is achieved via the encryption of EPP sessions. The registry system and associated toolkits support AES 128 and 256 via TLS.

The Production and Operational Testing and Evaluation (OTE) EPP service is protected behind a secure firewall that only accepts connections from registered IP addresses. Registrars are required to supply host IP addresses that they intend to use to access the EPP service.

Certificates are used for encrypted communications with the registry. Registrars require a valid public/private key pair signed by the ARI CA to verify authenticity. These certificates are used to establish a TLS secure session between client and server.

EPP contains credential elements in its specification which are used as an additional layer of authentication. In accordance with the EPP specification, the server does not allow client sessions to carry out any operations until credentials are verified.

The EPP server software combines the authentication and authorisation elements described above to ensure the various credentials supplied are associated with the same identity. This verification requires that:

- The username must match the common name in the digital certificate.
- The certificate must be presented from a source IP listed against the Registrar whose common name appears in the certificate.
- The username and password must match the user name and password listed against the Registrar's account with that source IP address.

To manage normal operations and prevent an accidental or intentional Denial of Service, the EPP server can be configured to rate limit activities by individual Registrars.

#### 2.1.1.2 Stability Considerations

The measures that restrict Registrars to a limit of connections and operations for security purposes also serve to keep the SRS and the EPP server within an acceptable performance and resource utilisation band. Therefore, scaling the service is an almost linear calculation based on well-defined parameters.

The EPP server offers consistent information between Registrars and the SRS Web Interface. The relevant pieces of this information are replicated to the DNS within seconds of alteration, thus ensuring that a strong consistency between the SRS and DNS is maintained at all times.

#### 2.1.2 SRS Web Interface

The registry SRS Web Interface offers Registrars an alternative SRS interaction mechanism to the EPP server. Available over HTTPS, this interface can be used to carry out all operations which would otherwise occur via EPP, as well as many others. Registrars can use the SRS Web Interface, the EPP server interface or both - with no loss of consistency within the SRS.

##### 2.1.2.1 Security and Consistency Considerations for SRS Web Interface

The SRS Web Interface contains measures to prevent abuse and to mitigate fraudulent operations. By restricting access, providing user level authentication and authorisation, and protecting the communications channel, the application limits both the opportunity and scope of security compromise. Registrars are able to create individual users that are associated with their Registrar account. By allocating the specific operations each user can access, Registrars have full control over how their individual staff members interact with the SRS. Users can be audited to identify which operations were conducted and to which objects those operations were applied.

A secure connection is required before credentials are exchanged and once authenticated. On login, any existing user sessions are invalidated and a new session is generated, thereby mitigating session-fixation attacks and reducing possibilities that sessions could be compromised.

##### 2.1.3 Securing and Maintaining Consistency of Registry-Registrar Interaction Systems

ARI ensures all systems through which Registrars interact with the SRS remain consistent with each other and apply the same security rules. Additionally, ARI

also ensures that operations on SRS objects are restricted to the appropriate entity. For example:

- In order to initiate a transfer a Registrar must provide the associated domain password (authinfo) which will only be known by the registrant and the current sponsoring Registrar.
- Only sponsoring Registrars are permitted to update registry objects.

All operations conducted by Registrars on SRS objects are auditable and are identifiable to the specific Registrar's user account, IP address and the time of the operation.

## 2.2 Disseminate Status Information of TLD Zone Servers to Registrars

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

Normal operations are those when:

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

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

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

### 2.2.1 Communication Policy

ARI maintains close communication with Registrars regarding the performance and consistency of the TLD zone servers.

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

Communication using the Registrar contact information discussed above will occur prior to any maintenance that has the potential to effect the access to, consistency of, or reliability of the TLD zone servers. If such maintenance is required within a short time frame, immediate communication occurs using the above contact information. In either case, the nature of the maintenance and how it affects the consistency or accessibility of the TLD zone servers, and the estimated time for full restoration, are included within the communication. That being said, the TLD zone server infrastructure has been designed in such a way that we expect no down time. Only individual sites will potentially require downtime for maintenance; however the DNS service itself will continue to operate with 100% availability.

### 2.2.2 Security and Stability Considerations

ARI restricts zone server status communication to Registrars, thereby limiting the scope for malicious abuse of any maintenance window. Additionally, ARI ensures Registrars have effective operational procedures to deal with any status change of the TLD nameservers and will seek to align its communication policy to those procedures.

## 2.3 Zone File Access Provider Integration

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

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

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

#### 2.4 Zone File Update

To ensure changes within the SRS are reflected in the zone file rapidly and securely, ARI updates the zone file on the TLD zone servers using software compliant with RFC 2136 (Dynamic Updates in the Domain Name System (DNS UPDATE)) and RFC 2845 (Secret Key Transaction Authentication for DNS (TSIG)). This updating process follows a staged but rapid propagation of zone update information from the SRS, outwards to the TLD zone servers - which are visible to the Internet. As changes to the SRS data occur, those changes are updated to isolated systems which act as the authoritative primary server for the zone, but remain inaccessible to systems outside ARI's network. The primary servers notify the designated secondary servers, which service queries for the TLD zone from the public. Upon notification, the secondary servers transfer the incremental changes to the zone and publicly present those changes. The protocols for dynamic update are robust and mature, as is their implementation in DNS software. The protocols' mechanisms for ensuring consistency within and between updates are fully implemented in ARI's TLD zone update procedures. These mechanisms ensure updates are quickly propagated while the data remains consistent within each incremental update, regardless of the speed or order of individual update transactions. ARI has used this method for updating zone files in all its TLDs including the .au ccTLD, pioneering this method during its inception in 2002. Mechanisms separate to RFC 2136-compliant transfer processes exist; to check and ensure domain information is consistent with the SRS on each TLD zone server within 10 minutes of a change.

#### 2.5 Operation of Zone Servers

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

##### 2.5.1 Security and Operational Considerations of Zone Server Operations

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

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

The TLD zone servers are protected from accessibility loss by malicious intent or misadventure, via the provision of significant over-capacity of resources and access paths. Multiple independent network paths are provided to each TLD zone server and the query servicing capacity of the network exceeds the extremely conservatively anticipated peak load requirements by at least 10 times, to prevent loss of service should query loads significantly increase. As well as the authentication, authorisation and consistency checks carried out by the Registrar access systems and DNS update mechanisms, ARI reduces the



scope for alteration of DNS data by following strict DNS operational practices:

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

## 2.6 Dissemination of Contact or Other Information

Registries are required to provide a mechanism to identify the relevant contact information for a domain. The traditional method of delivering this is via the WhoIs service, a plain text protocol commonly accessible on TCP port 43. ARI also provides the same functionality to users via a web-based WhoIs service. Functionality remains the same with the web-based service, which only requires a user to have an Internet browser.

Using the WhoIs service, in either of its forms, allows a user to query for domain-related information. Users can query for domain details, contact details, nameserver details or Registrar details.

A WhoIs service, which complies with RFC 3912, is provided to disseminate contact and other information related to a domain within the TLD zone.

### 2.6.1 Security and Stability Considerations

ARI ensures the service is available and accurate for Internet users, while limiting the opportunity for its malicious use. Many reputation and anti-abuse services rely on the availability and accuracy of the WhoIs service, however the potential for abuse of the WhoIs service exists.

Therefore, certain restrictions are made to the access of WhoIs services, the nature of which depend on the delivery method - either web-based or the traditional text-based port 43 service. In all cases, there has been careful consideration given to the benefits of WhoIs to the Internet community, as well as the potential harm to registrants - as individuals and a group - with regard to WhoIs access restrictions.

The WhoIs service presents data from the registry database in real time. However this access is restricted to reading the appropriate data only. The WhoIs service does not have the ability to alter data or to access data not related to the WhoIs service. The access limitations placed on the WhoIs services prevent any deliberate or incidental denial of service that might impact other registry services.

Restrictions placed on accessing WhoIs services do not affect legitimate use. All restrictions are designed to target abusive volume users and to provide legitimate users with a fast and available service. ARI has the ability to 'whitelist' legitimate bulk users of WhoIs, to ensure they are not impacted by standard volume restrictions.

The data presentation format is consistent with the canonical representation of equivalent fields, as defined in the EPP specifications and ICANN agreement.

#### 2.6.1.1 Port 43 WhoIs

A port 43-based WhoIs service complying with RFC 3912 is provided and will be updated to meet any other relevant standards or best practice guidelines related to the operation of a WhoIs service.

While the text-based service can support thousands of simultaneous queries, it has dynamic limits on queries per IP address to restrict data mining efforts. In the event of identified malicious use of the service, access from a single IP address or address ranges can be limited or blocked.

#### 2.6.1.2 Web-based WhoIs

ARI's web-based WhoIs service provides information consistent with that contained within the SRS.

The web-based WhoIs service contains an Image Verification Check (IVC) and query limits per IP address. These restrictions strike a balance between

acceptable public usage and abusive use or data mining. The web-based WhoIs service can blacklist IP addresses or ranges to prevent abusive use of the service.

## 2.7 IDNs - Internationalised Domain Names

An Internationalised Domain Name (IDN) allows registrants to register domains in their native language and have it display correctly in IDN aware software. This includes allowing a language to be read in the manner that would be common for its readers. For example, an Arabic domain would be presented right to left for an Arabic IDN aware browser.

The inclusion of IDNs into the TLD zones is supported by ARI. All the registry services, such as the EPP service, SRS Web Interface and RDPS (web and port 43), support IDNs. However there are some stability and security considerations related to IDNs which fall outside the general considerations applicable individually to those services.

### 2.7.1 Stability Considerations Specific to IDN

To avoid the intentional or accidental registration of visually similar chars, and to avoid identity confusion between domains, there are several restrictions on the registration of IDNs.

#### 2.7.1.1 Prevent Cross Language Registrations

Domains registered within a particular language are restricted to only the chars of that language. This avoids the use of visually similar chars within one language which mimic the appearance of a label within another language, regardless of whether that label is already within the DNS or not.

#### 2.7.1.2 Inter-language and Intra-language Variants to Prevent Similar Registrations

ARI restricts child domains to a specific language and prevents registrations in one language being confused with a registration in another language, for example Cyrillic a (U+0430) and Latin a (U+0061).

## 2.8 DNSSEC

DNSSEC provides a set of extensions to the DNS that allow an Internet user (normally the resolver acting on a user's behalf) to validate that the DNS responses they receive were not manipulated en-route.

This type of fraud, commonly called 'man in the middle', allows a malicious party to misdirect Internet users. DNSSEC allows a domain owner to sign their domain and to publish the signature, so that all DNS consumers who visit that domain can validate that the responses they receive are as the domain owner intended.

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

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

### 2.8.1 Stability and Operational Considerations for DNSSEC

#### 2.8.1.1 DNSSEC Practice Statement

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

Framework document.

#### 2.8.1.2 Receipt of Public Keys from Registrars

The public key for a child domain is received by ARI from the Registrar via either the EPP or SRS Web Interface. ARI uses an SHA-256 digest to generate the DS Resource Record (RR) for inclusion into the zone file.

#### 2.8.1.3 Resolution Stability

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

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

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

### 3 APPROACH TO SECURITY AND STABILITY

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

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

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

## Demonstration of Technical & Operational Capability

### 24. Shared Registration System (SRS) Performance

The Applicant has engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q24 - ARI Background & Roles.pdf'. This response describes the SRS as implemented by ARI.

#### 1 INTRODUCTION

ARI has demonstrated delivery of an SRS with exceptional availability,

performance and reliability. ARI are experienced running mission critical SRSs and have significant knowledge of the industry and building and supporting SRSs.

ARI's SRS has successfully supported a large group of Registrars for ASCII and IDN based TLDs. The system is proven to sustain high levels of concurrency, transaction load, and system uptime. ARI's SRS meets the following requirements:

- Resilient to wide range of security & availability threats
- Consistently exceeds performance & availability SLAs
- Allows capacity increase with minimal impact to service
- Provides fair & equitable provisioning for all Registrars

## 2 CAPACITY

ARI's SRS was built to sustain 20M domain names. Based on ARI's experience running a ccTLD registries and industry analysis, ARI were able to calculate the conservative characteristics of a registry this size.

Through conservative statistical analysis of the .au registry and data presented in the May 2011 ICANN reports for the .com & .net, .org, .mobi, .info, .biz and .asia [<http://www.icann.org/en/resources/registries/reports>] we know there is:

- An average of 70 SRS TPS per domain, per month
- A ratio of 3 query to 2 transform txs

This indicates an expected monthly transaction volume of 1,400M txs (840M query and 560M transforms).

Through statistical analysis of the .au registry and backed up by the data published in the .net RFP responses [<http://archive.icann.org/en/tlds/net-rfp/net-rfp-public-comments.htm>] we also know:

- The peak daily TPS is 6% of monthly total
- The peak 5 min is 5% of the peak day

Thus we expect a peak EPP tx rate of 14,000 TPS (5,600 transform TPS and 8,400 query TPS)

Through conservative statistical analysis of the .au registry we know:

- The avg no. contacts/domain is 3.76
- The avg no. hosts/domain is 2.28

This translates into a requirement to store 75.2M contacts and 45.6M hosts.

Finally through real world observations of the .au registry, which has a comprehensive web interface when compared to those offered by current gTLD registries, we know there is an avg of 0.5 HTTP requests/sec to the SRS web interface per Registrar. We also know that this behaviour is reasonably flat. To support an estimated 1000 Registrars, would require 500 requests/second. For perspective on the conservativeness of this, the following was taken from data in the May 2011 ICANN reports referenced above:

- .info: ~7.8M names peaks at ~1,400 TPS (projected peak TPS of ~3,600 with 20M)
- .com: ~98M names peaks at ~41,000 TPS (projected peak TPS of ~8,300 TPS with 20M)
- .org: ~9.3M names, peaks at ~1,400 TPS (projected peak TPS of ~3,100 with 20M)

After performing this analysis the projected TPS for .com was still the largest value.

ARI understand the limitations of this method but it serves as a best estimate of probable tx load. ARI has built overcapacity of resources to account for limitations of this method, however as numbers are more conservative than real world observations, we are confident this capacity is sufficient.

This TLD is projected to reach 150000 domains at its peak volume and will generate 105 EPP TPS. This will consume 0,75% of the resources of the SRS infrastructure. As is evident ARI's SRS can easily accommodate this TLD's growth plans. See attachment 'Q24 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI expects to provide Registry services to 100 TLDs and a total of 12M domains by end of 2014. With all the TLDs and domains combined, ARI's SRS infrastructure will be 60% utilized. The SRS infrastructure capacity can be easily scaled as described in Q32

ARI benchmarked their SRS infrastructure and used the results to calculate the

required computing resources for each of the tiers within the architecture; allowing ARI to accurately estimate the required CPU, IOPS, storage and memory requirements for each server, and the network bandwidth & packet throughput requirements for the anticipated traffic. These capacity numbers were then doubled to account for unanticipated traffic spikes, errors in predictions, and headroom for growth. Despite doubling numbers, effective estimated capacity is still reported as 20M. The technical resource allocations are explored in Q32.

### 3 SRS ARCHITECTURE

ARI's SRS has the following major components:

- Network Infrastructure
- EPP Application Servers
- SRS Web Interface Application Servers
- SRS Database

Attachment 'Q24 - SRS.pdf' shows the SRS systems architecture and data flows. Detail on this architecture is in our response to Q32. ARI provides two distinct interfaces to the SRS: EPP and SRS Web. Registrar SRS traffic enters the ARI network via the redundant Internet link and passes (via the firewall) to the relevant application server for the requested service (EPP or SRS Web). ARI's EPP interface sustains high volume and throughput domain provisioning transactions for a large number of concurrent Registrar connections. ARI's SRS Web interface provides an alternative to EPP with a presentation centric interface and provides reporting and verification features additional to those provided by the EPP interface.

#### 3.1 EPP

ARI's EPP application server is based on EPP as defined in RFCs 5730 - 5734. Registrars send XML based transactions to a load balanced EPP interface which forwards to one of the EPP application servers. The EPP application server then processes the XML and converts the request into database calls that retrieve or modify registry objects in the SRS database. The EPP application server tier comprises of three independent servers with dedicated connections to the registry database. Failure of any one of these servers will cause Registrar connections to automatically re-establish with one of the remaining servers. Additional EPP application servers can be added easily without any downtime. All EPP servers accept EPP both IPv4 & IPv6.

#### 3.2 SRS Web

The SRS Web application server is a Java web application. Registrars connect via the load balancer to a secure HTTP listener running on the web servers. The SRS web application converts HTTPs requests into database calls which query or update objects in the SRS database. The SRS Web application server tier consists of two independent servers that connect to the database via JDBC. If one of these servers is unavailable the load balancer re-routes requests to the surviving server. Additional servers can be added easily without any downtime. These servers accept both IPv4 & IPv6.

#### 3.3 SRS Database

The SRS database provides persistent storage for domains and supporting objects. It offers a secure way of storing and retrieving objects provisioned within the SRS and is built on the Oracle 11g Enterprise Edition RDBMS. The SRS Database tier consists of four servers clustered using Oracle Real Application Clusters (RAC). In the event of failure of a database server, RAC will transparently transition its client connections to a surviving database host. Additional servers can be added easily without any downtime.

#### 3.4 Number of Servers

**EPP Servers** - The EPP cluster consists of 3 servers that can more than handle the anticipated 20M domains. This TLD will utilize 0,75% of this capacity at its peak volume. As the utilisation increases ARI will add additional servers ensuring the utilisation doesn't exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime.

**SRS Web Servers** - The SRS Web cluster consists of 2 servers that can more than handle the anticipated 20M domains. This TLD will utilize 0,75% of this

capacity at its peak volume. As the utilisation increases ARI will add additional servers ensuring the utilisation doesn't exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime. SRS DB Servers - The SRS DB cluster consists of 4 servers that can more than handle the anticipated 20M domains. This TLD will utilize 0,75% of this capacity at its peak volume. As the utilisation increases ARI will add additional servers ensuring the total utilisation doesn't exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime.

### 3.5 SRS Security

ARI adopts a multi-layered security solution to protect the SRS. An industry leading firewall is deployed behind the edge router and is configured to only allow traffic on the minimum required ports and protocols. Access to the ARI EPP service is restricted to a list of known Registrar IPs.

An Intrusion Detection device is in-line with the firewall to monitor and detect suspicious activity.

All servers are configured with restrictive host based firewalls, intrusion detection, and SELinux. Direct root access to these servers is disabled and all access is audited and logged centrally.

The SRS database is secured by removal of non-essential features and accounts, and ensuring all remaining accounts have strong passwords. All database accounts are assigned the minimum privileges required to execute their business function.

All operating system, database, and network device accounts are subject to strict password management controls such as validity & complexity requirements. Registrar access to the SRS via EPP or the Web interface is authenticated and secured with multi-factor authentication (NIST Level 3) and digital assertion as follows:

- Registrar's source IP must be allowed by the front-end firewalls. This source IP is received from the Registrar via a secure communication channel from within the SRS Web interface
- Registrar must use a digital certificate provided by ARI
- Registrar must use authentication credentials that are provided by encrypted email

All communication between the Registrar and the SRS is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57.

### 3.6 SRS High Availability

SRS availability is of paramount. Downtime is eliminated or minimised where possible. The infrastructure contains no single points of failure. N+1 redundancy is used as a minimum, which not only protects against unplanned downtime but also allows ARI to execute maintenance without impacting service. Redundancy is provided in the network with hot standby devices & multiple links between devices. Failure of any networking component is transparent to Registrar connections.

N+N redundancy is provided in the EPP and SRS Web application server tiers by the deployment of multiple independent servers grouped together as part of a load-balancing scheme. If a server fails the load balancer routes requests to the remaining servers.

N+N redundancy is provided in the database tier by the use of Oracle Real Application Cluster technology. This delivers active/active clustering via shared storage. This insulates Registrars from database server failure. Complete SRS site failure is mitigated by the maintenance of a remote standby site - a duplicate of the primary site ready to be the primary if required. The standby site database is replicated using real time transaction replication from the main database using Oracle Data Guard physical standby. If required the Data Guard database can be activated quickly and service resumes at the standby site.

### 3.7 SRS Scalability

ARI's SRS scales efficiently. At the application server level, additional computing resource can be brought on-line rapidly by deploying a new server online. During benchmarking this has shown near linear.

The database can be scaled horizontally by adding a new cluster node into the RAC cluster online. This can be achieved without disruption to connections. The SRS has demonstrated over 80% scaling at the database level, but due to the distributed locking nature of Oracle RAC, returns are expected to diminish as the number of servers approaches double digits. To combat this ARI ensures that when the cluster is 'scaled' more powerful server equipment is added rather than that equal to the current members. Capacity can be added to the SAN at any time without downtime increasing storage and IOPs.

### 3.8 SRS Inter-operability and Data Synchronisation

The SRS interfaces with a number of related registry systems as part of normal operations.

#### 3.8.1 DNS Update

Changes made in the SRS are propagated to the DNS via an ARI proprietary DNS Update process. This process runs on the 'hidden' primary master nameserver and waits on a queue. It is notified when the business logic inserts changes into the queue for processing. The DNS Update process reads these queue entries and converts them into DNS update (RFC2136) commands that are sent to the nameserver. The process of synchronising changes to SRS data to the DNS occurs in real-time.

#### 3.8.2 WhoIs

The provisioned data supporting the SRS satisfies WhoIs queries. Thus the WhoIs and SRS share data sets and the WhoIs is instantaneously updated. Under normal operating conditions the WhoIs service is provided by the infrastructure at the secondary site in order to segregate the load and protect SRS from WhoIs demand (and vice versa). WhoIs queries that hit the standby site will query data stored in the standby database - maintained in near real-time using Oracle Active Data Guard. If complete site failure occurs WhoIs and SRS can temporarily share the same operations centre at the same site (capacity numbers are calculated for this).

#### 3.8.3 Escrow

A daily Escrow extract process executes on the database server via a dedicated database account with restricted read-only access. The results are then transferred to the local Escrow Communications server by SSH.

## 4 OPERATIONAL PLAN

ARI follow defined policies/procedures that have developed over time by running critical registry systems. Some principals captured by these are:

- Conduct all changes & upgrades under strict and well-practised change control procedures
- test, test and test again
- Maintain Staging environments as close as possible to production infrastructure/configuration
- Eliminate all single points of failure
- Conduct regular security reviews & audits
- Maintain team knowledge & experience via skills transfer/training
- Replace hardware when no longer supported by vendor
- Maintain spare hardware for all critical components
- Execute regular restore tests of all backups
- Conduct regular capacity planning exercises
- Monitor everything from multiple places but ensure monitoring is not 'chatty'
- Employ best of breed hardware & software products & frameworks (such as ITIL, ISO27001 and Prince2)
- Maintain two distinct OT&E environments to support pre-production testing for Registrars

## 5 SLA, RELIABILITY & COMPLIANCE

ARI's SRS adheres to and goes beyond the scope of Specification 6 and Specification 10 of the Registry Agreement. ARI's EPP service is XML compliant and XML Namespace aware. It complies with the EPP protocol defined in RFC5730, and the object mappings for domain, hosts & contacts are compliant with RFC

5731, 5732 & 5733 respectively. The transport over TCP is compliant with RFC5734. The service also complies with official extensions to support DNSSEC, RFC5910, & Redemption Grace Period, RFC 3915.

ARI's SRS is sized to sustain a peak transaction rate of 14,000 TPS while meeting strict internal Operational Level Agreements (OLAs). The monthly-based OLAs below are more stringent than those in Specification 10 (Section 2).

EPP Service Availability: 100%

EPP Session Command Round Trip Time (RTT): <=1000ms for 95% of commands

EPP Query Command Round Trip Time (RTT): <=500ms for 95% of commands

EPP Transform Command Round Trip Time (RTT): <=1000ms for 95% of commands

SRS Web Interface Service Availability: 99.9%

ARI measure the elapsed time of every query, transform and session EPP transaction, and calculate the percentage of commands that fall within OLA on a periodic basis. If percentage value falls below configured thresholds on-call personnel are alerted.

SRS availability is measured by ARI's monitoring system which polls both the EPP and SRS Web services status. These checks are implemented as full end to end monitoring scripts that mimic user interaction, providing a true representation of availability. These 'scripts' are executed from external locations on the Internet.

## 6 RESOURCES

This function will be performed by ARI. ARI staff are industry leading experts in domain name registries with the experience and knowledge to deliver outstanding SRS performance.

The SRS is designed, built, operated and supported by the following ARI departments:

- Products and Consulting Team (7 staff)
- Production Support Group (27 staff)
- Development Team (11 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided in attachment 'Q24 - ARI Background & Roles.pdf'. This attachment describes the functions of the teams and the number and nature of staff within. The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.

ARI provides registry backend services to 5 TLDs and has a vast experience in estimating the number of resources required to support a SRS.

Based on past experience ARI estimates that the existing staff is adequate to support an SRS that supporting at least 50M domains. Since this TLD projects 150000 domains, 0,3% of these resources are allocated to this TLD. See attachment 'Q24 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required, trained resources can be added to any of the teams with a 2 month lead time.

The Products and Consulting team is responsible for product management of the SRS solution including working with clients and the industry to identify new features or changes required. The team consists of:

- 1 Products and Consulting Manager
- 1 Product Manager
- 1 Technical Product Manager
- 4 Domain Name Industry Consultants

The Production Support Group (PSG) is responsible for the design, deployment and maintenance of the SRS infrastructure including capacity planning and monitoring as well as security aspects - ensuring the SRS services are available and performing at the appropriate level and operating correctly. The team consists of:

- Production Support Manager
- Service Desk:
  - 1 Level 1 Support Team Lead
  - 8 Customer Support Representatives (Level 1 support)



- 1 Level 2 Support Team Lead
- 4 Registry Specialists (Level 2 support)
- Operations (Level 3 support):
  - 1 Operations Team Lead
  - 2 Systems Administrators
  - 2 Database Administrators
  - 2 Network Engineers
- Implementation:
  - 1 Project Manager
  - 2 Systems Administrators
  - 1 Database Administrator
  - 1 Network Engineer

The development team is responsible for implementing changes and new features into the SRS as well as bug fixing and complex issue diagnosis. The team consists of:

- 1 Development Manager
- 2 Business Analysts
- 6 Developers
- 2 Quality Analysts

These resources sufficiently accommodate the needs of this TLD, and are included in ARI's fees as described in our Financial responses.

## 25. Extensible Provisioning Protocol (EPP)

The Applicant has engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q25 - ARI Background & Roles.pdf'. This response describes the Extensible Provisioning Protocol (EPP) interface as implemented by ARI.

### 1 INTRODUCTION

ARI's EPP service is XML compliant and XML Namespace aware. The service complies with the EPP protocol defined in RFC5730, and the object mappings for domain, hosts and contacts are compliant with RFC5731-3 respectively. The transport over TCP is implemented in compliance with RFC5734. The service also complies with the official extensions to support DNSSEC, RFC5910 and Redemption Grace Period, RFC3915. ARI implemented EPP draft version 0.6 in 2002, then migrated to EPP RFC 1.0 on its publishing in 2004. The system has operated live since 2002 in the .au ccTLD.

Descriptions in this response follow the terminology used in the EPP RFCs. When referring to the software involved in the process, ARI's EPP interface is called the server, and the software used by Registrars is called the client.

### 2 TRANSPORT LAYER

The ARI EPP service implements the RFC5734 - EPP Transport over TCP. Connections are allowed using TLSv1 encryption, optionally supporting SSLv2 Hello for compatibility with legacy clients. AES cipher suites for TLS as described in RFC3268 are the only ones allowed.

#### 2.1 Authentication

Registrar access to the EPP interface is authenticated and secured with multi-factor authentication (NIST Level 3) and digital assertion as follows.

Registrars must:

- present a certificate, during TLS negotiation, signed by the ARI Certificate Authority (CA). The server returns a certificate also signed by the ARI CA. Not presenting a valid certificate results in session termination. ARI requires that the Common Name in the subject field of the certificate identifies the

Registrar.

- originate connections from an IP address that is known to be assigned to the Registrar with that Common Name.
- Registrar must use authentication credentials provided to the Registrar via encrypted email
- Registrars aren't able to exceed a fixed number of concurrent connections. The connection limit is prearranged and designed to prevent abuse of Registrars' systems from affecting the Registry. The limit is set to reasonable levels for each Registrar, but can be increased to ensure legitimate traffic is unaffected. If any of the above conditions aren't met the connection is terminated.

All communication between the Registrars and the EPP service is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57.

### 2.3 Connection Close

The server may close the connection as a result of a logout, an error where the state of the connection is indeterminate, or after a timeout. Timeout occurs where no complete EPP message is received on the connection for 10 minutes.

## 3 EPP PROTOCOL

This section describes the interface relating to the EPP protocol described in RFC5730. This includes session management, poll message functionality and object mappings for domains, hosts and contacts.

### 3.1 Session Management

Session management refers to login and logout commands, used to authenticate and end a session with the SRS. The Login command is used to establish a session between the client and the server. This command succeeds when:

- The username supplied matches the Common Name in the digital certificate used in establishing the TLS session.
- The provided password is valid for the user.
- The user's access to the system isn't suspended.

The Logout command is used to end an active session. On processing a logout the server closes the underlying connection. The Hello command can be used as a session keep-alive mechanism.

### 3.2 Service Messages

Offline notifications pertaining to certain events are stored in a queue. The client is responsible for polling this queue for new messages and to acknowledge read messages. Messages include notification about server modification of sponsored objects, transfer operations, and balance thresholds.

## 4 EPP OBJECT MAPPINGS

This section covers the interface for the 3 core EPP objects; domain, host and contact objects, as per RFC5731, 5732, & 5733 respectively.

The EPP domain, contact and host object mapping describes an interface for the check, info, create, delete, renew (domain only), transfer (domain & contact only) and update commands. For domain objects the server doesn't support the use of host attributes as described by RFC5731, but rather uses host objects as described by RFC5731 and RFC5732. Details of each command are:

- check command: checks availability of 1 or more domain, contact or host objects in the SRS. Domain names will be shown as unavailable if in use, invalid or reserved, other objects will be unavailable if in use or invalid.
- info command: retrieves the information of an object provisioned in the SRS. Full information is returned to the sponsoring client or any client that provides authorisation information for the object. Non-sponsoring clients are returned partial information (no more than is available in the WhoIs).
- create command: provisions objects in the SRS. To ascertain whether an object is available for provisioning, the same rules for the check command apply.
- delete command: begins the process of removing an object from the SRS. Domain

names transition into the redemption period and any applicable grace periods are applied. Domain names within the Add Grace Period are purged immediately. All other objects are purged immediately if they are not linked.

- renew command (domain only): extends the registration period of a domain name. The renewal period must be between 1 to 10 years inclusive and the current remaining registration period, plus the amount requested in the renewal mustn't exceed 10 years.
- transfer command (domain and contact only): provides several operations for the management of the transfer of object sponsorship between clients. Clients that provide correct authorisation information for the object can request transfers. Domain names may be rejected from transfer within 60 days of creation or last transfer. The requesting client may cancel the transfer, or the sponsoring client may reject or approve the transfer. Both the gaining and losing clients may query the status of the current pending or last completed transfer.
- update command: updates authorisation information, delegation information (domains), and registration data pertaining to an object.

## 5 NON-PROPRIETARY EPP MAPPINGS

ARI's EPP service implements 2 non-proprietary EPP mappings, to support the required domain name lifecycle and to provide & manage DNSSEC information. The relevant schema documents aren't provided as they are published as RFCs in the RFC repository.

### 5.1 Grace Period Mapping

The Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (as per RFC 3915) is used to support the domain name lifecycle as per existing TLDs. The update command is extended by the restore command to facilitate the restoration of previously deleted domains in the redemption period. This command defines 2 operations, request & report, described here:

- Request operation: requests the restoration of a domain.
- Report operation: completes the restoration by specifying the information supporting the restoration of the domain. The restore report must include a copy of the WhoIs information at both the time the domain was deleted & restored, including the restore reason.

### 5.2 DNSSEC Mapping

The Domain Name System (DNS) Security Extensions Mapping for EPP, as per RFC5910, is used to support the provisioning of DNS Security Extensions. ARI requires clients use the Key Data interface. Clients may associate a maximum of 4 keys per domain. The registry system generates the corresponding DS data using the SHA-256 digest algorithm for the domain and any active variant domains.

ARI is aware of issues DNSSEC causes when transferring DNS providers - a transfer of Registrar usually means a change in DNS provider. DNSSEC key data won't be removed from the SRS or the DNS if a transfer occurs. It is the responsibility of and requires the cooperation of the registrant, Registrars, and DNS providers, to provide a seamless transition. ARI observes progress with this issue and implements industry agreed solutions as available. DNSSEC information is included in info responses when the secDNS namespace in login.

## 6 PROPRIETARY MAPPING

The registry system supports 3 additional EPP extensions where no published standard for the required functionality exists. Developed to conform to the requirements specified in RFC3735, these extensions include the provisioning of Internationalised Domain Names and domain name variants, and the association of arbitrary data with a domain name. These 3 extensions are introduced below, and further described in the attached schema documentation.

### 6.1 Internationalised Domain Names

ARI has developed an extension to facilitate the registration and management of Internationalised Domain Names as per RFCs 5890-5893 (collectively known as the

IDNA 2008 protocol). This extension extends the domain create command and the info response.

The create command is extended to capture the language table identifier that identifies the corresponding IDN language table for the domain name.

Additionally the extension requires the Unicode form to avoid an inconsistency with DNS-form, as per RFC 5891.

The domain info command is extended to identify the language tag and Unicode form provided in the initial create command. This information is disclosed to all querying clients that provided the extension namespace at login. This extension is documented in the attachment 'Q25 - idnadomain-1.0.pdf'.

## 6.2 Variant

ARI has developed an extension to facilitate the management of Domain Name variants. This extension extends the domain update command and the domain create and info responses. The domain update command is extended to allow the addition (activation) and removal (de-activation) of domain name variants subject to registry operator policy.

The domain create and info responses are extended to return the list of activated domain name variants. This information is disclosed to all querying clients that provided the extension namespace at login. The extension is documented in the attachment 'Q25 - variant-1.1.pdf'.

## 6.3 Key-Value

ARI has developed an extension to facilitate the transport of arbitrary data between clients and the SRS without the need for developing EPP Extensions for each specific use-case. This extension extends the domain create and domain update transform commands and the domain info query command. This extension is documented in the attachment 'Q25 - kv-1.0.pdf'.

## 7 ADDITIONAL SECURITY

The registry system provides additional mechanisms to support a robust interface. The use of command rate limiting enables the registry to respond to and withstand erroneous volumes of commands, while a user permission model provides fine-grained access to the EPP interface. These 2 mechanisms are described below.

### 7.1 Rate Limiting

The registry system supports command and global rate limits using a token-bucket algorithm. Limits apply to each connection to ensure fair and equitable use by all. Clients that exceed limits receive a command failed response message indicating breach of the limit.

### 7.2 User Permission Model

The registry system supports a fine-grained permission model controlling access to each specific command. By default, clients receive access to all functionality; however it is possible to remove access to a specific command in response to abuse or threat to stability of the system. Clients that attempt a command they have lost permission to execute, receive an EPP command failed response indicating loss of authorisation.

## 8 COMPLIANCE

Compliance with EPP RFCs is achieved through design and quality assurance (QA). The EPP interface was designed to validate all incoming messages against the respective XML Schema syntax. The XML Schema is copied directly from the relevant RFCs to avoid any ambiguity on version used. Inbound messages that are either malformed XML or invalid are rejected with a 2400 response. Outbound messages are validated against the XML Schema, and if an invalid response is generated, it is replaced with a known valid pre-composed 2400 response, and logged for later debugging.

A QA process provides confidence that changes don't result in regressions in the interface. Automated build processes execute test suites that ensure every facet of the EPP service (including malformed input, commands sequencing and

synchronisation, and boundary values) is covered and compliant with RFCs and the EPP service specification. These tests are executed prior to committing code and automatically nightly. The final deliverable is packaged and tested again to ensure no defects were introduced in the packaging process.

New versions of the EPP Service follow a deployment schedule. The new version is deployed into an OT&E environment for Registrar integration testing. Registrars are encouraged during this stage to test their systems operate correctly. After a fixed time in OT&E without issue, new versions are scheduled for production deployment. This ensures incompatibilities with RFCs that made it through QA processes are detected in test environments prior reaching production.

ARI surveys Registrars for information about the EPP client toolkit. These surveys indicated that while many Registrars use ARI toolkits, several Registrars use either their own or that from another registry. The ability for Registrars to integrate with the ARI EPP service without using the supplied toolkit indicates the service is compliant with RFCs.

ARI is committed to providing an EPP service that integrates with third party toolkits and as such tests are conducted using said toolkits. Any issues identified during testing fall into the following categories:

- Third-party toolkit not compliant with EPP
- EPP service not compliant with EPP
- Both third-party toolkit and EPP service are compliant, however another operational issue causes an issue

Defects are raised and change management processes are followed. Change requests may also be raised to promote integration of third-party toolkits and to meet common practice.

## 9 CAPACITY

This TLD is projected to reach 150000 domains at its peak volume and will generate 105 EPP TPS. This will consume 0,75% of the EPP resources. ARI's SRS can easily accommodate this TLD. This was described in considerable detail in the capacity section of question 24.

## 10 RESOURCES

This function will be performed by ARI. ARI provides a technical support team to support Registrars and also provides Registrars with a tool kit (in Java and C++) implementing the EPP protocol. Normal operations for all registry services are managed by ARI's Production Support Group (PSG), who ensure the EPP server is available and performing appropriately.

Faults relating to connections with or functionality of the EPP server are managed by PSG. ARI monitors EPP availability and functionality as part of its monitoring practices, and ensures PSG staff are available to receive fault reports from Registrars any time. PSG has the appropriate network, Unix and application (EPP and load balancing) knowledge to ensure the EPP service remains accessible and performs as required. These ARI departments support EPP:

- Products and Consulting Team (7 staff)
- Production Support Group (27 staff)
- Development Team (11 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q25 - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system. Based on past experience ARI estimates that existing staff are adequate to support a registry system that supports in excess of 50M domains. Since this TLD projects 150000 domains, 0,3% of these resources are allocated to this TLD. See attachment 'Q25 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required, trained resources can be added to any of the above teams with a 2-month lead time.

#### 10.1 Team Details

The products and consulting team is responsible for product management of the EPP solution, and works with clients and industry to identify required system features or changes. The team consists of:

- 1 Products and Consulting Manager
- 1 Product Manager
- 1 Technical Product Manager
- 4 Domain Name Industry Consultants

The Production Support Group (PSG) is responsible for the design, deployment and maintenance of the EPP infrastructure including capacity planning, monitoring, and security. This team ensures the EPP services are available and performing appropriately. The team consists of:

- Production Support Manager
- Service Desk:
  - 1 Level 1 Support Team Lead
  - 8 Customer Support Representatives (Level 1 support)
  - 1 Level 2 Support Team Lead
  - 4 Registry Specialists (Level 2 support)
- Operations (Level 3 support):
  - 1 Operations Team Lead
  - 2 Systems Administrators
  - 2 Database Administrators
  - 2 Network Engineers
- Implementation:
  - 1 Project Manager
  - 2 Systems Administrators
  - 1 Database Administrator
  - 1 Network Engineer

The development team is responsible for EPP changes and features, bug fixes and issue diagnosis. The team consists of:

- 1 Development Manager
- 2 Business Analysts
- 6 Developers
- 2 Quality Analysts

These resources sufficiently accommodate the needs of this TLD, and are included in ARI's fees as described in our financial responses.

## 26. Whois

The Applicant has engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q26 - ARI Background & Roles.pdf'. This response describes the WhoIs interface as implemented by ARI.

### 1 INTRODUCTION

ARI's WhoIs service is for all domain names, contacts, nameservers and Registrars provisioned in the registry database. This response describes the port 43 and web interfaces of WhoIs, security controls to mitigate abuse, compliance with bulk access requirements for registration data, and the architecture delivering the service.

## 2 PORT 43 WHOIS SERVICE

WhoIs is on TCP port 43 in accordance with RFC3912. Requests are made in semi-free text format and ended by CR & LF. The server responds with a semi-free text format, terminating the response by connection close.

To support IDNs and Localised data we assume the query is encoded in UTF-8 and sends responses encoded in UTF-8. UTF-8 is backwards compatible with the ASCII charset and its use is consistent with the IETF policy on charsets as defined in BCP 18 [<http://tools.ietf.org/html/bcp18>].

### 2.1 Query Format

By default WhoIs searches domains. To facilitate the queries of other objects keywords must be used. Supported keywords are:

- Domain
- Host/Nameserver
- Contact
- Registrar

Keywords are case-insensitive. The rest of the input is the search string. Wildcard chars may be used in search strings to match zero or more chars (%), or match exactly one char(\_). Wildcard chars must not be in the first 5 chars.

### 2.2 Response Format

The response follows a semi-structured format of object-specific data, followed by query-related meta-information, then a disclaimer.

The object-specific data is represented by key/value pairs, beginning with the key, followed by a colon and a space then the value terminated by an ASCII CR & LF. Where no object is found 'No Data Found' is returned.

The meta-information is used to identify data freshness and indicate when limits have been exceeded. It appears on one line within ' > > > ' and ' < < < ' chars.

The legal disclaimer is presented without leading comment marks wrapped at 72 chars. This format is consistent with that in the registry agreement.

### 2.3 Domain Data

Domain data is returned in response to a query with the keyword omitted, or with the 'domain' keyword. Domain queries return information on domains that are provisioned in the registry database.

The IDN domains may be specified in either the ASCII-compatible encoded form or the Unicode form. Clients are expected to perform any mappings, in conformance with relevant guidelines such as those specified in RFC5894 and UTS46.

Variant domains may be specified in the search string and WhoIs will match (using case-insensitive comparison) and return information for the primary registered domain.

For queries containing wildcard chars, if only one domain name is matched its details are returned, if more than one domain name is matched then the first 50 matched domain names are listed.

#### 2.3.1 Internationalised Domain Names

The WhoIs response format, prescribed in Specification 4, does not provide a mechanism to identify active variant domain names. ARI will include active variant domain names in WhoIs responses until a common approach for handling and display of variant names is determined.

#### 2.3.2 Reserved Domain Names

Domain names reserved from allocation will have a specific response that indicates the domain is not registered but also not available.

### 2.4 Nameserver Data

Nameserver data is returned in response to a query where the 'nameserver' or 'host' keywords have been used. Nameserver queries return information on hosts that are provisioned in the registry.

The search string for a nameserver query can be either a hostname or IP.

Queries using the hostname produce one result unless wildcards are used.

Queries using the IP produce one or more results depending on the number of

hostnames that match that address. Queries for the hostname are matched case-insensitively.

The quad-dotted notation is expected for IPv4 and the RFC3513 - IPv6 Addressing Architecture format for IPv6. Wildcards cannot be used for IP queries.

#### 2.5 Contact Data

Contact data is returned in response to a query where the 'contact' keyword was used. Contact queries return information on contacts that are provisioned in the registry.

The search string for a contact query is the contact identifier. Contact identifiers are matched using a case-insensitive comparison. Wildcards cannot be used.

#### 2.6 Registrar Data

Registrar data is returned in response to a query where the 'Registrar' keyword was used. Registrar queries return information on Registrar objects that are provisioned in the registry.

The search string for a Registrar query can be name or IANA ID. Queries using the name or the IANA ID produce only one result. Queries for the name are matched using a case-insensitive comparison. Wildcards cannot be used.

#### 2.7 Non-standard Data

The SRS supports domain-related data beyond that above. It may include information used to claim eligibility to participate in the sunrise process, or other arbitrary data collected using the Key-Value Mapping to the EPP. This information will be included in the WhoIs response after the last object-specific data field and before the meta-information.

### 3 WEB-BASED WHOIS SERVICE

WhoIs is also available via port 80 using HTTP, known as Web-based WhoIs. This interface provides identical query capabilities to the port 43 interface via an HTML form.

### 4 SECURITY CONTROLS

WhoIs has an in-built mechanism to blacklist malicious users for a specified duration. Blacklisted users are blocked by source IP address and receive a specific blacklisted notification instead of the normal WhoIs response. Users may be blacklisted if ARI's monitoring system determines excessive use. A whitelist is used to facilitate legitimate use by law enforcement agencies and other reputable entities.

### 5 BULK ACCESS

The registry system complies with the requirements for the Periodic Access to Thin Registration Data and Exceptional Access to Thick Registration Data as described in Specification 4.

#### 5.1 Periodic Access to Thin Registration Data

ARI shall provide ICANN with Periodic Access to Thin Registration Data. The data will contain the following elements as specified by ICANN. The format of the data will be consistent with the format specified for Data Escrow. The Escrow Format prescribes an XML document encoded in UTF-8. The generated data will be verified to ensure that it is well formed and valid.

The data will be generated every Monday for transactions committed up to and on Sunday unless otherwise directed by ICANN. The generated file will be made available to ICANN using SFTP. Credentials, encryption material, and other parameters will be negotiated between ARI and ICANN using an out-of-band mechanism.

#### 5.2 Exceptional Access to Thick Registration Data

If requested by ICANN, ARI shall provide exceptional access to thick registration data for a specified Registrar. The data will contain full



information for the following objects:

- Domain names sponsored by the Registrar
- Hosts sponsored by the Registrar
- Contacts sponsored by the Registrar
- Contacts linked from domain names sponsored by the Registrar

As above the format of the data will be consistent with the format specified for Data Escrow. And will be made available to ICANN using SFTP.

## 6 CAPACITY

ARI's WhoIs infrastructure is built to sustain 20M domain names. Based on ARI's experience running a high volume ccTLD registry (.au) and industry analysis, ARI were able to calculate the conservative characteristics of a registry of this size.

Through conservative statistical analysis of the .au registry and data presented in the May 2011 ICANN reports for the .com & .net, .org, .mobi, .info, .biz and .asia [<http://www.icann.org/en/resources/registries/reports>] we know there is:

- An average of 30 SRS txs per domain, per month.

Which indicates an expected monthly transaction volume of 600M txs?

Through statistical analysis of the .au registry and backed up by the data published in the .net RFP responses [<http://archive.icann.org/en/tlds/net-rfp/net-rfp-public-comments.htm>] we also know:

- The peak daily transactions is 6% of the monthly total
- The peak 5 min is 5% of the peak day

Thus we expect a peak WhoIs tx rate of WhoIs 6,000 TPS.

For perspective on the conservativeness of this, the following numbers were taken from data in the May 2011 ICANN reports referenced above:

- .info ~7.8M domain names, peaks at ~1,300 TPS (projected peak TPS of ~3,400 with 20M names).
- .mobi ~1M domain names, peaks at ~150 TPS (projected peak TPS of ~3,000 TPS with 20M names).
- .org ~9.3M domain names, peaks at ~1,300 TPS (projected peak TPS of ~2,800 with 20M names).

ARI understand the limitations of these calculations but they serve as a best estimate of probable transaction load. ARI has built overcapacity of resources to account for limitations of this method, however as conservative numbers were used and these are greater than real world observations, we are confident these capacity numbers are sufficient.

ARI benchmarked their WhoIs infrastructure and used the results to calculate the required computing resources for each of the tiers within the WhoIs architecture - allowing ARI to accurately estimate the required CPU, IOPS, storage and memory requirements for each server within the architecture, as well as the network bandwidth and packet throughput requirements for the anticipated WhoIs traffic. These capacity numbers were then doubled to account for unanticipated traffic spikes, errors in predictions and head room for growth. The technical resource allocations are explored in question 32. This TLD is projected to reach 150000 domains at its peak volume and will generate 45 WhoIs transactions per second. This will consume 0,75% of the resources of the WhoIs infrastructure. As is evident ARI's WhoIs can easily accommodate this TLD's growth plans. See attachment 'Q26 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI expects to provide Registry services to 100 TLDs and a total of 12M domains by end of 2014. With all the TLDs and domains combined, ARI's WhoIs infrastructure will be only 60% utilized. The WhoIs infrastructure capacity can also be easily scaled as described in question 32

## 7 ARCHITECTURE

WhoIs uses a database separate from the SRS database as it operates from the secondary site such that network and database resources are decoupled from the operation of the SRS. Oracle Data Guard ensures the two databases are synchronised in real-time. The WhoIs service is operated live from the SRS 'failover' site, with the SRS 'primary' site serving as the 'failover' site for

the WhoIs service. Both sites have enough capacity to run both services simultaneously, however by separating them, in normal operating modes headroom above the already over provisioned capacity is available. The architecture and data flow diagrams are described below and shown in the attachment 'Q26 - WhoIs.pdf'.

Traffic enters the network from the Internet through border routers and then firewalls. All traffic destined for this service except for TCP ports 43, 80 & 443 is blocked. Load balancers forward the request to one of the application servers running ARI built WhoIs software. Each server is connected to the database cluster through another firewall further restricting access to the. Each server uses a restricted Oracle user that has read only access to the registry data and can only access the data that is relevant to the WhoIs queries. This ensures that in the unlikely event of an application server compromise the effects are limited.

All components are configured and provisioned to provide N+1 redundancy. Multiple Internet providers with separate upstream bandwidth suppliers are used. At least one additional component of all hardware exists, enabling maintenance without downtime. This configuration provides a service exceeding the availability requirements in Specification 10.

The use of load balancing allows addition of application servers with no downtime. From a database perspective, the ability to scale is enabled by utilising Oracle RAC database clustering. The entire service, including routers, firewalls and application is IPv6 compatible and WhoIs is offered on both IPv4 and IPv6. Detail about this architecture is available in our response to Question 32.

#### 7.1 Synchronisation

The WhoIs database is synchronised with the SRS database using Oracle Data Guard. Committed transactions in the SRS database are reflected in the WhoIs database in real-time. Should synchronisation break, WhoIs continues to operate with the latest available data until the issue is reconciled. The channel between the two sites consists of two independent dedicated point to point links as well as the Internet. Replication traffic flows via the dedicated links or if both links fail replication traffic flows over Internet tunnels.

#### 7.2. Interconnectivity with Other Services

The WhoIs service is not directly interconnected with other registry services or systems. The software has been developed to provide the WhoIs service exclusively and retrieve response information from a database physically separate to the SRS transactional database. This database is updated as described in 'Synchronisation' above. Although for smaller system the WhoIs and SRS can be configured to use the same data store. The WhoIs servers log every request to a central repository that is logically separate from the WhoIs database. This repository is used for query counts, detection of data mining and statistical analysis on query trends.

#### 7.3 IT and Infrastructure Resources

The WhoIs service is provided utilizing Cisco networking equipment, IBM servers & SAN. They are described in the attachment 'Q26 - WhoIs.pdf'. For more information on the architecture including server specifications and database capabilities please see Questions 32 & 33.

### 8 COMPLIANCE

Compliance with WhoIs RFCs is achieved through design and QA. The WhoIs interface was designed to conform to the RFCs as documented and independent test cases have been developed.

QA processes provide confidence that any changes to the service don't result in regression of the WhoIs. Automated build processes execute test suites that ensure every facet of the WhoIs service (including malformed input, commands sequencing and synchronisation, and boundary values) is covered and compliant with RFCs. These tests are executed prior to the committing of code and nightly. The final deliverable is packaged and tested again to ensure no defects were introduced in the packaging of the software.

New versions of the WhoIs follow a deployment schedule. The new version is deployed into an OT&E environment for Registrar integration testing. Registrars who rely on WhoIs functionality are encouraged during this stage to test their systems operate without change. After a fixed time in OT&E without issue, new versions are scheduled for production deployment. This ensures incompatibilities with RFCs that made it through QA processes are detected in test environments prior to reaching production.

ARI is committed to providing a WhoIs service that integrates with third party tools and as such tests are conducted using these tools such as jWhoIs, a popular UNIX command line WhoIs client. Any issues identified during integration fall into 1 of the following categories:

- Third-party tool not compliant with the WhoIs specification
- WhoIs service not compliant
- Both third-party tool and WhoIs service are compliant, however another operational issue causes a problem

Defects are raised and follow the change management. Change requests may also be raised to promote integration of third-party tools and to meet common practice.

## 9 RESOURCES

This function will be performed by ARI. The WhoIs system is supported by a number of ARI departments:

- Products and Consulting Team (7 staff)
- Production Support Group (27 staff)
- Development Team (11 staff)
- Legal, Abuse and Compliance Team (6 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q26 - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system. Based on past experience ARI estimates that the existing staff is adequate to support a registry system that supports in excess of 50M domains. Since this TLD projects 150000 domains, 0,3% of these resources are allocated to this TLD. See attachment 'Q26 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

The products and consulting team is responsible for product management of the WhoIs solution including working with clients and the industry to identify new features or changes required to the system. The team consists of:

- 1 Products and Consulting Manager
- 1 Product Manager
- 1 Technical Product Manager
- 4 Domain Name Industry Consultants

ARI employ a development team responsible for the maintenance and continual improvement of the WhoIs software. The team consists of:

- 1 Development Manager
- 2 Business Analysts
- 6 Developers
- 2 Quality Analysts

ARI's Production Support Team ensures the successful operation of the WhoIs system. The team comprises Database Administrators, Systems Administrators and Network Administrators. This team routinely checks and monitors bandwidth, disk and CPU usages to plan and respond to expected increases in the volume of queries, and perform maintenance of the system including security patches and

failover and recovery testing. The team consists of:

- Production Support Manager
- Service Desk:
  - 1 Level 1 Support Team Lead
  - 8 Customer Support Representatives (Level 1 support)
  - 1 Level 2 Support Team Lead
  - 4 Registry Specialists (Level 2 support)
- Operations (Level 3 support)
  - 1 Operations Team Lead
  - 2 Systems Administrators
  - 2 Database Administrators
  - 2 Network Engineers
- Implementation
  - 1 Project Manager
  - 2 Systems Administrators
  - 1 Database Administrators
  - 1 Network Engineers

ARI's registry provides abuse monitoring detection mechanisms to block data mining. ARI support staff may be contacted to remove blacklisted users during which they may be referred to the Legal, Abuse and Compliance Team for evaluation of their activities. Additionally the support team in conjunction with the Legal, Abuse and Compliance team administer requests for listing on the whitelist. The team consists of:

- 1 Legal Manager
- 1 Legal Counsel
- 4 Policy Compliance Officers

These resources sufficiently accommodate the needs of this TLD, and are included in ARI's fees as described in our Financial responses.

## 27. Registration Life Cycle

The Applicant has engaged ARI to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q27 - ARI Background & Roles.pdf'. This response describes the Registration Lifecycle as implemented by ARI.

### 1 INTRODUCTION

The lifecycle described matches current gTLD registries. All states, grace periods and transitions are supported by the EPP protocol as described in RFC5730 - 5734 & the Grace Period Mapping published in RFC3915. An overview is in attachment 'Q27 - Registration Lifecycle.pdf'.

### 2 REGISTRATION PERIODS

The registry supports registration up to 10 years and renewals for 1 to 10 years. The total current validity period can't exceed 10 years. Transfers under part A of the ICANN Policy on Transfer of Registrations between Registrars (Adopted 7 November 2008) extend registration by 1 year. The period truncates to 10 years if required.

### 3 STATES

The states that a domain can exist in are: Registered, Pending Transfer, Redemption, Pending Restore & Pending Delete. All domain name statuses (RFC3915, 5730-5734 and 5910) are covered below

#### 3.1 Registered

EPP Status: ok

In DNS: Yes

Allowed Operations: Update, Renew, Transfer (request) & Delete

The default state of a domain - no pending operations. The sponsoring Registrar may update the domain.

### 3.2 Pending Transfer

EPP Status: pendingTransfer

In DNS: Yes

Allowed Operations: Transfer (cancel, reject, approve)

Another Registrar has requested transfer of the domain and it is not yet completed. All transform operations, other than those to cancel, reject, or approve the transfer are rejected.

### 3.3 Redemption

EPP Status: pendingDelete

RGP Status: redemptionPeriod

In DNS: No

Allowed Operations: Restore (request)

Domain has been deleted. The sponsor may request restoration of the domain. The domain continues to be withheld from the DNS unless it is restored. No transform operations other than restore are allowed.

### 3.4 Pending Restore

EPP Status: pendingDelete

RGP Status: pendingRestore

In DNS: Yes

Allowed Operations: Restore (report)

A restore request is pending. The sponsor must submit a restore report. The domain is provisioned the DNS. No transform operations other than the restore report are allowed.

### 3.5 Pending Delete

EPP Status: pendingDelete

RGP Status: pendingDelete

In DNS: No

Allowed Operations: None

The Redemption Grace Period has lapsed and the domain is pending purge from the registry. This state prohibits the sponsor from updating, restoring or modifying the domain. This status applies for 5 days. At the end of this period the domain is purged from the database and made available for registration.

## 4 GRACE PERIODS

The registry system supports 4 grace periods: add, renew, auto-renew, and transfer, described below with consideration for overlap of grace periods. States described here are additional to those above.

### 4.1 Add Grace Period

Length: 5 days

RGP Status: addPeriod

Allows for the no-cost cancellation of a domain registrations resulting from typing mistakes and other errors by Registrars and registrants - beginning on the creation of a domain and lasting for 5 days. When the following operations are performed during this period these rules apply:

- Delete: the sponsoring Registrar, who must have created the domain, may delete the domain and receive a refund. The domain is deleted with immediate effect. The refund is subject to the Add Grace Period Limits consensus policy. Excess deletions over 50 or 10% of creates (whichever is greater), are not subject to a refund, except in extraordinary circumstances.
- Renew: the sponsor may renew the domain but does not receive any refund for the initial registration fee. The Registrar is charged for the renewal operation. The total period for the domain is the sum of the initial period in the create and any renewal term, limited to a 10 year maximum.

- Transfer: Under ICANN policy a transfer can't occur during the Add Grace Period or at any other time in the first 60 days after the initial registration. The registry system enforces this, rejecting such requests.
- Bulk Transfers: Under Part B of the ICANN Policy on Transfer of Registrations between Registrars, a bulk transfer can occur during the Add Grace Period. Any bulk transfer causes the Add Grace Period to not apply. The Add Grace Period does not have any impact on other commands.

#### 4.2 Renew Grace Period

Length: 5 days

RGP Status: renewPeriod

Allows the sponsoring Registrar to undo a renewal via the deletion of a domain

- beginning on the receipt of a renewal command and lasting for 5 days. If any of the following operations are performed during this period these rules apply:
  - Delete: the sponsoring Registrar, who must have initiated the renewal, may delete the domain and receive a renewal fee refund. The extension to the registration period caused by the preceding renew is reversed and unless the domain is also in the Add Grace Period, the domain enters the Redemption state. If also in the Add Grace Period it is deleted with immediate effect and availability for registration.
  - Renew: the sponsoring Registrar, who must have performed the initial renew, can subsequently renew the domain again, causing a second independent Renewal Grace Period to start. The Registrar is charged for the operation and the total registration period for the domain is extended by the renewal term, limited to the 10 year maximum.
  - Transfer: an approved transfer command ends the current Renew Grace Period without a refund and begins a Transfer Grace Period.
  - Bulk Transfers: bulk transfers cause the Renew Grace Period to end without a refund, consequently registration periods are not changed. The Renew Grace Period has no impact on other commands.

#### 4.3 Auto-Renew Grace Period

Length: 45 days

RGP Status: autoRenewPeriod

Auto-Renew Grace Period allows for domains to remain in the DNS past registration expiration while giving adequate time for the sponsoring Registrar to obtain intention of renewal from the registrant.

This period begins on the expiration of the domain and lasts for 45 days. If any of the following are performed during this period these rules apply:

- Delete: the sponsoring Registrar, who must be the sponsor when the Auto-Renew Grace Period commenced, may delete the domain and receive an auto-renew fee refund. The registration period auto-renew extension is reversed and the domain enters the Redemption state.
- Renew: the sponsoring Registrar, who must be the sponsor when the auto-renew occurred, can renew the domain again causing an independent Renewal Grace Period to begin. The Registrar is charged and the registration period is extended by the renewal term, limited to the 10 year maximum.
- Transfer: an approved transfer command ends the current Auto-Renew Grace Period with a refund to the losing Registrar and begins a Transfer Grace Period. The registration period auto-renew extension is reversed and the registration is extended by the period specified in the transfer.
- Bulk Transfers: bulk transfers cause the Auto-Renew Grace Period to end without a refund consequently registration periods are not changed. The Auto-Renew Grace Period does not have any impact on other commands.

#### 4.4 Transfer Grace Period

Length: 5 days

RGP Status: transferPeriod

Transfer Grace Period allows the sponsoring Registrar to undo the registration period extension (due to a transfer command), via the deletion of a domain.

This period begins on a transfer completion and lasts for 5 calendar days. If the following are performed during the period these rules apply:

- Delete: the sponsoring Registrar, who must have initiated the transfer, may delete the domain and receive a transfer fee refund. The extension to the

registration period of the preceding transfer is reversed and the Redemption state is entered.

- Renew: the sponsoring Registrar can renew the domain thus causing an independent Renewal Grace Period to begin. The Registrar is charged and the registration period for the domain is extended by the renewal term, limited to the 10 year maximum.
- Transfer: under Part A of the ICANN Policy on Transfer of Registrations between Registrars a transfer may not occur during the 60 day period after transfer (except in special circumstances). The registry system enforces this - effects of transfer do not require consideration. Should a special situation require transfer back to the losing Registrar, this is dealt with by taking into account the specific situation. The registry system does not allow this without intervention by registry staff.
- Bulk Transfers: bulk transfers cause the Transfer Grace Period to end without a refund; consequently registration periods are not changed. The Transfer Grace Period does not have any impact on other commands.

#### 4.5 Redemption Grace Period

Length: 30 days

RGP Status: as described in Redemption state

Redemption Grace Period refers to the period of time the domain spends in the Redemption state, starting after a domain is deleted. The Redemption state description provides information on operations during this period.

#### 4.6 Overlap of Grace Periods

The 4 possible overlapping grace periods are:

- Add Grace Period with 1 or more Renew Grace Periods.
- Renew Grace Period with 1 or more other Renew Grace Periods.
- Transfer Grace Period with 1 or more Renew Grace Periods.
- Auto-Renew Grace Period with 1 or more Renew Grace Periods.

These are treated independently with respect to timelines however action that is taken has the combined effects of all grace periods still current.

##### 4.6.1 Transfer Clarification

If several billable operations, including a transfer, are performed on a domain and it is deleted in the operations' grace periods, only those operations performed after including the latest transfer are eligible for refund.

## 5 TRANSITIONS

### 5.1 Available > Registered

Triggered by the receipt of a create command to register the domain. The sponsoring Registrar is charged for the creation amount. This transition begins the Add Grace Period.

### 5.2 Registered > Pending Transfer

Triggered by the receipt of a request transfer command. The transfer must result in domain registration extension - the gaining Registrar is charged for the transfer. Requests to transfer the domain within 60 days of creation or a previous transfer are rejected. As per '4.4 Transfer Grace Period', exceptions specified in ICANN's Transfer Policy apply - dealt with individually.

### 5.3 Pending Transfer > Registered

Triggered by 1 of 4 operations:

- Operation 1 (Cancel): during the Pending Transfer period the gaining Registrar may cancel the transfer by issuing a cancel transfer command. The gaining Registrar is refunded the transfer fee, the registration period remains unchanged and all existing grace periods at the time of transfer request remain in effect.
- Operation 2 (Reject): during the Pending Transfer period the losing Registrar may reject the transfer by issuing a reject transfer command. The gaining Registrar is refunded the transfer. The registration period remains unchanged and all grace periods existing at the time of transfer request remain in effect if not elapsed.

- Operation 3 (Approve): During the Pending Transfer period the losing Registrar may approve the transfer by issuing an approve transfer command. If the transfer was requested during the Auto-Renew Grace Period, the extension to the registration period is reversed and the losing Registrar is refunded the auto-renew. The registration period is extended by the amount specified in the transfer request. This begins the Transfer Grace Period.

- Operation 4 (Auto-Approve): If after 5 days, no action has been taken, the system approves the transfer. If the transfer was requested during the Auto-Renew Grace Period the extension to the registration period is reversed and the losing Registrar is refunded the auto-renew. The registration period is extended by the amount specified in the transfer request. This begins the Transfer Grace Period.

#### 5.4 Registered ) Deleted

On receipt of a delete command if the domain is in the Add Grace Period, it is purged from the Database and immediately available for registration. Renew Grace Period may also be in effect.

#### 5.5 Registered ) Redemption

On receipt of a delete command if the domain is not in the Add Grace Period, it transitions to the Redemption Period state and all grace periods in effect are considered.

#### 5.6 Redemption ) Pending Restore

On receipt of a restore command if the Redemption Period has not lapsed, the domain transitions to the Pending Restore state. The domain is provisioned in the DNS. The sponsoring Registrar is charged a fee for the restore request.

#### 5.7 Pending Restore ) Registered

During the Pending Restore period the sponsoring Registrar may complete the restore via a restore report containing the WhoIs information - submitted prior to the deletion, the WhoIs information at the time of the report, and the reason for the restoration.

#### 5.8 Pending Restore ) Redemption

Seven calendar days after the transition to the Pending Restore state, if no restore report is received the domain transitions to the Redemption state, which begins a new redemption period. The domain is removed from the DNS. The restore has no refund.

#### 5.9 Redemption ) Pending Delete

Thirty calendar days after the transition to the Redemption state, if no restore request is received the domain transitions to the Pending Delete state.

#### 5.10 Pending Delete ) Deleted

Five calendar days after the transition to the Pending Delete state, the domain is removed from the Database and is immediately available for registration.

## 6 LOCKS

Locks may be applied to the domain to prevent specific operations occurring. The sponsoring Registrar may set the locks prefixed with 'client' while locks prefixed with 'server' are added and removed by the registry operator. Locks are added and removed independently but they can be combined to facilitate the enforcement of higher processes, such as 'Registrar Lock', and outcomes required as part of UDRP. All locks are compatible with EPP RFCs. The available locks are:

- clientDeleteProhibited, serverDeleteProhibited - Requests to delete the object are rejected
- clientHold, serverHold - DNS information is not published
- clientRenewProhibited, serverRenewProhibited - Requests to renew the object are rejected. Auto-renew is allowed
- clientTransferProhibited, serverTransferProhibited - Requests to transfer the object are rejected



- clientUpdateProhibited, serverUpdateProhibited - Requests to update the object are rejected, unless the update removes this status

## 7 SPECIAL CONSIDERATIONS

### 7.1 ICANN-Approved Bulk Transfers

ICANN-Approved Bulk Transfers do not follow the typical transfer lifecycle. Existing grace periods are invalidated and no refunds are credited to the losing Registrar. The prohibition of transfer period on domains created or transferred within 60 days does not apply.

### 7.2 Uniform Rapid Suspension

In the Uniform Rapid Suspension (URS) process, as described in the 'gTLD Applicant Guidebook' 11th January 2012, the following modification to the above processes is required.

Remedy allows for the addition of a year to the registration period, limited to the 10 year maximum. During this time no transform operations may be performed other than to restore the domain as allowed by Appeal. At the expiration of the registration period the domain is not automatically renewed, but proceeds to the Redemption state as per the lifecycle described above, and it is not eligible for restoration.

## 8 UPDATE/DNS

The update command does not impact the state of the domain through the Registration Lifecycle, however the command can be used to add and remove delegation information, which changes the DNS state of the domain. A domain is required to have 2 or more nameservers published in the DNS. An update that results in a domain having less than 2 nameservers removes the domain from the DNS. An exception is when 1 nameserver remains assigned to a domain due to deletion of its other nameservers due to purge of their parent domain. The next update that modifies delegation information ends the exception and from then on the domain requires 2 nameservers be in the DNS.

## 9 RESOURCES

This function will be performed by ARI. ARI's registry performs all time-based transitions automatically and enforces all other business rules - without requiring human resources for normal operation. If changes to the automatic behaviours or restrictions enforced by the policy system are required, ARI has a development team for this.

Domain Name Lifecycle aspects requiring human resources to manage are included in the ARI outsourcing include:

- Processing Add Grace Period exemptions as requested by Registrars.
- Processing restore reports provided by Registrars.
- Meeting the registry operator's obligations under ICANN's Transfer Dispute Policy.
- Performing exception processing in the case of approved transfers during the 60 day transfer prohibition window.

The Registration Lifecycle is designed, built, operated and supported by these ARI departments:

- Products and Consulting Team (7 staff)
- Legal, Abuse and Compliance Team (6 staff)
- Development Team (11 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q27 - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system. Based on past experience ARI estimates that the existing staff is adequate to

support a registry system that supports in excess of 50M domains. Since this TLD projects 150000 domains, 0,3% of these resources are allocated to this TLD. See attachment 'Q27 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

The Products and Consulting team is responsible for product management of the Registration Lifecycle, including working with clients and the industry to identify new features or changes required to the system. The team consists of:

- 1 Products and Consulting Manager
- 1 Product Manager
- 1 Technical Product Manager
- 4 Domain Name Industry Consultants

Most manual tasks fall to the Legal, Abuse and Compliance team, with staff experienced in development of policy for policy rich TLD environments. They have the required legal and industry background to perform this function. The team consists of:

- 1 Legal Manager
- 1 Legal Counsel
- 4 Policy Compliance Officers

The automated aspects of the Registration lifecycle are supported by ARI's Domain Name Registry software. ARI has a development team for maintenance and improvement of the software. The team consist of:

- 1 Development Manager
- 2 Business Analysts
- 6 Developers
- 2 Quality Analysts

Information on these roles is in Resources in our response to Question 31.

These resources sufficiently accommodate the needs of this TLD, and are included in ARI's fees as described in our Financial responses.

## 28. Abuse Prevention and Mitigation

The Applicant has engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q28 - ARI Background & Roles.pdf'.

### 1 INTRODUCTION

The efforts that will be undertaken in this TLD to minimise abusive registrations and other activities that have a negative impact on Internet users are described below. We will be utilising the Anti-Abuse Service of our managed registry service provider, ARI. This service includes the implementation of our comprehensive Anti-Abuse Policy. This policy, developed in consultation with ARI, clearly defines abusive behaviour and identifies particular types of abusive behaviour and the mitigation response to such behaviour.

### 2 OVERVIEW

We have engaged ARI to deliver registry services for this TLD. ARI will, owing to their extensive industry experience and established anti-abuse operations, implement and manage on our behalf various procedures and measures adopted to mitigate the potential for abuse, identify abuse and handle identified abuse. ARI will forward to us all matters requiring determination by the registry

operator which fall beyond the scope of ARI's Anti-Abuse Service. This is described below in the context of the implementation of our Anti-Abuse Policy. Despite utilisation of ARI's Anti-Abuse Service, we are nonetheless cognisant of our responsibility to minimise abusive registrations and other activities that have a negative impact on Internet users in the TLD. In recognition of this responsibility, we will play an instrumental role in overseeing the implementation of the Anti-Abuse Service by ARI. We will also have contractual commitments in the form of SLA's in place to ensure that ARI's delivery of the Anti-Abuse Service is aligned with our strong commitment to minimise abuse in our TLD.

That strong commitment is further demonstrated by our adoption of many of the requirements proposed in the '2011 Proposed Security, Stability and Resiliency Requirements for Financial TLDs' (at

<http://www.icann.org/en/news/correspondence/aba-bits-to-beckstrom-crocker-20dec11-en.pdf>) (the 'BITS Requirements'). We acknowledge that these

requirements were developed by the financial services sector in relation to financial TLDs, but nevertheless believe that their adoption in this TLD (which is not financial-related) results in a more robust approach to combating abuse.

Consistent with Requirement 6 of the BITS Requirements, we will certify to ICANN on an annual basis our compliance with our Registry Agreement.

Please note that the various policies and practices that we have implemented to minimise abusive registrations and other activities that affect the rights of trademark holders are specifically described in our response to Question 29.

### 3 POLICY

In consultation with ARI we have developed a comprehensive Anti-Abuse Policy, which is the main instrument that captures our strategy in relation to abuse in the TLD.

#### 3.1 Definition of Abuse

Abusive behaviour in a TLD may relate to the core domain name-related activities performed by Registrars and registries including, but not limited to:

- The allocation of registered domain names.
- The maintenance of and access to registration information.
- The transfer, deletion, and reallocation of domain names.
- The manner in which the registrant uses the domain name upon creation.

Challenges arise in attempting to define abusive behaviour in the TLD due to its broad scope. Defining abusive behaviour by reference to the stage in the domain name lifecycle in which the behaviour occurs presents difficulty given that a particular type of abuse may occur at various stages of the life cycle. With this in mind, ARI has fully adopted the definition of abuse developed by the Registration Abuse Policies Working Group (Registration Abuse Policies Working Group Final Report 2010, at <http://gnso.icann.org/issues/rap/rap-wg-final-report-29may10-en.pdf>), which does not focus on any particular stage in the domain name life cycle.

Abusive behaviour in a TLD may be defined as an action that:

- causes actual and substantial harm, or is a material predicate of such harm.
- is illegal or illegitimate, or is otherwise considered contrary to the intention and design of the mission/purpose of the TLD.

In applying this definition the following must be noted:

1. The party or parties harmed, and the severity and immediacy of the abuse, should be identified in relation to the specific alleged abuse.
2. The term "harm" is not intended to shield a party from fair market competition.
3. A predicate is a related action or enabler. There must be a clear link between the predicate and the abuse, and justification enough to address the abuse by addressing the predicate (enabling action).

For example, WhoIs data can be used in ways that cause harm to domain name registrants, intellectual property (IP) rights holders and Internet users. Harmful actions may include the generation of spam, the abuse of personal data, IP infringement, loss of reputation or identity theft, loss of data, phishing

and other cybercrime-related exploits, harassment, stalking, or other activity with negative personal or economic consequences. Examples of predicates to these harmful actions are automated email harvesting, domain name registration by proxy/privacy services to aid wrongful activity, support of false or misleading registrant data, and the use of WhoIs data to develop large email lists for commercial purposes. The misuse of WhoIs data is therefore considered abusive because it is contrary to the intention and design of the stated legitimate purpose of WhoIs data.

### 3.2 Aims and Overview of Our Anti-Abuse Policy

Our Anti-Abuse Policy will put registrants on notice of the ways in which we will identify and respond to abuse and serve as a deterrent to those seeking to register and use domain names for abusive purposes. The policy will be made easily accessible on the Abuse page of our registry website which will be accessible and have clear links from the home page along with FAQs and contact information for reporting abuse.

Consistent with Requirements 15 and 16 of the BITS Requirements, our policy:

- Defines abusive behaviour in our TLD.
- Identifies types of actions that constitute abusive behaviour, consistent with our adoption of the RAPWG definition of 'abuse'.
- Classifies abusive behaviours based on the severity and immediacy of the harm caused.
- Identifies how abusive behaviour can be notified to us and the steps that we will take to determine whether the notified behaviour is abusive.
- Identifies the actions that we may take in response to behaviour determined to be abusive.

Our RRA will oblige all Registrars to do the following in relation to the Anti-Abuse Policy:

- comply with the Anti-Abuse Policy; and
- include in their registration agreement with each registrant an obligation for registrants to comply with the Anti-Abuse Policy and each of the following requirements:

'operational standards, policies, procedures, and practices for the TLD established from time to time by the registry operator in a non-arbitrary manner and applicable to all Registrars, including affiliates of the registry operator, and consistent with ICANN's standards, policies, procedures, and practices and the registry operator's Registry Agreement with ICANN. Additional or revised registry operator operational standards, policies, procedures, and practices for the TLD shall be effective upon thirty days notice by the registry operator to the Registrar. If there is a discrepancy between the terms required by this Agreement and the terms of the Registrar's registration agreement, the terms of this Agreement shall supersede those of the Registrar's registration agreement'.

Our RRA will additionally incorporate the following BITS Requirements:

- Requirement 7: Registrars must certify annually to ICANN and us compliance with ICANN's Registrar Accreditation Agreement (RAA) our Registry-Registrar Agreement (RRA).
- Requirement 9: Registrars must provide and maintain valid primary contact information (name, email address, and phone number) on their website.
- Requirement 14: Registrars must notify us immediately regarding any investigation or compliance action, including the nature of the investigation or compliance action by ICANN or any outside party (eg law enforcement, etc.) along with the TLD impacted.
- Requirement 19: Registrars must disclose registration requirements on their website.

We will re-validate our RRAs at least annually, consistent with Requirement 10.

### 3.3 Anti-Abuse Policy

Our Anti-Abuse Policy is as follows:

#### Anti-Abuse Policy

##### Introduction:

The abusive registration and use of domain names in the TLD is not tolerated given that the inherent nature of such abuses creates security and stability

issues for all participants in the Internet environment.

Definition of Abusive Behaviour:

Abusive behaviour is an action that:

- causes actual and substantial harm, or is a material predicate of such harm; or
- is illegal or illegitimate, or is otherwise considered contrary to the intention and design of the mission/purpose of the TLD.

A 'predicate' is an action or enabler of harm.

'Material' means that something is consequential or significant.

Examples of abusive behaviour falling within this definition:

- Spam: the use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of web sites and Internet forums. An example, for purposes of illustration, would be the use of email in denial-of-service attacks.
- Phishing: the use of a fraudulently presented web site to deceive Internet users into divulging sensitive information such as usernames, passwords or financial data.
- Pharming: the redirecting of unknowing users to fraudulent web sites or services, typically through DNS hijacking or poisoning, in order to deceive Internet users into divulging sensitive information such as usernames, passwords or financial data.
- Wilful distribution of malware: the dissemination of software designed to infiltrate or cause damage to devices or to collect confidential data from users without the owner's informed consent.
- Fast Flux hosting: the use of DNS to frequently change the location on the Internet to which the domain name of an Internet host or nameserver resolves in order to disguise the location of web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast flux hosting may only be used with prior permission of the registry operator.
- Botnet command and control: 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.
- Distribution of child pornography: the storage, publication, display and/or dissemination of pornographic materials depicting individuals under the age of majority in the relevant jurisdiction.
- Illegal access to other computers or networks: the illegal accessing of computers, accounts, or networks belonging to another party, or attempt to penetrate security measures of another individual's system (hacking). Also, any activity that might be used as a precursor to an attempted system penetration.

Detection of Abusive Behaviour:

Abusive behaviour in the TLD may be detected in the following ways:

- By us through our on-going monitoring activities and industry participation.
- By third parties (general public, law enforcement, government agencies, industry partners) through notification submitted to the abuse point of contact on our website, or industry alerts.

Reports of abusive behaviour will be notified immediately to the Registrar of record.

Handling of abusive behaviour:

When abusive behaviour is detected in our TLD through notification by a third party, a preliminary assessment will be performed in order to determine whether the notification is legitimately made. Applying the definitions of types of abusive behaviours identified in this policy, we will classify each incidence of legitimately reported abuse into one of two categories based on the probable severity and immediacy of harm to registrants and Internet users. These categories are provided below and are defined by reference to the action that may be taken by us. The examples of types of abusive behaviour falling within each category are illustrative only.

Category 1:

Probable Severity or Immediacy of Harm: Low

Examples of types of abusive behaviour: Spam, Malware

Mitigation steps:

1. Investigate
2. Notify registrant

Category 2:

Probable Severity or Immediacy of Harm: Medium to High

Examples of types of abusive behaviour: Fast Flux Hosting, Phishing, Illegal Access to other Computers or Networks, Pharming, Botnet command and control

Mitigation steps:

1. Suspend domain name
2. Investigate
3. Restore or terminate domain name

In the event that we receive specific instructions regarding a domain name from a law enforcement agency, government or quasi-governmental agency utilising the expedited process for such agencies, our mitigation steps will be in accordance with those instructions provided that they do not result in the contravention of applicable law. In addition, we will take all reasonable efforts to notify law enforcement agencies of abusive behaviour in our TLD which we believe may constitute evidence of a commission of a crime, eg distribution of child pornography.

Note that these expected actions are intended to provide a guide to our response to abusive behaviour rather than any guarantee that a particular action will be taken.

The identification of abusive behaviour in the TLD, as defined above, shall give us the right, but not the obligation, to take such actions in accordance with the following text in the RRA, which provides that the registry operator: '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, or instruct Registrars to take such an action as we deem necessary in our discretion to;

1. protect the integrity and stability of the registry;
2. comply with any applicable laws, government rules or requirements, requests of law enforcement, or dispute resolution process;
3. avoid any liability, civil or criminal, on the part of the registry operator, as well as its affiliates, subsidiaries, officers, directors, and employees, per the terms of the registration agreement; and
4. correct mistakes made by the registry operator or any Registrar in connection with a domain name registration.

We reserve the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

We also reserve the right to deny registration of a domain name to a registrant who has repeatedly engaged in abusive behaviour in our TLD or any other TLD. Registrars only and not Resellers may offer proxy registration services to private individuals using the domain name for non-commercial purposes. We may amend or otherwise modify this policy to keep abreast of changes in consensus policy or new and emerging types of abusive behaviour in the Internet.

Registrar's failure to comply with this Anti-Abuse Policy shall constitute a material breach of the RRA, and shall give rise to the rights and remedies available to us under the RRA.

#### 4 ABUSE PREVENTION AND MITIGATION

This section describes the implementation of our abuse related processes regarding:

- Building awareness of the Anti-Abuse Policy.
- Mitigating the potential for abusive behaviour.
- Identifying abusive behaviour.
- Handling abusive behaviour.

##### 4.1. Awareness of Policy

The Anti-Abuse Policy will be published on the Abuse page of our registry website, which will be accessible and have clear links from the home page. In addition, the URL to the Abuse page will be included in all email correspondence to the registrant, thereby placing all registrants on notice of

the applicability of the Anti-Abuse Policy to all domain names registered in our TLD. The Abuse page will, consistent with Requirement 8 of the BITS Requirements, provide registry contact information (name, email address, and phone number) to enable the public to communicate with us about TLD policies. The Abuse page will emphasise and evidence our commitment to combating abusive registrations by clearly identifying what our policy on abuse is and what effect our implementation of the policy may have on registrants. We anticipate that this clear message, which communicates our commitment to combating abusive registrations, will serve to minimise abusive registrations in our TLD.

#### 4.2 Pre-emptive - Mitigating of the Potential for Abuse

The following practices and procedures will be adopted to mitigate the potential for abusive behaviour in our TLD.

##### 4.2.1 ICANN Prescribed Measures

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

- DNSSEC deployment, which reduces the opportunity for pharming and other man-in-the-middle attacks. We will encourage Registrars and Internet Service Providers to deploy DNSSEC capable resolvers in addition to encouraging DNS hosting providers to deploy DNSSEC in an easy-to-use manner in order to facilitate deployment by registrants. DNSSEC deployment is further discussed in the context of our response to Question 43.
- Prohibition on Wild Carding as required by section 2.2 of Specification 6 of the Registry Agreement.
- Removal of Orphan Glue records (discussed below in '4.2.8 Orphan Glue Record Management').

##### 4.2.2 Increasing Registrant Security Awareness

In accordance with our commitment to operating a secure and reliable TLD, we will attempt to improve registrant awareness of the threats of domain name hijacking, registrant impersonation and fraud, and emphasise the need for and responsibility of registrants to keep registration (including WhoIs) information accurate. Awareness will be raised by:

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

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

##### 4.2.3 Mitigating the Potential for Abusive Registrations that Affect the Legal Rights of Others

Many of the examples of abusive behaviour identified in our Anti-Abuse Policy may affect the rights of trademark holders. While our Anti-Abuse Policy addresses abusive behaviour in a general sense, we have additionally developed specific policies and procedures to combat behaviours that affect the rights of trademark holders at start-up and on an ongoing basis. These include the implementation of a trademark claims service and a sunrise registration service at start-up and implementation of the UDRP, URS and PDDRP on an ongoing basis. The implementation of these policies and procedures serves to mitigate the potential for abuse in the TLD by ensuring that domain names are allocated to those who hold a corresponding trademark.

These policies and procedures are described in detail in our response to Question 29.

#### 4.2.4 Safeguards Against Allowing for Unqualified Registrations

The eligibility restrictions for this TLD are outlined in our response to Question 18.

Eligibility restrictions will be implemented contractually through our RRA, which will require Registrars to include the following in their Registration Agreements:

- Registrant warrants that it satisfies eligibility requirements.

Where applicable, eligibility restrictions will be enforced through the adoption of the Charter Eligibility Dispute Resolution Policy or a similar policy, and Registrars will be obliged to require in their registration agreements that registrants agree to be bound by such policy and acknowledge that a registration may be cancelled in the event that a challenge against it under such policy is successful.

Providing an administrative process for enforcing eligibility criteria and taking action when notified of eligibility violations mitigates the potential for abuse. This is achieved through the risk of cancellation in the event that it is determined in a challenge procedure that eligibility criteria are not satisfied.

#### 4.2.5 Registrant Disqualification

As specified in our Anti-Abuse Policy, we reserve the right to deny registration of a domain name to a registrant who has repeatedly engaged in abusive behaviour in our TLD or any other TLD.

Registrants, their agents or affiliates found through the application of our Anti-Abuse Policy to have repeatedly engaged in abusive registration will be disqualified from maintaining any registrations or making future registrations. This will be triggered when our records indicate that a registrant has had action taken against it an unusual number of times through the application of our Anti-Abuse Policy. Registrant disqualification provides an additional disincentive for qualified registrants to maintain abusive registrations in that it puts at risk even otherwise non-abusive registrations, through the possible loss of all registrations.

In addition, nameservers that are found to be associated only with fraudulent registrations will be added to a local blacklist and any existing or new registration that uses such fraudulent NS record will be investigated. The disqualification of 'bad actors' and the creation of blacklists mitigates the potential for abuse by preventing individuals known to partake in such behaviour from registering domain names.

#### 4.2.6 Restrictions on Proxy Registration Services

Whilst it is understood that implementing measures to promote WhoIs accuracy is necessary to ensure that the registrant may be tracked down, it is recognised that some registrants may wish to utilise a proxy registration service to protect their privacy. In the event that Registrars elect to offer such services, the following conditions apply:

- Proxy registration services may only be offered by Registrars and NOT resellers.

- Registrars must ensure that the actual WhoIs data is obtained from the registrant and must maintain accurate records of such data.

- Registrars must provide Law Enforcement Agencies (LEA) with the actual WhoIs data upon receipt of a verified request.

- Proxy registration services may only be made available to private individuals using the domain name for non-commercial purposes.

These conditions will be implemented contractually by inclusion of corresponding clauses in the RRA as well as being published on the Abuse page of our registry website. Individuals and organisations will be encouraged through our Abuse page to report any domain names they believe violate the above restrictions, following which appropriate action may be taken by us. Publication of these conditions on the Abuse page of our registry website ensures that registrants are aware that despite utilisation of a proxy registration service, actual WhoIs information will be provided to LEA upon request in order to hold registrants liable for all actions in relation to their domain name. The certainty that WhoIs information relating to domain names which draw the attention of LEA will be disclosed results in the TLD



being less attractive to those seeking to register domain names for abusive purposes, thus mitigating the potential for abuse in the TLD.

#### 4.2.7 Registry Lock

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

Upon receipt of a list of domain names to be placed on registry lock by an authorised representative from a Registrar, ARI will:

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

#### 4.2.8 Orphan Glue Record Management

The ARI registry SRS database does not allow orphan records. Glue records are removed when the delegation point NS record is removed. Other domains that need the glue record for correct DNS operation may become unreachable or less reachable depending on their overall DNS service architecture. It is the registrant's responsibility to ensure that their domain name does not rely on a glue record that has been removed and that it is delegated to a valid nameserver. The removal of glue records upon removal of the delegation point NS record mitigates the potential for use of orphan glue records in an abusive manner.

#### 4.2.9 Promoting WhoIs Accuracy

Inaccurate WhoIs information significantly hampers the ability to enforce policies in relation to abuse in the TLD by allowing the registrant to remain anonymous. In addition, LEAs rely on the integrity and accuracy of WhoIs information in their investigative processes to identify and locate wrongdoers. In recognition of this, we will implement a range of measures to promote the accuracy of WhoIs information in our TLD including:

- Random monthly audits: registrants of randomly selected domain names are contacted by telephone using the provided WhoIs information by a member of the ARI Abuse and Compliance Team in order to verify all WhoIs information. Where the registrant is not contactable by telephone, alternative contact details (email, postal address) will be used to contact the registrant, who must then provide a contact number that is verified by the member of the ARI Policy Compliance team. In the event that the registrant is not able to be contacted by any of the methods provided in WhoIs, the domain name will be cancelled following five contact attempts or one month after the initial contact attempt (based on the premise that a failure to respond is indicative of inaccurate WhoIs information and is grounds for terminating the registration agreement).
- Semi-annual audits: to identify incomplete WhoIs information. Registrants will be contacted using provided WhoIs information and requested to provide missing information. In the event that the registrant fails to provide missing information as requested, the domain name will be cancelled following five contact attempts or one month after the initial contact attempt.
- Email reminders: to update WhoIs information to be sent to registrants every

6 months.

- Reporting system: a web-based submission service for reporting WhoIs accuracy issues available on the Abuse page of our registry website.

- Analysis of registry data: to identify patterns and correlations indicative of inaccurate WhoIs (eg repetitive use of fraudulent details).

Registrants will continually be made aware, through the registry website and email reminders, of their responsibility to provide and maintain accurate WhoIs information and the ramifications of a failure to do so or respond to requests to do so, including termination of the Registration Agreement.

The measures to promote WhoIs accuracy described above strike a balance between the need to maintain the integrity of the WhoIs service, which facilitates the identification of those taking part in illegal or fraudulent behaviour, and the operating practices of the registry operator and Registrars, which aim to offer domain names to registrants in an efficient and timely manner.

Awareness by registrants that we will actively take steps to maintain the accuracy of WhoIs information mitigates the potential for abuse in the TLD by discouraging abusive behaviour given that registrants may be identified, located and held liable for all actions in relation to their domain name.

#### 4.3 Reactive - Identification

The methods by which abusive behaviour in our TLD may be identified are described below. These include detection by ARI and notification from third parties. These methods serve to merely identify and not determine whether abuse actually exists. Upon identification of abuse, the behaviour will be handled in accordance with '4.4 Abuse Handling'.

Any abusive behaviour identified through one of the methods below will, in accordance with Requirement 13 of the BITS Requirements, be notified immediately to relevant Registrars.

##### 4.3.1 Detection - Analysis of Data

ARI will routinely analyse registry data in order to identify abusive domain names by searching for behaviours typically indicative of abuse. The following are examples of the data variables that will serve as indicators of a suspicious domain name and may trigger further action by the ARI Abuse and Compliance Team:

- Unusual Domain Name Registration Practices: practices such as registering hundreds of domains at a time, registering domains which are unusually long or complex or include an obvious series of numbers tied to a random word (abuse40, abuse50, abuse60) may, when considered as a whole, be indicative of abuse.

- Domains or IP addresses identified as members of a Fast Flux Service Network (FFSN): ARI uses the formula developed by the University of Mannheim and tested by participants of the Fast Flux PDP WG to determine members of this list. IP addresses appearing within identified FFSN domains, as either NS or A records shall be added to this list.

- An Unusual Number of Changes to the NS record: the use of fast-flux techniques to disguise the location of web sites or other Internet services, to avoid detection and mitigation efforts, or to host illegal activities is considered abusive in the TLD. Fast flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or nameserver resolves. As such an unusual number of changes to the NS record may be indicative of the use of fast-flux techniques given that there is little, if any, legitimate need to change the NS record for a domain name more than a few times a month.

- Results of WhoIs audits: The audits conducted to promote WhoIs accuracy described above are not limited to serving that purpose but may also be used to identify abusive behaviour given the strong correlation between inaccurate WhoIs data and abuse.

- Analysis of cross-validation of registrant WhoIs data against WhoIs data known to be fraudulent.

- Analysis of Domain Names belonging to a registrant subject to action under the Anti-Abuse Policy: in cases where action is taken against a registrant through the application of the Anti-Abuse Policy, we will also investigate other domain names by the same registrant (same name, nameserver IP address, email address, postal address etc).

#### 4.3.2 Abuse Reported by Third Parties

Whilst we are confident in our abilities to detect abusive behaviour in the TLD owing to our robust ongoing monitoring activities, we recognise the value of notification from third parties to identify abuse. To this end, we will incorporate notifications from the following third parties in our efforts to identify abusive behaviour:

- Industry partners through ARI's participation in industry forums which facilitate the sharing of information.
- LEA through a single abuse point of contact (our Abuse page on the registry website, as discussed in detail below) and an expedited process (described in detail in '4.4 Abuse Handling') specifically for LEA.
- Members of the general public through a single abuse point of contact (our Abuse page on the registry website).

##### 4.3.2.1 Industry Participation and Information Sharing

ARI is a member of the Registry Internet Safety Group (RISG), whose mission is to facilitate data exchange and promulgate best practices to address Internet identity theft, especially phishing and malware distribution. In addition, ARI coordinates with the Anti-Phishing Working Group (APWG) and other DNS abuse organisations and is subscribed to the NXdomain mailing list. ARI's strong participation in the industry facilitates collaboration with relevant organisations on abuse-related issues and ensures that ARI is responsive to new and emerging domain name abuses.

The information shared as a result of this industry participation will be used to identify domain names registered or used for abusive purposes. Information shared may include a list of registrants known to partake in abusive behaviour in other TLDs. Whilst presence on such lists will not constitute grounds for registrant disqualification, ARI will investigate domain names registered to those listed registrants and take action in accordance with the Anti-Abuse Policy. In addition, information shared regarding practices indicative of abuse will facilitate detection of abuse by our own monitoring activities.

##### 4.3.2.2 Single Abuse Point of Contact on Website

In accordance with section 4.1 of Specification 6 of the Registry Agreement, we will establish a single abuse point of contact (SAPOC) responsible for addressing and providing a timely response to abuse complaints concerning all names registered in the TLD through all Registrars of record, including those involving a reseller. Complaints may be received from members of the general public, other registries, Registrars, LEA, government and quasi-governmental agencies and recognised members of the anti-abuse community.

The SAPOC's accurate contact details (email and mailing address as well as a primary contact for handling inquiries related to abuse in the TLD) will be provided to ICANN and published on the Abuse page of our registry website, which will also include:

- All public facing policies in relation to the TLD, including the Anti-Abuse Policy.
- A web-based submission service for reporting inaccuracies in WhoIs information.
- Registrant Best Practices.
- Conditions that apply to proxy registration services and direction to the SAPOC to report domain names that violate the conditions.

As such, the SAPOC may receive complaints regarding a range of matters including but not limited to:

- Violations of the Anti-Abuse Policy.
- Inaccurate WhoIs information.
- Violation of the restriction of proxy registration services to individuals.

The SAPOC will be the primary method by which we will receive notification of abusive behaviour from third parties. It must be emphasised that the SAPOC will be the initial point of contact following which other processes will be triggered depending on the identity of the reporting organisation. Accordingly, separate processes for identifying abuse exist for reports by LEA/government and quasi-governmental agencies and members of the general public. These processes will be described in turn below.

#### 4.3.2.2.1 Notification by LEA of Abuse

We recognise that LEA, governmental and quasi-governmental agencies may be privy to information beyond the reach of others which may prove critical in the identification of abusive behaviour in our TLD. As such, we will provide an expedited process which serves as a channel of communication for LEA, government and quasi-governmental agencies to, amongst other things, report illegal conduct in connection with the use of the TLD.

The process will involve prioritisation and prompt investigation of reports identifying abuse from those organisations. The steps in the expedited process are summarised as follows:

1. ARI's Abuse and Compliance Team will identify relevant LEA, government and quasi-governmental agencies who may take part in the expedited process, depending on the mission/purpose and jurisdiction of our TLD. A means of verification will be established with each of the identified agencies in order to verify the identity of a reporting agency utilising the expedited process.
2. We will publish contact details on the Abuse page of the registry website for the SAPOC to be utilised by only those taking part in the expedited process.
3. All calls to this number will be responded to by the ARI Service Desk on a 24/7 basis. All calls will result in the generation of a ticket in ARI's case management system (CMS).
4. The identity of the reporting agency will be identified using the established means of verification (ARI's Security Policy has strict guidelines regarding the verification of external parties over the telephone). If no means of verification has been established, the report will be immediately escalated to the ARI Abuse and Compliance Team. Results of verification will be recorded against the relevant CMS ticket.
6. Upon verification of the reporting agency, the ARI Service Desk will obtain the details necessary to adequately investigate the report of abusive behaviour in the TLD. This information will be recorded against the relevant CMS ticket.
7. Reports from verified agencies may be provided in the Incident Object Description Exchange Format (IODEF) as defined in RFC 5070. Provision of information in the IODEF will improve our ability to resolve complaints by simplifying collaboration and data sharing.
8. Tickets will then be forwarded to the ARI Abuse and Compliance Team to be dealt with in accordance with '4.4 Abuse Handling'.

#### 4.3.2.2.2 Notification by General Public of Abuse

Abusive behaviour in the TLD may also be identified by members of the general public including but not limited to other registries, Registrars or security researchers. The steps in this notification process are summarised as follows:

1. We will publish contact details on the Abuse page of the registry website for the SAPOC (note that these contact details are not the same as those provided for the expedited process).
2. All calls to this number will be responded to by the ARI Service Desk on a 24/7 basis. All calls will result in the generation of a CMS ticket.
3. The details of the report identifying abuse will be documented in the CMS ticket using a standard information gathering template.
4. Tickets will be forwarded to the ARI Abuse and Compliance Team, to be dealt with in accordance with '4.4 Abuse Handling'.

### 4.4 Abuse Handling

Upon being made aware of abuse in the TLD, whether by ongoing monitoring activities or notification from third parties, the ARI Abuse and Compliance Team will perform the following functions:

#### 4.4.1 Preliminary Assessment and Categorisation

Each report of purported abuse will undergo an initial preliminary assessment by the ARI Abuse and Compliance Team to determine the legitimacy of the report. This step may involve simply visiting the offending website and is intended to weed out spurious reports, and will not involve the in-depth investigation needed to make a determination as to whether the reported behaviour is abusive. Where the report is assessed as being legitimate, the type of activity reported

will be classified as one of the types of abusive behaviour as found in the Anti-Abuse Policy by the application of the definitions provided. In order to make this classification, the ARI Abuse and Compliance Team must establish a clear link between the activity reported and the alleged type of abusive behaviour such that addressing the reported activity will address the abusive behaviour.

While we recognise that each incident of abuse represents a unique security threat and should be mitigated accordingly, we also recognise that prompt action justified by objective criteria are key to ensuring that mitigation efforts are effective. With this in mind, we have categorised the actions that we may take in response to various types of abuse by reference to the severity and immediacy of harm. This categorisation will be applied to each validated report of abuse and actions will be taken in accordance with the table below. It must be emphasised that the actions to mitigate the identified type of abuse in the table are merely intended to provide a rough guideline and may vary upon further investigation.

#### Category 1

Probable Severity or Immediacy of Harm: Low

Examples of types of abusive behaviour: Spam, Malware

Mitigation steps:

1. Investigate
2. Notify registrant

#### Category 2

Probable Severity or Immediacy of Harm: Medium to High

Examples of types of abusive behaviour: Fast Flux Hosting, Phishing, Illegal Access to other Computers or Networks, Pharming, Botnet command and control

Mitigation steps:

1. Suspend domain name
2. Investigate
3. Restore or terminate domain name

The mitigation steps for each category will now be described:

#### 4.4.2 Investigation - Category 1

Types of abusive behaviour that fall into this category include those that represent a low severity or immediacy of harm to registrants and Internet users. These generally include behaviours that result in the dissemination of unsolicited information or the publication of illegitimate information. While undesirable, these activities do not generally present such an immediate threat as to justify suspension of the domain name in question. We will contact the registrant to instruct that the breach of the Anti-Abuse Policy be rectified. If the ARI Abuse and Compliance Team's investigation reveals that the severity or immediacy of harm is greater than originally anticipated, the abusive behaviour will be escalated to Category 2 and mitigated in accordance with the applicable steps. These are described below. The assessment made and actions taken will be recorded against the relevant CMS ticket.

#### 4.4.3 Suspension - Category 2

Types of abusive behaviour that fall into this category include those that represent a medium to high severity or immediacy of harm to registrants and Internet users. These generally include behaviours that result in intrusion into other computers' networks and systems or financial gain by fraudulent means. Following notification of the existence of such behaviours, the ARI Abuse and Compliance Team will suspend the domain name pending further investigation to determine whether the domain name should be restored or cancelled. Cancellation will result if, upon further investigation, the behaviour is determined to be one of the types of abuse defined in the Anti-Abuse Policy. Restoration of the domain name will result where further investigation determines that abusive behaviour, as defined by the Anti-Abuse Policy, does not exist. Due to the higher severity or immediacy of harm attributed to types of abusive behaviour in this category, ARI will, in accordance with their contractual commitment to us in the form of SLA's, carry out the mitigation response within 24 hours by either restoring or cancelling the domain name. The assessment made and actions taken will be recorded against the relevant CMS ticket.

Phishing is considered to be a serious violation of the Anti-Abuse Policy owing to its fraudulent exploitation of consumer vulnerabilities for the purposes of financial gain. Given the direct relationship between phishing uptime and extent of harm caused, we recognise the urgency required to execute processes that handle phish domain termination in a timely and cost effective manner. Accordingly, the ARI Abuse and Compliance Team will prioritise all reports of phishing from brand owners, anti-phishing providers or otherwise and carry out the appropriate mitigation response within 12 hours in accordance with the SLA's in place between us and ARI. In addition, since a majority of phish domains are subdomains, we believe it is necessary to ensure that subdomains do not represent an unregulated domain space to which phishers are known to gravitate. Regulation of the subdomain space is achieved by holding the registrant of the parent domain liable for any actions that may occur in relation to subdomains. In reality, this means that where a subdomain determined to be used for phishing is identified, the parent domain may be suspended and possibly cancelled, thus effectively neutralising every subdomain hosted on the parent. In our RRA we will require that Registrars ensure that their Registration Agreements reflect our ability to address phish subdomains in this manner.

#### 4.4.4 Executing LEA Instructions

We understand the importance of our role as a registry operator in addressing consumer vulnerabilities and are cognisant of our obligations to assist LEAs, government and quasi-governmental agencies in the execution of their responsibilities. As such, we will make all reasonable efforts to ensure the integration of these agencies into our processes for the identification and handling of abuse by, amongst other things:

1. Providing expedited channels of communication (discussed above).
2. Notifying LEA of abusive behaviour believed to constitute evidence of a commission of a crime eg distribution of child pornography.
3. Sharing all available information upon request from LEA utilising the expedited process, including results of our investigation.
4. Providing bulk WhoIs information upon request from LEA utilising the expedited process.
5. Acting on instructions from a verified reporting agency.

It is anticipated that these actions will assist agencies in the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties. The relevant agencies are not limited to those enforcing criminal matters but may also include those enforcing civil matters in order to eliminate consumer vulnerabilities.

Upon notification of abusive behaviour by LEA, government or quasi-governmental agencies through the expedited process and verification of the reporting agency, a matter will be immediately communicated to us for our consideration. If we do not instruct ARI to refer the matter to us for our resolution, the CMS ticket will be forwarded to the ARI Abuse and Compliance Team, which will take one of the following actions:

1. The reported behaviour will be subject to preliminary assessment and categorisation as described above. The reported behaviour will then be mitigated based on the results of the categorisation. A report describing the manner in which the notification from the agency was handled will be provided to the agency within 24 hours. This report will be recorded against the relevant CMS ticket.

OR

2. Where specific instructions are received from the reporting agency in the required format, ARI will act in accordance with those instructions provided that they do not result in the contravention of applicable law. ARI will, in accordance with their contractual commitment to us in the form of SLA's, execute such instructions within 12 hours. The following criteria must be satisfied by the reporting agency at this stage:

- a. The request must be made in writing to ARI using a Pro Forma document on the agency's letterhead. The Pro Forma document will be sent to the verified agency upon request.

- b. The Pro Forma document must be delivered to ARI by fax.

c. The Pro Forma document must:

i. Describe in sufficient detail the actions the agency seeks ARI to take.

ii. Provide the domain name/s affected.

iii. Certify that the agency is an 'enforcement body' for the purposes of the Privacy Act 1988 (Cth) or local equivalent.

iv. Certify that the requested actions are required for the investigation and/or enforcement of relevant legislation which must be specified.

v. Certify that the requested actions are necessary for the agency to effectively carry out its functions.

Following prompt execution of the request, a report will be provided to the agency in a timely manner. This report will be recorded against the relevant CMS ticket.

Finally, whilst we do not anticipate the occurrence of a security situation owing to our robust systems and processes deployed to combat abuse, we are aware of the availability of the Expedited Registry Security Request Process to inform ICANN of a present or imminent security situation and to request a contractual waiver for actions we might take or have taken to mitigate or eliminate the security concern.

## 5 RESOURCES

This function will be performed by ARI. Abuse services are supported by the following departments:

- Abuse and Compliance Team (6 staff)
- Development Team (11 staff)
- Service Desk (14 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q28 - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system. Based on past experience ARI estimates that the existing staff is adequate to support a registry system that supports in excess of 50M domains. Since this TLD projects 150000 domains, 0,3% of these resources are allocated to this TLD. See attachment 'Q28 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required.

ARI's Anti-Abuse Service serves to prevent and mitigate abusive behaviour in the TLD as well as activities that may infringe trademarks. These responsibilities will be undertaken by three teams. ARI's Development Team will be responsible for developing the technical platforms and meeting technical requirements needed to implement the procedures and measures adopted to mitigate the potential for abuse, identify abuse and handle identified abuse. ARI's Abuse and Compliance Team will be responsible for the ongoing implementation of measures to minimise abusive registrations and other activities that have a negative impact on Internet users. ARI's Service Desk will be responsible for responding to reports of abuse received through the abuse point of contact on the registry's website and logging these in a ticket in ARI's case management system.

The responsibilities of these teams relevant to the initial implementation and ongoing maintenance of our measures to minimise abusive registrations and other activities that affect the rights of trademark holders are described in our response to Question 29.

All of the responsibilities undertaken by ARI's Development Team, Abuse and

Compliance Team, and Service Desk are inclusive in ARI's Managed TLD Registry services fee, which is accounted for as an outsourcing cost in our response to Question 47. The resources needs of these teams have been determined by applying the conservative growth projections for our TLD (which are identified in our response to Question 48) to the team's responsibilities at start-up and on an ongoing basis.

#### 5.1 ARI Development Team

All tools and systems needed to support the initial and ongoing implementation of measures adopted to mitigate the potential for abuse, identify abuse and handle identified abuse will be developed and maintained by ARI. ARI has a software development department dedicated to this purpose which will ensure that the tools are fit for purpose and adjusted as requirements change.

ARI's Development Team participate actively in the industry; this facilitates collaboration with relevant organisations on abuse related issues and ensures that the ARI Development Team is responsive to new and emerging domain name abuses and the tools and systems required to be built to address these abuses.

This team consists of:

- 1 Development Manager
- 2 Business Analysts
- 6 Developers
- 2 Quality Analysts

#### 5.2 ARI Abuse and Compliance Team

ARI's Abuse and Compliance Team will be staffed by six full-time equivalent positions. These roles will entail the following:

**Policy Compliance Officers:** A principal responsibility of the Policy Compliance Officers will be handling notifications of abuse through the SAPOC. This will involve managing the expedited process, identifying and categorising suspected abuse according to our Anti-Abuse Policy, and carrying out the appropriate mitigation response for all categorised abuses. When abuse is identified, Policy Compliance Officers will investigate other domain names held by a registrant whose domain name is subject to a mitigation response. They will maintain a list of and disqualify registrants found to have repeatedly engaged in abusive behaviour. They will also be responsible for analysing registry data in search of behaviours indicative of abuse, reviewing industry lists in search of data that may identify abuse in the TLD.

Another key responsibility of Policy Compliance Officers will be implementing measures to promote WhoIs accuracy (including managing and addressing all reports of inaccurate WhoIs information received from the web submission service) and verifying the physical address provided by a registrant against various databases for format and content requirements for the region.

Policy Compliance Officers will act on the instructions of verified LEA and Dispute Resolution Providers and participate in ICANN and industry groups involved in the promulgation of policies and best practices to address abusive behaviour. They will escalate complaints and issues to the Legal Manager when necessary and communicate with all relevant stakeholders (Registrars, registrants, LEA, general public) as needed in fulfilling these responsibilities. This role will be provided on a 24/7 basis, supported outside of ordinary business hours by ARI's Service Desk.

Policy Compliance Officers will be required to have the following skills/qualifications: customer service/fault handling experience, comprehensive knowledge of abusive behaviour in a TLD and related policies, Internet industry knowledge, relevant post-secondary qualification, excellent communication and professional skills, accurate data entry skills, high-level problem solving skills, and high-level computer skills.

**Legal Manager:** The Legal Manager will be responsible for handling all potential disputes arising in connection with the implementation of ARI's Anti-Abuse service and related policies. This will involve assessing escalated complaints and issues, liaising with Legal Counsel and the registry operator, resolving disputes and communicating with all relevant stakeholders (Registrars, registrants, LEA, general public) as needed in fulfilling these responsibilities. The Legal Manager will be responsible for forwarding all matters requiring determination by the registry operator which fall outside the



scope of ARI's Anti-Abuse functions. The Legal Manager will be required to have the following skills/qualifications: legal background (in particular, intellectual property/information technology law) or experience with relevant tertiary or post-graduate qualifications, dispute resolution experience, Internet industry experience, strong negotiation skills, excellent communication and professional skills, good computer skills, high-level problem solving skills.

Legal Counsel: A qualified lawyer who will be responsible for all in-house legal advice, including responding to LEA and dealing with abusive behaviour.

The team consists of:

- 4 Policy Compliance Officers
- 1 Legal Manager
- 1 Legal Counsel

### 5.3 ARI Service Desk

ARI's Service Desk will be staffed by 14 full-time equivalent positions. Responsibilities of Service Desk relevant to ARI's Anti-Abuse Service include the following: responding to notifications of abuse through the abuse point of contact and expedited process for LEA, logging notifications as a ticket in ARI's case management system, notifying us of a report received through the expedited process for LEA, government and quasi-governmental agencies, and forwarding tickets to ARI's Abuse and Compliance team for resolution in accordance with the Anti-Abuse Policy.

For more information on the skills and responsibilities of these roles please see the in-depth resources section in response to Question 31.

Based on the projections and the experience of ARI, the resources described here are more than sufficient to accommodate the needs of this TLD.

The use of these resources and the services they enable is included in the fees paid to ARI which are described in the financial responses.

## 29. Rights Protection Mechanisms

The Applicant has engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q29 - ARI Background & Roles.pdf'.

### 1 INTRODUCTION

This response is organised by first addressing the RPMs that we will apply during start-up of our TLD (sunrise and trademark claims service) and then by addressing the RPMs that we will apply on an ongoing basis (URS, UDRP and efforts to avoid infringement trademark infringement including implementation of and compliance with the Trademark PDDRP). Each measure is described and the technological and contractual steps needed for its implementation are identified.

The abusive behaviour primarily targeted by these RPMs is cybersquatting, which is the registration of names constituting trademarks by registrants lacking rights in such trademarks. Cybersquatting is one of the many forms of abuse we will seek to minimise in our TLD. Our approach to combating abusive behaviours other than cybersquatting is described in our response to Question 28. Some overlap between the responses to Questions 28 and Question 29 is inherent because the prevention of cybersquatting can also serve to minimise other abusive behaviours such as phishing and pharming. By implementing the RPMs discussed below we thus aim to minimise not only cybersquatting but also some of the abusive behaviours identified in the response to Question 28. The registration policy of our TLD is described in our response to Question 18. We acknowledge that the legal rights protected by ICANN-mandated RPMs are limited to trademarks. Different RPMs define the scope of protectable trademarks slightly differently; we therefore clearly identify the scope of

protectable marks as respects each RPM.

In addition to the RPMs mandated by the Applicant Guidebook, we have also adopted certain requirements proposed in the '2011 Proposed Security, Stability and Resiliency Requirements for Financial TLDs' (at <http://www.icann.org/en/news/correspondence/aba-bits-to-beckstrom-crocker-20dec11-en.pdf>) (the 'BITS Requirements'). We acknowledge that these requirements were developed by the financial services sector in relation to financial TLDs, but nevertheless believe that their adoption in this TLD (which is not financial-related) results in a more robust approach to combating abuse.

In particular, we will adopt the following:

Requirement 6: we will certify annually to ICANN our compliance with our Registry Agreement.

Requirement 8: we will provide and maintain valid primary contact information (name, email address, and phone number) on our registry website.

Requirement 10: we will re-validate our Registry-Registrar Agreements at least annually.

Requirement 13: we will notify Registrars immediately regarding any RPM investigation or compliance action including the nature of the investigation or compliance action by ICANN or any outside party (eg, law enforcement etc).

We will additionally require through our Registry-Registrar Agreement (RRA) that Registrars comply with the following:

Requirement 7: Registrars must certify annually to ICANN their compliance with ICANN's Registrar Accreditation Agreement (RAA).

Requirement 9: Registrars must provide and maintain valid primary contact information (name, email address, and phone number) on their website.

Requirement 19: Registrars must disclose registration requirements on their website.

## 2 START-UP RPMs

Below we identify our start-up RPM timeline and describe our implementation of:

- A sunrise period.
- The trademark claims service ('TM claims service') during a landrush period.

### 2.1 Start-up RPMs Timeline

The timeline for start-up RPMs in our TLD is as follows:

Day 1: Single sunrise round opens

Day 30: Sunrise round closes

Day 31: Sunrise allocation begins

Day 40: Landrush (including TM claims service) opens

Day 100: Landrush closes

Day 101: Landrush allocation begins

Day 110: General availability begins

### 2.2 Sunrise Registration Service

Our sunrise will provide trademark holders with a 30-day priority period in which to register their trademarks as domain names.

The following stakeholders are involved in implementation of the sunrise registration service:

- TMCH Service Provider/s
- Trademark owner prospective domain name registrants
- Registrars
- Registry operator
- Auction provider

The role played by these stakeholders is described below by reference to:

- A summary of our Sunrise Policy and Sunrise Dispute Resolution Policy (SDRP)
- Our Sunrise Implementation Plan
- Our SDRP Implementation Plan
- Our implementation of sunrise and SDRP through contractual relationships

#### 2.2.1 Sunrise Policy Summary and SDRP Summary

Through our Sunrise Policy we will offer a single, 30-day sunrise round in which trademark holders satisfying (i), (iii) and (iv) of the Sunrise

Eligibility Requirements (SERs) and any general eligibility requirements (as identified in our response to Question 18) proposed in the Applicant Guidebook at Trademark Clearinghouse s6.2.3 will be eligible to apply for a domain name. Our Sunrise Policy will specify that applications satisfying the SERs received by a Registrar within the 30-day sunrise period will be accepted for participation in the sunrise. This will be the first opportunity for registration in our TLD.

Our Sunrise Policy will mandate that the trademarks upon which sunrise applications are based must fall within s7.2 of the Applicant Guidebook (Trademark Clearinghouse) and be supported by an entry in the TMCH. Consistent with Requirement 2 of the BITS Requirements, our Sunrise Policy will describe how we will allocate domain names applied for during the sunrise period, as follows: allocation will start at the end of the 30-day sunrise period. Where only one validated application is received for a domain name, that domain will be allocated to the applicant during the 10-day period between the close of the sunrise applications period and start of the landrush. Where multiple validated applications are received for a domain name, applicants will be invited to participate in an auction to determine the party to which the domain will be allocated. Our Sunrise Policy will specify that by making a sunrise application (or, where relevant, by agreeing to participate in an auction), the applicant agrees to purchase the domain if it is allocated to the applicant. Domain names registered during the sunrise period will have a term of one year from the date of registration.

We will adopt an SDRP to allow any party to raise a challenge on the four grounds identified in the Applicant Guidebook at Trademark Clearinghouse, s6.2.4. The remedy will be cancellation or deletion of a successfully challenged domain. All registrants will be required to submit to proceedings under the SDRP. Our SDRP will specify that SDRP claims may be raised after registration of a sunrise domain and will require that complaints clearly identify the challenger, the challenged domain, and the ground/s on which the complaint is based.

If a TMCH service provider is not able to receive challenges directly as part of its undertaking to 'maintain the SERs, validate and authenticate marks, as applicable, and hear challenges' (Applicant Guidebook at Trademark Clearinghouse, s6.2.5), ARI will receive SDRP challenges and communicate these to the SDRP provider.

## 2.2.2 Implementation

Our Sunrise and SDRP Implementation Plan are set out below followed by a description of the implementation that will take place through contractual relationships.

### 2.2.2.1 Sunrise Implementation Plan

1. Prior to or during our 30-day sunrise period, trademark holders can apply for validation of marks by the TMCH and inclusion of validated marks in the TMCH database.
2. ARI will develop a website and make available on that website our Sunrise Policy and SDRP.
3. A trademark holder warranting satisfaction of the SERs in our Sunrise Policy (as described above) will submit to an ICANN-accredited Registrar its application to register a domain corresponding to its TMCH entry with evidence of the TMCH entry. A non-refundable sunrise application/validation fee will be payable by the applicant to the Registrar on submitting the application.
4. Registrars will be required through our RRA to communicate sunrise application information to ARI. On receipt of this information, ARI will charge the sunrise application/validation fee to the submitting Registrar.
5. ARI will perform standard checks (including IDN validity checks where relevant, reserved and restricted words in accordance with the Registry Agreement, composition requirements, etc) to ensure that the domain being applied for is technically valid; an error message will be returned to the Registrar if the domain fails any of these checks. If the domain passes these checks, ARI will hold the application for allocation.
6. Allocation will commence upon conclusion of the 30-day sunrise period. As an initial step, ARI will compile a list of applied-for names and reserve these

from registration in landrush and general availability.

7. Through an interface with the TMCH, ARI will identify all sunrise applications constituting an 'Identical Match' (as defined in the Applicant Guidebook at Trademark Clearinghouse s6.1.5) with a TMCH entry and provide notice to the holders of those marks of the filing of a corresponding sunrise application.

8. Where a single application exists for a particular domain, between the end of the sunrise application period and start of the landrush period ARI will enable the sponsoring Registrar to CREATE (using EPP or the SRS web interface) the domain and charge the sunrise registration fee to the Registrar, who will collect this fee from the registrant.

9. Where multiple sunrise applications exist for an identical domain name, ARI will compile and communicate to a third-party auction services provider a list of competing applicants, who will be invited to participate in an auction.

10. The auction services provider will facilitate the auction process and upon its completion will notify all participants of the outcome and collect the auction payment from the winning participant.

11. Upon payment of the auction bid, the auction services provider will communicate to ARI the details of the winning auction participant and submit the revenue collected to ARI.

12. ARI will validate the communication from the auction services provider and enable the sponsoring Registrar to CREATE (using EPP or the SRS web interface) the domain name. ARI will charge the sunrise registration fee to the auction winner's Registrar, who will collect this fee from the registrant.

#### 2.2.2.2 SDRP Implementation Plan

1. If a TMCH service provider is not able to directly receive complaints under our SDRP, we will specify in our SDRP the email address to which SDRP filings must be sent. This email address will be monitored by ARI's Abuse and Compliance Team.

2. ARI will develop a process of manual or automatic interface with the TMCH to communicate the SERs and any SDRP challenges received by ARI. This interface will also enable the TMCH Service Provider to notify ARI of successful SDRP challenges.

3. Upon notification from a TMCH service provider of a successful SDRP challenge, ARI will cancel or delete the successfully challenged domain.

#### 2.2.2.3 Implementation through Contractual Relationships

The following features of the Sunrise and SDRP implementation plan described above will be executed by inclusion of corresponding clauses in our RRA, which will require inclusion in Registrars' Registration Agreements:

- By making a sunrise application (or, where relevant, by agreeing to participate in an auction), applicant agrees to purchase the domain name if that name is allocated to the applicant.
- The sunrise application fee is non-refundable.
- All sunrise applicants must submit to proceedings under the SDRP.

#### 2.3 TM Claims Service During Landrush

Ten days after the day that sunrise allocations begin, a 60-day landrush period will commence during which we will offer the TM claims service. This is a service whereby prospective domain name registrants receive notice of existing trademark rights matching their applied-for domain and trademark owners receive notice of domain name registrations matching their trademark. In accordance with the Applicant Guidebook, our TM claims service will be supported exclusively by the TMCH and will recognize and honour all word marks falling within the Applicant Guidebook at Trademark Clearinghouse s7.1.

The following stakeholders are involved in implementation of the TM claims service:

- TMCH Service Provider/s
- Trademark owners
- Landrush domain name applicants
- Landrush domain name registrants
- Registrars
- Registry operator

The role played by these stakeholders is described below by reference to:

- Our Landrush™ Claims Service Implementation Plan
- Our implementation of Landrush™ Claims Service through contractual relationships

Consistent with Requirement 2 of the BITS Requirements, the Landrush™ Claims Service Implementation Plan identifies how we will allocate domain names applied for during the landrush.

### 2.3.1 Implementation

Our Landrush™ Claims Service Implementation Plan is set out below followed by a description of the implementation that will take place through contractual relationships.

#### 2.3.1.1 Landrush™ Claims Service Implementation Plan

1. Prior to or during our 60-day landrush period trademark holders can apply for validation of their marks by the TMCH and inclusion of validated marks in the TMCH database. This will enable provision of notice to landrush applicants of entries in the TMCH and provision of notice to trademark holders of registrations matching TMCH entries (how and by whom this will be achieved is detailed in subsequent steps of this implementation plan).
2. An applicant warranting compliance with the registration policies in this TLD (as described in our response to Question 18) will make an application to an ICANN-accredited Registrar for a domain name during the 60-day landrush period. A non-refundable landrush application/validation fee will be payable by the applicant to the Registrar on submitting the application.
3. Registrars will be required through our RRA to communicate landrush application information to ARI. On receipt of this information, ARI will charge the landrush application/validation fee to the submitting Registrar.
4. Registrars will be required through our RRA to interface with the TMCH to determine whether an applied-for domain constitutes an 'Identical Match' with a mark in the TMCH. If an 'Identical Match' is identified, the Registrar will provide to the landrush applicant a TM Claims Notice in the form prescribed by the Applicant Guidebook. Following receipt of this notice a landrush applicant must communicate to the Registrar its decision either to proceed with or abandon the application. If the applied-for name does not constitute an 'Identical Match' with a trademark in the TMCH, no TM Claims Notice will be generated.
5. ARI will utilise the manual or automatic interface it establishes for implementation of the SDRP (described above in 'Implementation Plan') to facilitate reporting by the TMCH of attempts to register domains that are an 'Identical Match' with a trademark (within the scope of the Applicant Guidebook at Trademark Clearinghouse s7.1) in the TMCH database.
6. ARI will perform standard checks (including IDN validity checks where relevant, reserved and restricted words in accordance with the Registry Agreement, composition requirements, etc) on all landrush applications (irrespective of whether they have generated a TM Claims Notice) to ensure that the domain being applied for is technically valid and an error message will be returned to the Registrar if the domain fails any of these checks. If the domain passes these checks, ARI will hold the application for allocation.
7. Allocation of landrush applications will commence on conclusion of the 60-day landrush application period. Where a single landrush application exists for a particular domain, between the end of the landrush application period and start of general availability, ARI will enable the sponsoring Registrar to CREATE (using EPP or the SRS web interface) the domain and charge the landrush registration fee to the Registrar, who will collect this fee from the registrant.
8. Where multiple landrush applications exist for an identical domain, ARI will compile and communicate to a third-party auction services provider a list of competing applicants, who will be invited to participate in an auction for the domain name.
9. The auction services provider will facilitate the auction process and on its completion will notify all participants of the outcome and collect payment from the winning participant.
10. Upon payment of the auction bid the auction services provider will

communicate to ARI the details of the winning participant and will submit the revenue collected to ARI.

11. ARI will validate the communication from the auction services provider and enable the auction winner's Registrar to CREATE (using EPP or the SRS web interface) the domain name. ARI will charge the landrush registration fee to the Registrar, who will collect this fee from the registrant.

12. The Registrar will be required through our RRA to interface with the TMCH to promptly notify relevant mark holders of the registration of a domain constituting an 'Identical Match' to their TMCH entry.

13. Ten days after the start of the landrush allocation period, general availability of domain names (at first-come, first-served allocation) will commence.

#### 2.3.1.2 Implementation through Contractual Relationships

The following features of our Landrush™ Claims Service Implementation Plan described above will additionally be executed by the inclusion of corresponding clauses in our RRA:

- Registrars must use the TMCH as required by ICANN and the TMCH Service Provider/s.
- Registrars must not in their provision of the TM Claims Service make use of any trademark information aggregation, notification or validation service other than the TMCH.
- In order to prevent a chilling effect on registration, Registrars must ensure that landrush applicants are not prevented from registering domains considered an 'Identical Match' with a mark in the TMCH.
- Registrars must provide clear notice in the specific form provided by the Applicant Guidebook to the prospective registrant of relevant entries in the TMCH.
- The landrush application fee is non-refundable. Registrars must also include this in their Registration Agreements.

### 3 ONGOING RPMS

Below we describe the way in which we will implement on an ongoing basis the URS and UDRP and address issues related to the Trademark PDDRP. These RPMS serve to mitigate not only cybersquatting but other types of abuse that frequently occur in conjunction with cybersquatting, such as phishing and pharming.

#### 3.1 URS

The URS is a new RPM the implementation of which is mandated in all new gTLDs. The URS is targeted at providing a rapid takedown solution to clear-cut cases of cybersquatting. It is intended to have a deterrent effect and reduce the number of UDRP disputes.

The URS is intended to supplement and not replace the UDRP, and the Applicant Guidebook foreshadows (at URS ss8.6 and 13) the likelihood of URS claimants also commencing UDRP claims. For this reason, we have considered in our URS Implementation Plan the potential interaction between URS stakeholders and UDRP stakeholders.

The following stakeholders are involved in implementation of the URS:

- URS claimants (holders of valid and enforceable trade or service marks)
- Registrants
- Registrars
- Registry operator
- URS provider/s
- URS Examiner

The role played by these stakeholders is described below by reference to:

- Our URS Implementation Plan
- Our implementation of the URS through contractual relationships

Our URS Implementation Plan identifies certain aspects of implementation that are not clearly addressed in the Applicant Guidebook. For example, the Guidebook does not specify how, from an operational perspective, suspension of a domain name will transform to another domain name status (eg the transfer of

a domain following a successful UDRP challenge); we assume that such a status change would only occur upon expiry of the registration, but acknowledge the potential for further development of URS policy to allow for change of status as a result of a subsequent UDRP decision.

In addition to identifying such gaps, our URS Implementation Plan identifies our proposed method of addressing these. Furthermore, understanding that a fundamental aim of the URS is expediency, all of the steps in our Implementation Plan below will be undertaken as soon as practical but without compromising security or accuracy.

### 3.1.1 Implementation

Our URS Implementation Plan is set out below followed by a description of the implementation that will take place through contractual relationships.

#### 3.1.1.1 URS Implementation Plan

1. As an initial step, ARI will notify to each URS provider an email address for all URS-related correspondence. On an ongoing basis, ARI's Abuse and Compliance Team will monitor this address for communications from URS providers, including the Notice of Complaint, Notice of Default, URS Determination, Notice of Appeal and Appeal Panel Findings.
2. ARI will validate correspondence from a URS provider to ensure that it originates from the URS Provider.
3. ARI will within 24 hours of receipt of a URS Notice of Complaint lock the domain name/s the subject of complaint by restricting all changes to the registration data, including transfer and deletion of the domain. The domain will continue to resolve while in this locked status.
4. ARI will immediately notify the URS provider in the manner requested by the URS provider once the domain name/s have been locked.
5. Upon receipt of a favourable URS Determination ARI will lock the domain name the subject of the Determination for the balance of the registration period and redirect the nameservers to an informational web page provided by the URS provider. While a domain name is locked, ARI will continue to display all of the WhoIs information of the original registrant except for the redirection of the nameservers and (subject to future policy development taking into account the transfer of a URS-locked domain name following a successful UDRP challenge) the additional statement that the domain will not be able to be transferred, deleted or modified for the life of the registration.
6. Upon receipt of notification from the URS provider of termination of a URS proceeding ARI will promptly unlock the domain and return full control to the registrant.
7. Where a default has occurred (because a registrant has not submitted an answer to a URS complaint in accordance with the Applicant Guidebook at URS s6.1) and a Determination has been made in favour of the complainant, in the event that ARI receives notice from a URS provider that a Response has been filed in accordance with the Applicant Guidebook at URS s6.4, ARI will as soon as practical restore a domain to resolve to the original IP address while preserving its locked status until a Determination from de novo review is notified to ARI.
8. ARI will ensure that no changes are made to the resolution of a registration the subject of a successful URS Determination until expiry of the registration or the additional registration year unless otherwise instructed by UDRP provider.
9. ARI will make available to successful URS complainants an optional extension of the registration period for one additional year at commercial rates. We understand that this requirement has been based on the provision in the Expired Domain Deletion Policy (3.7.5.7 of the 2009 RAA), under which there is no requirement of notification to the complainant that a name is due to expire. From this we conclude that there is likewise no requirement in the operation of our TLD that ARI notify a successful URS complainant that a name is due to expire.
10. The Applicant Guidebook specifies that renewal must be offered 'at commercial rates' but it does not specify how and to whom payment for renewal should be made. If payment is to be made to a stakeholder other than the registry operator, it is not clear how this will be received by the registry

operator. ARI's Abuse and Compliance Team will be prepared and have the expertise and flexibility necessary to develop the technical and financial interfaces necessary to facilitate the receipt of renewal fees by ARI.

#### 3.1.1.2 Implementation of the URS through Contractual Relationships

The following features of our URS Implementation Plan described above will be executed by inclusion of corresponding clauses in our RRA:

- In the event that a registrant does not submit an answer to a URS complaint in accordance with the Applicant Guidebook at URS s6.1 (default), Registrars must prevent registrants from making changes to the WhoIs information of a registration while it is in default.
- Registrars must prevent changes to a domain it is in locked status to ensure that both the Registrar's systems and registry's systems contain the same information for the locked domain.
- Registrars must not take any action relating to a URS proceeding except as in accordance with a validated communication from ARI or URS provider.

### 3.2 UDRP

The UDRP is applicable to domain name registrations in all new gTLDs. It is available to parties with rights in valid and enforceable trade or service marks and is actionable on proof of all of the following three grounds:

- i. The registrant's domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights.
- ii. The registrant has no rights or legitimate interests in respect of the domain name.
- iii. The registrant's domain name has been registered and is being used in bad faith.

Available remedies are cancellation of a domain or transfer of a domain to a successful UDRP claimant.

The following stakeholders are involved in implementation of the UDRP:

- UDRP claimants
- Registrants
- Registrar
- Registry operator
- UDRP providers

The role played by these stakeholders is described below by reference to:

- Our UDRP Implementation Plan
- Our implementation of the UDRP through contractual relationships

Our UDRP Implementation Plan considers the potential overlap between URS implementation and UDRP implementation because we consider it likely that URS complainants may commence UDRP claims as a second recourse or simultaneously. We note that neither policy prohibits complainants from commencing proceedings simultaneously.

#### 3.2.1 Implementation

Our UDRP Implementation Plan is set out below followed by a description of the implementation that will take place through contractual relationships.

##### 3.2.1.1 UDRP Implementation Plan

Our UDRP Implementation Plan focuses on interaction with Registrars because there is currently no interaction between existing gTLD registry operators and UDRP providers. On this basis we anticipate ARI has two responsibilities to facilitate Registrars' implementation of the UDRP.

1. ARI's Development Team (as described in '4 RESOURCES') will maintain awareness of UDRP requirements and be capable of taking action when required and sufficiently skilled and flexible to respond to any changes to UDRP policy.
2. ARI will provide EPP and the SRS web interface to enable Registrars to perform required UDRP functions in accordance with the Policy on Transfer of Registrations between Registrars.

##### 3.2.1.2 Implementation of the UDRP through Contractual Relationships

The UDRP is applicable to domain name registrations in all new gTLDs by force of a contractual obligation (Registry Agreement Art. 2.9) on registry operators to use only ICANN-accredited Registrars, who in turn are contractually required



(RAA, 21 May 2009, at s3.8) to incorporate the UDRP in their Registration Agreements.

### 3.3 Preventing Trademark Infringement in Operating the Registry

We take seriously our responsibilities in running a registry and understand that while offering a sunrise registration service and TM Claims Service during start-up of our TLD and the URS and UDRP on an ongoing basis serves to minimise abuse, this does not necessarily serve to minimise trademark infringement in our operation of the TLD. This responsibility is now clearly placed on registry operators through the new Trademark PDDRP, which targets infringement arising from the registry operator's manner of operation or use of its TLD.

While we will as required by the Registry Agreement agree to participate in all Trademark PDDRP procedures and be bound by resulting determinations, we will also have in place procedures to identify and address potential conflicts before they escalate to the stage of a Trademark PDDRP claim.

The following stakeholders are involved in our implementation of measures to prevent trademark infringement in operation of the TLD:

- Trademark holders
- Registry operator
- Trademark PDDRP provider/s

The role played by these stakeholders is described below by reference to:

- Our Trademark PDDRP Implementation Plan
- Our implementation of our Trademark PDDRP through contractual relationships

#### 3.3.1 Implementation

Our Trademark PDDRP Implementation Plan is set out below followed by a description of the implementation that will take place through contractual relationships.

##### 3.3.1.1 Trademark PDDRP Implementation Plan

1. ARI will notify to the Trademark PDDRP provider/s contact details for all communications regarding the Trademark PDDRP.

2. As described in our response to Question 28, ARI will publish our Anti-Abuse Policy on a website dedicated to abuse handling in our TLD. Consistent with Requirement 8 of the BITS Requirements, this website will include information necessary to enable trademark holders to raise concerns regarding infringement of their trademarks and resultant harm caused by our operation or use of our TLD.

3. Using the single abuse point of contact (SAPOC) discussed in our response to Question 28, a complainant can notify ARI's Service Desk of its belief that one or more of its marks have been infringed and harm caused by our operation or use of our TLD. The complainant will be required to provide the following information:

- Name of the complainant
- Contact details
- Trademark name
- Jurisdiction
- Registration date
- Registration number
- Nature of entitlement to trademark
- Explanation of why complainant believes that its mark has been infringed and harm caused by our operation or use of the TLD

4. ARI's Service Desk will receive complaints submitted through the SAPOC on a 24/7 basis and generate a ticket in ARI's case management system (CMS). The details of the complaint (which will at a minimum include the information above) will be documented using a standard information gathering template and forwarded to ARI's Abuse and Compliance Team.

5. Upon receipt of a complaint, the Abuse and Compliance Team will conduct a preliminary assessment to ensure that a complaint is not spurious. If it is determined that a complaint is not spurious, a member of the team will use the contact details provided in the complaint to acknowledge receipt of the complaint and commence investigation of the subject matter of the complaint and good faith negotiations with the complainant in accordance with the Applicant Guidebook at Trademark PDDRP s7.2.3(d). The results of this preliminary

assessment and subsequent actions taken will be recorded against the CMS ticket.

6. On an ongoing basis, ARI's Abuse and Compliance Team will monitor the email address notified to the Trademark PDDRP provider/s for all communications from the Trademark PDDRP provider, including threshold determination, Trademark PDDRP complaint, complainant's reply, notice of default, expert panel determination, notice of appeal and determination of an appeal panel.

7. In the event that a complaint cannot be resolved and a Trademark PDDRP claim is made, ARI's Abuse and Compliance Team will do the following:

- File a response to the complaint in accordance with the Applicant Guidebook at Trademark PDDRP s10 thus avoiding (whenever possible) default.
- Where appropriate, undertake discovery in compliance with the Applicant Guidebook at Trademark PDDRP s15, attend hearings raised under s16 if required, and gather evidence in compliance with ss20.5 and 20.6.

8. ARI's Abuse and Compliance Team will upon notification of an Expert Panel finding in favour of the Claimant (Applicant Guidebook at Trademark PDDRP s14.3), reimburse the Claimant.

9. ARI will implement any remedial measures recommended by the expert panel pursuant to the Applicant Guidebook at Trademark PDDRP s18.3.1 and take all steps necessary to cure violations found by the expert panel (s18.3.2) and notified by ICANN (s21.3).

### 3.3.2 Implementation of Trademark PDDRP through Contractual Relationships

All new gTLD registry operators are bound to comply with the Trademark PDDRP by Specification 7, cl 2 of the Registry Agreement. In accordance with Requirement 6 of the BITS Requirements, we will certify annually to ICANN our compliance with our Registry Agreement.

## 4 RESOURCES

ARI's abuse services are supported by the following departments:

- Abuse and Compliance Team (6 staff)
- Development Team (11 staff)
- Service Desk (14 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q29 - ARI Background & Roles.pdf'. This attachment describes the functions of these teams and the exact number and nature of staff within.

The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system. Based on past experience ARI estimates that the existing staff is adequate to support a registry system that supports in excess of 50M domains. Since this TLD projects 150000 domains, 0,3% of these resources are allocated to this TLD. See attachment 'Q29 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required.

The measures described in the context of the responses to Question 28 and Question 29 - which serve to prevent and mitigate abusive behaviour in the TLD as well as activities that may infringe trademarks - will be implemented and managed by ARI on our behalf. These responsibilities will be undertaken by two teams. ARI's Development Team will be responsible for developing the technical platforms and meeting technical requirements needed to implement the RPMs discussed above. ARI's Abuse and Compliance Team will be responsible for the ongoing operations of measures to minimise abusive registrations and other activities that affect trademark rights recognised through RPMs. ARI's Service Desk will be responsible for responding to reports of trademark infringement received through the abuse point of contact on the Registry's website and logging these in a ticket in ARI's case management system.

The responsibilities of these teams relevant to the initial implementation and ongoing maintenance for our measures to minimise the potential in our TLD for abuse not specifically affecting trademark rights are described in our response to Question 28.

All of the responsibilities undertaken by ARI's Development Team, Abuse and Compliance Team, and Service Desk are inclusive in ARI's Managed TLD Registry services fee, which is accounted for as an outsourcing cost in our response to Question 47. The resource needs of these teams have been determined by applying the conservative growth projections for our TLD (as identified in our response to Question 48) to the teams' responsibilities at startup and on an ongoing basis.

#### 4.1 ARI Development Team

All tools and systems used for the transmission and receipt of information related to RPMs will be developed and maintained by ARI. ARI has a Development Team dedicated to this purpose which will ensure that the tools are fit for purpose and adjusted as requirements change.

ARI will ensure that systems and tools will be compliant with the appropriate processes for dealing with Registrars, the TMCH, URS and Trademark PDDRP providers as these processes are defined. ARI has been and will remain active in the formulating of these processes, using its resources to remain current with the approved measures for exchange of any material relevant to RPMs, whether during sunrise, landrush or on an ongoing basis. This team consists of:

- 1 Development Manager
- 2 Business Analysts
- 6 Developers
- 2 Quality Analysts

#### 4.2 ARI Abuse and Compliance Team

ARI's Abuse and Compliance Team will be staffed by five full-time equivalent positions:

- 4 Policy Compliance Officers
- 1 Legal Manager

Policy Compliance Officers will be responsible for managing sunrise and landrush applications, supporting the SDRP, TM Claims Service, URS, UDRP and Trademark PDDRP, managing communications with the TMCH, receiving, assessing and managing trademark infringement complaints received through the single abuse point of contact, escalating complaints and issues to the Legal Manager when necessary and communicating with all relevant stakeholders (Registrars, registrants, trademark holders, general public) as needed in fulfilling these responsibilities. This role will be provided on a 24/7 basis supported outside of ordinary business hours by ARI's Service Desk. Policy Compliance Officers will be required to have the following skills/qualifications: customer service/fault handling experience, complete knowledge of all RPMs offered by the TLD and related policies, Internet industry knowledge, relevant post-secondary qualification, excellent communication and professional skills, accurate data entry skills, high-level problem solving skills, and high-level computer skills.

The Legal Manager will be responsible for handling all potential disputes arising in connection with RPMs and related policies. This will involve assessing complaints and issues, liaising with legal counsel and management, resolving disputes and communicating with all relevant stakeholders (Registrars, registrants, trademark holders, general public) as needed in fulfilling these responsibilities. The Legal Manager will be required to have the following skills/qualifications: legal background (in particular, intellectual property/information technology law) or experience with relevant tertiary or post-graduate qualifications, dispute resolution experience, Internet industry experience, excellent communication, negotiation, problem solving and professional skills and good computer skills.

For more information on the skills and responsibilities of these roles, please see the in-depth resources section in response to Question 31.

Based on the projections and the experience of ARI, the resources described here are more than sufficient to accommodate the needs of this TLD.

The use of these resources and the services they enable is included in the fees

paid to ARI, which are described in response to Question 47.

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

The Applicant has engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q30a - ARI Background & Roles.pdf'. This response describes Security as implemented by ARI under direction from the registry operator taking into account any specific needs for this TLD.

#### 1 SECURITY POLICY SUMMARY

ARI operates an ISO27001 compliant Information Security Management System (ISMS) for Domain Name Registry Operations; see attachment 'Q30a - SAI Global Certificate of Compliance.pdf'. The ISMS is an organisation-wide system encompassing all levels of Information Security policy, procedure, standards, and records. Full details of all the policies and procedures included in the ISMS are included in the attachment to Question 30b.

##### 1.1 The ISMS

ARI's ISMS's governing policy:

- Defines the scope of operations to be managed (Domain Name Registry Operations).
- Designates the responsible parties (COO, CTO and Information Security Officer) for governance, Production Support Group for implementation and maintenance, and other departments for supporting services.
- Requires a complete Risk Assessment (a developed Security Threat Profile for the Service - in this case registry services for the TLD - and a Risk Analysis tracing threats and vulnerabilities through to Risks) and Risk Treatment Plan (each major risk in the Risk Assessment references the Statement of Applicability indicating controls to be implemented, responsible parties, and the effectiveness metrics for each).
- Includes a series of major sub policies governing security, which include but are not limited to:
  - ICT acceptable use policy and physical security policies.
  - PSG Security Policy which outlines the registry operations policies, the management of end-user devices, classification of networks and servers according to the classification of information they contain, networking, server & database configuration and maintenance guidelines, vulnerability and patch management, data integrity controls, access management, penetration testing, third party management, logging and monitoring, and cryptography.
- Requires ongoing review:
  - Of risks, threats, the Risk Treatment Plan, client requirements and commitments, process and policy compliance, process and policy effectiveness, user etc.
  - Regular internal and external penetration testing & vulnerability scanning.
  - Ad-hoc review raised during normal operations, common sources being change management processes, scheduled maintenance or project debriefs, and security incidents.
  - Yearly review cycle which includes both internal and external audits, including external surveillance audits for compliance.
  - Additional yearly security controls assessment reviews, which include analysis of the security control implementations themselves (rather than compliance with any particular standard).
  - At 24 month intervals, external penetration testing of selected production services.
  - periodic ISO reaccreditation

ARI's ISMS encompasses the following ARI standards:

- Configuration standards for operating systems, networking devices and databases based on several key publications, including those released by NIST (eg SP800-123, SP800-44v2, SP-800-40, SP800-41) and the NSA, staff testing and experience, and vendor supplied standards.
- Security Incident Classification, which identifies the various classifications of security incidents and events to ensure that events that qualify as security incidents.
- Information Classification and Handling which specifies the information classification scheme and the specific requirements of handling, labelling, management and destruction for each level of classification.

## 1.2 SECURITY PROCESSES

Processes are used to implement the policies. These include, but are not limited to:

### 1.2.1 Change Management

This includes change management and its sub-processes for access management, software deployment, release of small changes and scheduled maintenance. This process includes:

- The classification of changes and the flow into sub processes by classification.
- The release and deployment process for change control into production environments, outlining peer review, testing steps, approval points, checklist sets, staging requirements and communication requirements.
- The software release and deployment process with its specific testing and staged rollout requirements.
- The scheduled maintenance process and its various review points.

### 1.2.2 Incident Management

This includes incident management process and its sub-process for unplanned outages. These outline:

- How incidents are managed through escalation points, recording requirements, communication requirements etc.
- The unplanned outage procedure which applies directly to situations where the registry itself or other critical services are unexpectedly offline.

### 1.2.3 Problem Management

The goal of problem management is to drive long term resolution of underlying causes of incidents. This process centres on finding and resolving the root causes of incidents. It defines escalation points to third parties or other ARI departments such as Development, as well as verification of the solution prior to problem closure.

### 1.2.4 Security Incident Management

This process deals with the specific handling of security incidents. It outlines the requirements and decision points for managing security incidents. Decision points, escalation points to senior management and authorities are defined, along with evidence-gathering requirements, classification of incidents and incident logging.

### 1.2.5 Access Management

This process handles all access changes to systems. HR must authorize new users, and access changes are authorized by departmental managers and approved by the Information Security Officer.

When staff leave or significantly change roles, a separation process is followed which ensures all access that may have been granted during their employment (not just their initially granted access) is checked and where appropriate, revoked.

Finally, quarterly review of all access is undertaken by the ISO, reviewing and approving or rejecting (with an action ticket) as appropriate.

## 2 ARI's SECURITY INFRASTRUCTURE SOLUTIONS

ARI has developed a layered approach to IT security infrastructure. At a high level, some of the layers are as follows:

- DDoS countermeasures are employed outside ARI networks. These include routing traps for DDoS attacks, upstream provider intervention, private peering links and third party filtering services.
- Routing controls at the edge of the network at a minimum ensures that only traffic with valid routing passes into ARI networks.
- Overprovisioning and burstable network capabilities help protect against DoS and DDoS attacks.
- Network firewalls filter any traffic not pre-defined by network engineering staff as valid.
- Application layer firewalls then analyse application level traffic and filter any suspicious traffic. Examples of these would be an attempt at SQL injection, script injection, cross-site scripting, or session hijacking.
- Server firewalls on front-end servers again filter out any traffic that is not strictly defined by systems administrators during configuration as valid traffic.
- Only applications strictly necessary for services are running on the servers.
- These applications are kept up-to-date with the latest security patches, as are all of the security infrastructure components that protect them or that they run on.
- ARI infrastructure is penetration-tested by external tools and contracted security professionals for vulnerabilities to known exploits.
- ARI applications are designed, coded and tested to security standards such as OWASP and penetration-tested for vulnerabilities to common classes of exploits by external tools and contracted security professionals.
- ARI configures SELinux on its production servers. Specific details of this configuration is confidential; essentially any compromised application is extremely limited in what it can do.
- Monitoring is used to detect security incidents at all layers of the security model. Specifically:
  - Network Intrusion Detection systems are employed to monitor ARI networks for suspicious traffic.
  - ARI maintains its own host-based Intrusion Detection system based on tripwire, which has now undergone four years of development. Specific details are confidential, but in summary, the system can detect any unusual activity with respect to configuration, program files, program processes, users, or network traffic.
  - More generic monitoring systems are used as indicators of security incidents. Any behaviour outside the norm across over 1,100 individual application, database, systems, network and environmental checks is investigated.
  - Capacity management components of the monitoring suite are also used to detect and classify security incidents. Some examples are:
    - Network traffic counts, packet counts and specific application query counts.
    - Long term trend data on network traffic vs. specific incident windows.
    - CPU, Storage, Memory and Process monitors on servers.
- A second layer of hardware firewalling separates application and middle tier servers from database servers.
- Applications only have as much access to database information as is required to perform their function.
- Finally, database servers have their own security standards, including server-based firewalls, vulnerability management for operating system and RDBMS software, and encryption of critical data.

### 2.1 Physical Security Infrastructure

ARI maintains a series of physical security infrastructure measures including but not limited to biometric and physical key access control to secured areas and security camera recording, alarm systems and monitoring.

### 3 COMMITMENTS TO REGISTRANTS

We commit to the following:

- Safeguarding the confidentiality, integrity and availability of registrant's

data.

- Compliance with the relevant regulation and legislation with respect to privacy.
- Working with law enforcement where appropriate in response to illegal activity or at the request of law enforcement agencies.
- Maintaining a best practice information security management system that continues to be ISO27001-compliant.
- Validating requests from external parties requesting data or changes to the registry to ensure the identity of these parties and that their request is appropriate. This includes requests from ICANN.
- That access to DNS and contact administrative facilities requires multi-factor authentication by the Registrar on behalf of the registrant.- That Registry data cannot be manipulated in any fashion other than those permitted to authenticated Registrars using the EPP or the SRS web interface. Authenticated Registrars can only access Registry data of domain names sponsored by them.
- A Domain transfer can only be done by utilizing the AUTH CODE provided to the Domain Registrant.
- Those emergency procedures are in place and tested to respond to extraordinary events affecting the integrity, confidentiality or availability of data within the registry.

#### 4 AUGMENTED LEVEL OF SECURITY

This TLD is a generic TLD and as such requires security considerations that are commensurate with its purpose. Our goal with this TLD is to provide registrants with adequate protections against unauthorized changes to their names, without making the registration process too onerous and thus increasing costs.

The following attributes describe the security with respect to the TLD:

- ARI, follows the highest security standards with respect to its Registry Operations. ARI is ISO 27001 certified and has been in the business of providing a Registry backend for 10 years. ARI have confirmed their adherence to all of the security standards as described in this application. As per recommendation 24 this ensures that the technical implementations do not compromise elevated security standards
- Registrant will only be permitted to make changes to their domain name after a authenticating to their Registrar.
- Registrants will only be able to access all interfaces for domain registration and management via HTTPS. A reputed digital certificate vendor will provide the SSL certificate of the secure site.
- Registrar identity will be manually verified before they are accredited within this TLD. This will include verification of corporate identity, identity of individuals involved / mentioned, and verification of contact information
- Registrars will only be permitted to connect with the SRS via EPP after a multi-factor authentication that validates their digital identity. This is described further ahead.
- Registrars will only be permitted to use a certificate signed by ARI to connect with the Registry systems. Self-signed certificates will not be permitted.
- The Registry is DNSSEC enabled and the TLD zone will be DNSSEC enabled. This is described in detail in our response to question 43. The following additional requirements will exist for Registrars who want to get accredited to sell this TLD:
  - Registrars must support DNSSEC capabilities within its control panels.
  - If the Registrar provides Managed DNS services to Registrants within this TLD they must provide the option for DNSSEC. This ensures that DNSSEC is deployed at each zone and subsequent sub-zones at Registry, Registrar and Registrant level as per recommendation 26.
  - Registrar access to all Registry Systems will be via TLS and secured with multi-factor authentication as per recommendation 27. This is described in detail in our responses to Question 24 and Question 25.
  - Registrant access to all Registrar and Registry Systems will be via TLS and secured with multi-factor authentication as per recommendation 28. This is described in detail in our response to Question 25, Question 27 and Question

29.

- All communication between the Registrar or the Registrars systems and the registry system is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57. This includes the following communication:

- Secure websites and control panels provided by the Registrar to the Registrant.
- Ticketing systems provided by the Registrar to the Registrant.
- Web and EPP interfaces provided by ARI to the Registrars.
- Ticketing systems provided by ARI to the Registrar.
- Any communication between the Registrant, Registrar and Registry that is deemed as critical or contains credentials or sensitive information.

Where these requirements put controls on Registrars these will be enforced through the RRA.

## 5 RESOURCES

This function will be performed by ARI. The following resources are allocated to performing the tasks required to deliver the services described:

- Executive Management Team (4 staff)
- Production Support Group (27 staff)

ARI has ten years' experience designing, developing, deploying, securing and operating critical Registry systems, as well as TLD consulting and technology leadership.

As a technology company, ARI's senior management are technology and methodology leaders in their respective fields who ensure the organisation maintains a focus on technical excellence and hiring, training and staff management.

Executive Management is heavily involved in ensuring security standards are met and that continued review and improvement is constantly undertaken. This includes the:

- Chief Operations Officer
- Chief Technology Officer

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q30a - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system. Based on past experience ARI estimates that the existing staff is adequate to support a registry system that supports in excess of 50M domains. Since this TLD projects 150000 domains, 0,3% of these resources are allocated to this TLD. See attachment 'Q30a - Registry Scale Estimates & Resource Allocation.xls' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

The Production Support Group is responsible for the deployment and operation of TLD registries.

The group consists of:

- Production Support Manager (also the ISO)
- Service Desk:
  - 1 Level 1 Support Team Lead
  - 8 Customer Support Representatives (Level 1 support)
  - 1 Level 2 Support Team Lead
  - 4 Registry Specialists (Level 2 support)
- Operations (Level 3 support):
  - 1 Operations Team Lead
  - 2 Systems Administrators



- 2 Database Administrators
- 2 Network Engineers
- Implementation:
  - 1 Project Manager
  - 2 Systems Administrators
  - 1 Database Administrators
  - 1 Network Engineers

ARI employs a rigorous hiring process and screening (Police background checks for technical staff and Australian Federal Government 'Protected' level security clearances for registry operations staff).

© *Internet Corporation For Assigned Names and Numbers.*



## **New gTLD Application Submitted to ICANN by: Vistaprint Limited**

**String: webs**

**Originally Posted: 13 June 2012**

**Application ID: 1-1033-73917**

### **Applicant Information**

#### **1. Full legal name**

Vistaprint Limited

#### **2. Address of the principal place of business**

Contact Information Redacted

#### **3. Phone number**

Contact Information Redacted

#### **4. Fax number**

Contact Information Redacted

## 5. If applicable, website or URL

<http://www.vistaprint.com>

## Primary Contact

### 6(a). Name

Mr. David Barron

### 6(b). Title

Vice President and Senior IP Counsel

### 6(c). Address

### 6(d). Phone Number

Contact Information Redacted

### 6(e). Fax Number

Contact Information Redacted

### 6(f). Email Address

Contact Information Redacted

## Secondary Contact

### 7(a). Name

Ms. Victoria Clifford

**7(b). Title**

Intellectual Property Paralegal

**7(c). Address****7(d). Phone Number**

Contact Information Redacted

**7(e). Fax Number**

Contact Information Redacted

**7(f). Email Address**

Contact Information Redacted

**Proof of Legal Establishment****8(a). Legal form of the Applicant**

Limited company (corporation)

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

Bermuda

The companies act 1981

Memorandum of association of company limited by shares (Section 7 (1) and (2) )

<http://www.bermulalaws.bm/Laws/Consolidated%20Laws/Companies%20Act%201981.pdf>

**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.**

Vistaprint N.V. (NASDAQ:VPRT)

**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**

Ernst Jan Teunissen	Director
Lawrence Adam Gold	Director

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

Ernst Jan Teunissen	President
Lawrence Adam Gold	Senior Vice President

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

Vistaprint N.V.	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.**

webs

**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.**

A number of operational and rendering issues may arise with the delegation, and subsequent operation and use of a new TLD. Some of these issues may be experienced just by the users of one or two particular TLDs, due to the nature or composition of the string itself; whereas other issues (such as software support) may be experienced across all new TLDs.

Evaluation of the potential operational and rendering issues for the .WEBS TLD was delegated to ARI. ARI is experienced with:

- The operational issues of operating TLDs
- TLDs that offer registrations at the third level (eg .com.au, .net.au) and below
- The rendering and operational issues surrounding the introduction of IDNs

ARI has executed a suite of tests to evaluate any issues arising from the use of the TLD string. ARI configured a test environment that consisted of DNS software, web server software, and an email server configured for sample domains in the .WEBS TLD. Where possible, ARI attempted to test many equivalent applications, however the number of and different versions of applications means that testing was limited to the most common environments.

The tests executed by ARI indicate that the .WEBS TLD is subject to the same issues already experienced by TLDs in the root, which are neither new nor unique. A summary of these common issues is provided below.

- Some applications make assumptions about known valid TLDs and fail to recognize new TLDs
- Some Non-IDN aware applications require the user to provide input in A-labels
- Some IDN aware applications present the user with the domain name using A-labels instead of U-labels
- Some IDN aware applications fail to render IRIs in a manner consistent with user expectations.

To mitigate these issues, ARI will work with the Applicant to ensure that maintainers of applications are made aware of the delegation and operation of the .WEBS TLD. When relevant, the Applicant and ARI will refer the maintainers to the verification code produced by ICANN in the area for Universal Acceptance of All Top Level Domains such that operational issues can be mitigated for other TLDs.

The Applicant and ARI will work with maintainers of applications to provide subject matter knowledge where required, and provide directions to the tools provided by third parties such as the International Components for Unicode project and other groups, that can assist the application maintainer in adding the required support. User education may be required enabling users to configure their applications for correct functioning of this TLD. An informational section on the TLD website will be considered to address questions raised by the Internet community.

The steps ARI will take to mitigate these issues are more than adequate. Thus, we do not believe the .WEBS TLD raises stability concerns and there is no reason that it should be denied on an operational and rendering issues bases.

## 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.

The Applicant, Vistaprint Limited, is the Intellectual Property holding company of the publicly traded company, Vistaprint NV, a large online supplier of printed and promotional material as well as marketing services to micro businesses and consumers. It offers business and consumer marketing and identity products and services worldwide. Vistaprint Limited and its subsidiaries also operate the WEBS and VISTAPRINT websites (webs.com, vistaprint.com and others) and benefits from online transactions with customers. Through its subsidiaries, the Applicant also provides hosting and other Internet related services. This is done in particular through the WEBS website, accessible through webs.com

According to the Applicant, the purpose of the TLD is manifold, as will be further explained below:

- i. Securing, protecting and operating one of the Applicant's business lines ("WEBS") to the benefit of its stakeholders, referred to below and in particular, members of the WEBS community;
- ii. Reflect and operate Applicant's "WEBS" business at the top level of the DNS' hierarchy;
- iii. Provide stakeholders of the Applicant, including subsidiaries, and their respective suppliers, customers, sponsorships, and their respective directors, officers, employees, with a recognizable and trusted location on the Internet;
- iv. Provide such stakeholders with a secure and safe Internet environment that is mainly or even fully under the control of the Applicant and its stakeholders.

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

i. WEBS is displayed by Applicant on its web site, webs.com. Through the WEBS community, Applicant has gained international exposure in hosting services and website related services. The proposed gTLD aims at consolidating the reputation of Applicant's WEBS services and the community it represents;

ii. From the Applicant's perspective, .WEBS will 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 .WEBS top-level domain will be unambiguous as regards the identity of the Registry Operator. Furthermore, it will be clear that the services offered under the .WEBS space were made possible thanks to the products and services offered by and for the Webs community;

iii. As mentioned in the vision / mission statement before, some of the key reasons why Applicant is applying for .WEBS are:

1. Marketing and branding: reflect the Applicant's WEBS business at the



top-level of the DNS' hierarchy,

2. Safety and security, given the fact that the TLD and most if not all of the domain names registered therein will be completely or at least partially under the control of the Registry Operator;

3. Affiliation between WEBS and the various product brands registered and/or used by the Applicant and/or its subsidiaries in their day-to-day business;

iv. The Applicant intends to implement the following policies and procedures with respect to the registration of domain names in the .WEBS top-level domain include but are not limited to:

1. Reservation of domain names in the name of the Applicant. These names include:

a) descriptive names, referring to the actual day-to-day business activities of the Applicant and/or its subsidiaries;

b) descriptive names, referring to the internal departments of the Applicant;

c) descriptive names, referring to the subsidiaries of the Applicant;

d) product and service brands promoted by the Applicant and/or its subsidiaries now and in the future;

e) etc.

2. Launch of the TLD:

a) Sunrise: allow physical persons, organizations and entities that meet the eligibility requirements in force at that point in time to choose the domain names that are identical to their trademarks;

b) 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.

c) 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 Applicant for the TLD (Vistaprint Limited). In any case, the Applicant reserves the right to impose additional and other restrictions from time to time at its sole discretion;

v. The Applicant currently has privacy and data protection policies in place in relation to the services it offers. The Applicant is committed to implement similar privacy policies in relation to the use of the TLD. The privacy policy that is currently in place in relation to services offered in connection with WEBS is accessible on <http://www.webs.com/privacy.htm>. At the time of submitting this application, this privacy policy is as follows:

"Webs is a website building and hosting service provided at <http://www.webs.com> and <http://www.freewebs.com> and its directly associated domains, widgets, tools, services and applications that are operated by Webs, Inc. (collectively, "Webs" or "Services"). Your privacy on the Internet is very important to us. We strive to make your online experience satisfying and safe.

This "Privacy Policy" explains what information we gather from our users and how we use it. By using or accessing our Services, you are accepting the practices described in this Privacy Policy. (Capitalized terms not defined herein have the meaning set forth in our Terms of Service).

Webs is not intended for children under 13 years of age. Consistent with the Federal Children's Online Privacy Protection Act of 1998 ("COPPA"), we will never knowingly gather or use personally identifiable information from anyone under the age of 13, and we do not allow anyone under the age of 13 to register on Webs.

What information does Webs gather?

Webs gathers and stores three types of information about users that are subject to our Privacy Policy:

Information users provide to us:

These are voluntary submissions made when creating an account on Webs or through your use of the Services, such as your name, date of birth, location and email address provided during registration, Content posted, or payment information provided during purchases. Please understand that when you sign into Webs or post Content, your information is not anonymous to us.

Information we collect when you interact with Webs:

We keep track of the actions you take on Webs, such as adding a friend, adding an application, or posting Content. Also, when you access our Services, we may collect information about your access method (such as hardware and software attributes), location, IP address, and pages you visit. In addition, we store certain information from your browser using "cookies". (For more on cookies, please see the section "What are cookies?")

Information we receive from third parties:

We do not own or operate the third-party applications, user websites and other services offered that you may use or interact with through Webs (collectively, "Webs-enhanced" applications, websites and services). Whenever you visit, use or interact with a Webs-enhanced application, website or service, we will receive information from them, including information about actions you take and Content you post on that application, website or service.

Why does Webs gather information about me?

Webs collects information in order to provide a safe, efficient and customized experience. This information allows us to better tailor our content to users' needs and to help us better understand the demographics of our audience. Webs may use some of this information for contacting you, customizing the content and advertising you view, improving our services, conducting research, and providing anonymous reporting for clients. We only collect personally identifiable information from you because you are voluntarily submitting the information to us in order to enjoy certain Services.

How will Websites and Applications on Webs treat my information?

As mentioned above, we do not own or operate Webs-enhanced applications, websites and services. We take steps to ensure that providers of Webs-enhanced applications, websites and services use information that you share on Webs in a manner consistent with your privacy settings and the terms of this Privacy Policy, but we cannot guarantee that they will follow our rules. Please take the time to familiarize yourself with the privacy settings of your account, as well as the settings and policies of the applications, websites and services that you visit, add or use on Webs. Here are some specific things to remember:

By visiting or becoming a Member of a Website on Webs, the Content and information you provide during the registration process (including your email address) and other interactions with the Website may be accessed by the Website Creator and their authorized representatives and administrators, as well as any Application Developer whose Applications run on that Website.

By adding or using an Application or a service provided by one of our affiliates or business partners, the information you provide in the interactions with that Application or service may be accessed by the respective Application Developer, affiliate or business partner and their authorized representatives.

Although certain categories of profile information (such as your birthday) have privacy settings, others (such as your name, gender, profile photo, geographic region, list of friends, list of websites you have joined) are considered publicly available and have no privacy settings associated with them.

Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere to the extent it has been shared with others, it was otherwise distributed pursuant to your privacy settings or privacy settings of the Website(s) or Application(s) you used, or it was copied or stored by other users.

Certain types of communications you send to other users cannot be removed, such as messages.

When you post information on a Website, that information is subject to that Website's privacy settings and privacy policy, which may change from time to time.

Publicly available information may be accessed by everyone on the Internet, including third-party search engines that may index, cache and store that information.

You should always review the policies of third party websites, applications and services to make sure you are comfortable with the ways in which they use information you share with them. Any information you share with them is at your own risk. If you find an application, website or service that violates our rules, you should report the violation to us using this automated form, and we reserve the right to take action as we deem appropriate without assuming any obligation or liability to do so.

What are cookies?

Webs may place a text file called a "cookie" in the browser files of your computer. These cookies help us make Webs easier to use, to make our advertising better, and to protect both you and Webs. For example, a cookie may be used to store or "remember" your Member login information (but not your password) so that you are not required to manually log into the site at every visit. You can remove or block cookies using the settings in your browser, but in some cases that may impact your ability to use some of our Services.

Our advertisers and partners may also set cookies through our Services. For more information, please see the section "What about third party advertisers and links?"

What about third party advertisers and links?

In the course of serving advertisements on Webs, a third-party advertiser may place or recognize a unique cookie on your browser. Additionally, some links from Webs may lead to websites operated by other companies. While these websites and advertisements may be co-branded with our name or logo, they are not operated or maintained by us. We do not control these cookies and users of Webs Services should check the privacy policy of the relevant advertiser to understand whether and how it uses cookies. Webs is not responsible for websites operated by third parties that are linked to by any of our sites.

Ads appearing on this website, Webs, and sites hosted by Webs may be delivered to you by Google Ad Manager, DoubleClick, or other advertising partners. Information about your visits to this site, such as the number of times you have viewed an ad (but not your name, address or other personal information), is used to serve ads to you. For more information about these partners, their cookies, and how to "opt-out," please follow the links below.

Network Advertising Initiative (NAI)

Google Ad Manager

DoubleClick

How secure is my information?

Webs uses commercially reasonable physical, electronic, and procedural measures to safeguard personally identifiable information in our possession against loss, theft and unauthorized use, disclosure or modification. We limit access to personal information about you to employees whom we believe reasonably need that information to provide support, products, or services to you or to fulfill their roles within our organization.

Although we have established and maintain security procedures to protect your personally identifiable information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information. We cannot guarantee that only authorized

persons will view your information. We cannot ensure that information you share on Webs will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Webs. You can reduce these risks by using common sense security practices such as choosing a strong password, using different passwords for different services, and using up-to-date antivirus software.

Please report any security violations to us on this automated form.

How private is the Content I upload?

Any Content uploaded or created using our Services and posted on a Website are by default hosted for the public and are thus publicly accessible unless explicitly protected by the Website Creator's optional password protection setting.

Please note that even if you do not publish links to Content or submit links to a search engine, individuals or search engines may discover and link to your Content by data-mining, guessing the address, spidering sites, or other methods. If you are concerned about the privacy or confidentiality of Content that you produce, please take all appropriate steps to ensure that sensitive materials are password-protected. Webs makes no guarantee as to the reliability or security of the password protection feature.

What control do I have over my information?

As a registered member, you may modify or update your personal account information at any time by logging into your account and (a) accessing the Settings area for each Website you have created, and (b) accessing the Manage Profile area for each Website you have joined by clicking on the corresponding Edit Profile link on your Dashboard page. You may also remove the Website(s) you may have created on Webs at any time by logging into your account and clicking on the corresponding "Delete Site" link on your Dashboard page. Should you desire to do so, you may also delete and close your Webs account at any time by contacting our support team. Note that removed or deleted information may persist in backup copies for a reasonable period of time.

How is information shared?

Webs will not share your personally identifiable information with others except as described herein with regards to sharing with Webs-enhanced applications, websites and services and in limited circumstances where we believe such sharing is reasonably necessary to offer the Services, legally required, or permitted by you. For example, we may provide information to service providers to help us bring you the services we offer. Specifically, we may use third parties to facilitate our business, such as to host the Services at a co-location facility for servers, to register your domain name, to send out email updates about Webs, to provide you with email functionality for your domain, to remove repetitive information from our user lists, to process payments for products or services, or to provide search results or links (including sponsored links). In connection with these offerings and business operations, our service providers may have access to your personal information for use for a limited time.

Where we utilize third parties for the processing of any personal information, we implement reasonable contractual and technical protections limiting the use of that information to the Webs-specified purposes. We may store personal information in locations outside the direct control of Webs (for instance, on servers or databases co-located with hosting providers).

Except as otherwise described in this Privacy Policy, we will not disclose personal information to any third party unless we believe that disclosure is necessary: (1) to conform to legal requirements or to respond to a subpoena, search warrant or other legal process received by Webs, whether or not a response is required by applicable law; (2) to enforce the Webs Terms of Service or to protect our rights; or (3) to protect the safety or rights of members of the public or users of the Services. Webs reserves the right to

transfer personal information to a successor in interest that acquires rights to that information as a result of the sale of Webs or substantially all of its assets to that successor in interest. We may also transfer such information in the course of corporate divestitures, mergers, or dissolution.

How am I notified of changes to this Privacy Policy

We may change this Privacy Policy pursuant to the procedures outlined in our Terms of Service. Unless stated otherwise, our current Privacy Policy applies to all information we have about you and your account. If we make changes to this Privacy Policy we will notify you by publication here.

Who can I contact about this Privacy Policy?

To submit an inquiry about our Privacy Policy, please contact our support department.

[Last updated: February 19, 2010]"

vi. The Applicant is part of a multinational organization that has been established in 1995. In December 2011, the Applicant acquired Webs, Inc., which has continuously been trading as WEBS since 2005 and under the webs.com domain name since 2005. Since its establishment, it has developed an important reputation in printing and Internet services. Therefore, the Applicant has different ways in order to make existing and future clients, visitors and stakeholders aware of the use and possibly the (gradual) move from the group's webs.com domain name to the .WEBS TLD, including but not limited to:

1. Internet advertising campaigns;
2. having Internet traffic to its key domain names resolving into domain names registered in the .WEBS TLD;
3. email marketing campaigns; etc.

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

i. The Applicant will organize the registry operation for the .WEBS TLD in such a manner that it will minimize the likelihood of having multiple applications for a particular domain name. This can be achieved in one of the following ways:

1. Given the fact that, at least prior to the launch of the .WEBS top-level domain, the Applicant / Registry Operator will reserve, delegate and use a large number of domain names that are directly or indirectly relevant to Applicant's business in its own name. Since quite a number of these domain names will 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 will 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 .WEBS top-level domain;

3. The Registry Operator may give existing (paying) customers a right of first offer or first refusal for the registration of certain types of domain names and/or during one or more specific launch phases. The duration and/or nature of the customer relationship may be used as a criteria to solve contention when multiple applications for a particular domain name occur;

4. 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.

ii. Given the Applicant's activity as an innovative web hosting provider at a limited cost, the Applicant intends to make the .WEBS top-level domain

available to qualifying domain name registrants at a limited cost or at no cost as part of a web hosting or other service package. As the Applicant will be less dependent on the service offerings of existing registries, the pricing of the Applicant's services will depend less on the pricing of the service offerings from those registries. The per domain name price to be paid by the Applicant for a web hosting service, inclusive of a domain name, is likely to be lower. This may result in a better price offering to Internet users for the Applicant's value added services. The Internet user and the Internet community would benefit from the Applicant being able to reduce costs, as this may result in better pricing and/or more room for investing in customer service, in innovative Internet solutions, etc. It must be noted that this does not preclude the Applicant / Registry Operator to charge higher fees for the registration of domain names under the .WEBS TLD at its discretion, e.g., as part of premium packages or for certain categories of clients and customers. The fact that some may be willing to pay more for the registration of particular domain names would again be beneficial for other potential domain name registrants in the .WEBS TLD.

iii. The Applicant / Registry Operator may at its discretion make contractual commitments to increase or decrease the fees for the registration of domain names under the .WEBS TLD.

## 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 multinational organization which holds interests in printing and other services worldwide, it has a vested interest in giving its visitors, clients and business partners a clear and predictable naming scheme in the .WEBS TLD. Since visitors and clients may mainly be looking for offers and activities organized by local branches and subsidiaries 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 or its Affiliates, 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 activities in printing, business and consumer marketing and identity products and services, and possibly other markets; and
- in order to directly and indirectly promote local commercial activity

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.

As mentioned in response to Question 18 (b) above, the Applicant is a large online supplier of printed and promotional material as well as marketing services to micro businesses and consumers. In connection to its business, the Applicant has a substantial experience and expertise in managing complex information technology infrastructures, hereby relying on in-house and external resources.

However, the Applicant has no in-depth experience in managing a domain name registry system and it would require too many efforts for the Applicant to develop a system itself that complies with the specific technical requirements imposed upon new gTLD registries. Therefore, the Applicant has decided to rely on ARI Registry Services ("ARI" - see [www.ariservices.com](http://www.ariservices.com)) and NetNames to provide a full suite of services in relation to the deployment and operation of its applied-for .WEBS TLD. It has been agreed between the Applicant and ARI that ARI will perform the back-end registry services for the .WEBS registry.

The response to this question describes the registry services for the .WEBS TLD as will be provided by ARI, in the name and on behalf of the Applicant. These registry services are referred to as ARI's Managed TLD Registry Service. When, throughout the responses to questions #23 to #44, it is stated that ARI will perform certain services or comply with certain standards or processes, ARI will do this in the name and on behalf of the Applicant, who itself is committed to comply with these standards or processes towards ICANN. Where use is made of the first person plural, reference is made to ARI, as the answer to this question is provided directly by ARI, the back-end provider of registry services for the applied-for .WEBS TLD (also referred to as 'this TLD').

It goes without saying that each and every service offered under the .WEBS gTLD will be provided under the authority and responsibility of the Applicant.

#### 1 INTRODUCTION

ARI's Managed TLD Registry Service is a complete offering, providing all of the required registry services. What follows is a description of each of those services.

#### 2 REGISTRY SERVICES

The following sections describe the registry services provided. Each of these services has, where required, been designed to take into account the requirements of consensus policies as documented here:

[<http://www.icann.org/en/resources/Registrars/consensus-policies>]

At the time of delegation into the root this TLD will not be offering any unique Registry services.

##### 2.1 Receipt of Data from Registrars

The day-to-day functions of the registry, as perceived by Internet users, involves the receipt of data from Registrars and making the necessary changes



to the SRS database. Functionality such as the creation, renewal and deletion of domains by Registrars, on behalf of registrants, is provided by two separate systems:

- An open protocol-based provisioning system commonly used by Registrars with automated domain management functionality within their own systems.
  - A dedicated website providing the same functionality for user interaction.
- Registrants (or prospective registrants) who wish to manage their existing domains or credentials, register new domains or delete their domains will have their requests carried out by Registrars using one of the two systems described below.

ARI operates Extensible Provisioning Protocol (EPP) server software and distributes applicable toolkits to facilitate the receipt of data from Registrars in a common format. EPP offers a common protocol for Registrars to interact with SRS data and is favoured for automating such interaction in the Registrar's systems. In addition to the EPP server, Registrars have the ability to use a web-based management interface (SRS Web Interface), which provides functions equivalent to the EPP server functionality.

#### 2.1.1 EPP

The EPP software allows Registrars to communicate with the SRS using a standard protocol. The EPP server software is compliant with all appropriate RFCs and will be updated to comply with any relevant new RFCs or other new standards, as and when they are finalised. All standard EPP operations on SRS objects are supported.

Specifically, the EPP service complies with the following standards:

- RFC 5730 Extensible Provisioning Protocol (EPP).
- RFC 5731 Extensible Provisioning Protocol (EPP) Domain Name Mapping.
- RFC 5732 Extensible Provisioning Protocol (EPP) Host Mapping.
- RFC 5733 Extensible Provisioning Protocol (EPP) Contact Mapping.
- RFC 5734 Extensible Provisioning Protocol (EPP) Transport over TCP.
- RFC 5910 Domain Name System (DNS) Security Extensions for the Extensible Provisioning Protocol (EPP).
- RFC 3915 Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (EPP).
- Extensions to ARI's EPP service comply with RFC 3735 Guidelines for Extending the Extensible Provisioning Protocol (EPP).

##### 2.1.1.1 Security for EPP Service

To avoid abuse and to mitigate potential fraudulent operations, the EPP server software uses a number of security mechanisms that restrict the source of incoming connections and prescribe the authentication and authorisation of the client. Connections are further managed by command rate limiting and are restricted to only a certain number for each Registrar, to help reduce unwanted fraudulent and other activities. Additionally, secure communication to the EPP interface is required, lowering the likelihood of the authentication mechanisms being compromised.

The EPP server has restrictions on the operations it is permitted to make to the data within the registry database. Except as allowed by the EPP protocol, the EPP server cannot update the credentials used by Registrars for access to the SRS. These credentials include those used by Registrars to login to ARI's SRS Web Interface and the EPP service.

Secure communication to the EPP server is achieved via the encryption of EPP sessions. The registry system and associated toolkits support AES 128 and 256 via TLS.

The Production and Operational Testing and Evaluation (OTE) EPP service is protected behind a secure firewall that only accepts connections from registered IP addresses. Registrars are required to supply host IP addresses that they intend to use to access the EPP service.

Certificates are used for encrypted communications with the registry. Registrars require a valid public/private key pair signed by the ARI CA to verify authenticity. These certificates are used to establish a TLS secure session between client and server.

EPP contains credential elements in its specification which are used as an additional layer of authentication. In accordance with the EPP specification, the server does not allow client sessions to carry out any operations until credentials are verified.

The EPP server software combines the authentication and authorisation elements described above to ensure the various credentials supplied are associated with the same identity. This verification requires that:

- The username must match the common name in the digital certificate.
- The certificate must be presented from a source IP listed against the Registrar whose common name appears in the certificate.
- The username and password must match the user name and password listed against the Registrar's account with that source IP address.

To manage normal operations and prevent an accidental or intentional Denial of Service, the EPP server can be configured to rate limit activities by individual Registrars.

#### 2.1.1.2 Stability Considerations

The measures that restrict Registrars to a limit of connections and operations for security purposes also serve to keep the SRS and the EPP server within an acceptable performance and resource utilisation band. Therefore, scaling the service is an almost linear calculation based on well-defined parameters.

The EPP server offers consistent information between Registrars and the SRS Web Interface. The relevant pieces of this information are replicated to the DNS within seconds of alteration, thus ensuring that a strong consistency between the SRS and DNS is maintained at all times.

#### 2.1.2 SRS Web Interface

The registry SRS Web Interface offers Registrars an alternative SRS interaction mechanism to the EPP server. Available over HTTPS, this interface can be used to carry out all operations which would otherwise occur via EPP, as well as many others. Registrars can use the SRS Web Interface, the EPP server interface or both - with no loss of consistency within the SRS.

##### 2.1.2.1 Security and Consistency Considerations for SRS Web Interface

The SRS Web Interface contains measures to prevent abuse and to mitigate fraudulent operations. By restricting access, providing user level authentication and authorisation, and protecting the communications channel, the application limits both the opportunity and scope of security compromise. Registrars are able to create individual users that are associated with their Registrar account. By allocating the specific operations each user can access, Registrars have full control over how their individual staff members interact with the SRS. Users can be audited to identify which operations were conducted and to which objects those operations were applied.

A secure connection is required before credentials are exchanged and once authenticated. On login, any existing user sessions are invalidated and a new session is generated, thereby mitigating session-fixation attacks and reducing possibilities that sessions could be compromised.

##### 2.1.3 Securing and Maintaining Consistency of Registry-Registrar Interaction Systems

ARI ensures all systems through which Registrars interact with the SRS remain consistent with each other and apply the same security rules. Additionally, ARI also ensures that operations on SRS objects are restricted to the appropriate entity. For example:

- In order to initiate a transfer a Registrar must provide the associated domain password (authinfo) which will only be known by the registrant and the current sponsoring Registrar.
- Only sponsoring Registrars are permitted to update registry objects.

All operations conducted by Registrars on SRS objects are auditable and are identifiable to the specific Registrar's user account, IP address and the time

of the operation.

## 2.2 Disseminate Status Information of TLD Zone Servers to Registrars

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

Normal operations are those when:

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

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

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

### 2.2.1 Communication Policy

ARI maintains close communication with Registrars regarding the performance and consistency of the TLD zone servers.

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

Communication using the Registrar contact information discussed above will occur prior to any maintenance that has the potential to effect the access to, consistency of, or reliability of the TLD zone servers. If such maintenance is required within a short time frame, immediate communication occurs using the above contact information. In either case, the nature of the maintenance and how it affects the consistency or accessibility of the TLD zone servers, and the estimated time for full restoration, are included within the communication. That being said, the TLD zone server infrastructure has been designed in such a way that we expect no down time. Only individual sites will potentially require downtime for maintenance; however the DNS service itself will continue to operate with 100% availability.

### 2.2.2 Security and Stability Considerations

ARI restricts zone server status communication to Registrars, thereby limiting the scope for malicious abuse of any maintenance window. Additionally, ARI ensures Registrars have effective operational procedures to deal with any status change of the TLD nameservers and will seek to align its communication policy to those procedures.

## 2.3 Zone File Access Provider Integration

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

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

- Zone file format and location.
- Availability of the zone file access host via FTP.

- Logging of requests to the service (including the IP address, time, user and activity log).
- Access frequency.

## 2.4 Zone File Update

To ensure changes within the SRS are reflected in the zone file rapidly and securely, ARI updates the zone file on the TLD zone servers using software compliant with RFC 2136 (Dynamic Updates in the Domain Name System (DNS UPDATE)) and RFC 2845 (Secret Key Transaction Authentication for DNS (TSIG)). This updating process follows a staged but rapid propagation of zone update information from the SRS, outwards to the TLD zone servers - which are visible to the Internet. As changes to the SRS data occur, those changes are updated to isolated systems which act as the authoritative primary server for the zone, but remain inaccessible to systems outside ARI's network. The primary servers notify the designated secondary servers, which service queries for the TLD zone from the public. Upon notification, the secondary servers transfer the incremental changes to the zone and publicly present those changes. The protocols for dynamic update are robust and mature, as is their implementation in DNS software. The protocols' mechanisms for ensuring consistency within and between updates are fully implemented in ARI's TLD zone update procedures. These mechanisms ensure updates are quickly propagated while the data remains consistent within each incremental update, regardless of the speed or order of individual update transactions. ARI has used this method for updating zone files in all its TLDs including the .au ccTLD, pioneering this method during its inception in 2002. Mechanisms separate to RFC 2136-compliant transfer processes exist; to check and ensure domain information is consistent with the SRS on each TLD zone server within 10 minutes of a change.

## 2.5 Operation of Zone Servers

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

### 2.5.1 Security and Operational Considerations of Zone Server Operations

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

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

The TLD zone servers are protected from accessibility loss by malicious intent or misadventure, via the provision of significant over-capacity of resources and access paths. Multiple independent network paths are provided to each TLD zone server and the query servicing capacity of the network exceeds the extremely conservatively anticipated peak load requirements by at least 10 times, to prevent loss of service should query loads significantly increase. As well as the authentication, authorisation and consistency checks carried out by the Registrar access systems and DNS update mechanisms, ARI reduces the scope for alteration of DNS data by following strict DNS operational practices:

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

## 2.6 Dissemination of Contact or Other Information

Registries are required to provide a mechanism to identify the relevant contact information for a domain. The traditional method of delivering this is via the WhoIs service, a plain text protocol commonly accessible on TCP port 43. ARI also provides the same functionality to users via a web-based WhoIs service. Functionality remains the same with the web-based service, which only requires a user to have an Internet browser.

Using the WhoIs service, in either of its forms, allows a user to query for domain-related information. Users can query for domain details, contact details, nameserver details or Registrar details.

A WhoIs service, which complies with RFC 3912, is provided to disseminate contact and other information related to a domain within the TLD zone.

### 2.6.1 Security and Stability Considerations

ARI ensures the service is available and accurate for Internet users, while limiting the opportunity for its malicious use. Many reputation and anti-abuse services rely on the availability and accuracy of the WhoIs service, however the potential for abuse of the WhoIs service exists.

Therefore, certain restrictions are made to the access of WhoIs services, the nature of which depend on the delivery method - either web-based or the traditional text-based port 43 service. In all cases, there has been careful consideration given to the benefits of WhoIs to the Internet community, as well as the potential harm to registrants - as individuals and a group - with regard to WhoIs access restrictions.

The WhoIs service presents data from the registry database in real time. However this access is restricted to reading the appropriate data only. The WhoIs service does not have the ability to alter data or to access data not related to the WhoIs service. The access limitations placed on the WhoIs services prevent any deliberate or incidental denial of service that might impact other registry services.

Restrictions placed on accessing WhoIs services do not affect legitimate use. All restrictions are designed to target abusive volume users and to provide legitimate users with a fast and available service. ARI has the ability to 'whitelist' legitimate bulk users of WhoIs, to ensure they are not impacted by standard volume restrictions.

The data presentation format is consistent with the canonical representation of equivalent fields, as defined in the EPP specifications and ICANN agreement.

#### 2.6.1.1 Port 43 WhoIs

A port 43-based WhoIs service complying with RFC 3912 is provided and will be updated to meet any other relevant standards or best practice guidelines related to the operation of a WhoIs service.

While the text-based service can support thousands of simultaneous queries, it has dynamic limits on queries per IP address to restrict data mining efforts. In the event of identified malicious use of the service, access from a single IP address or address ranges can be limited or blocked.

#### 2.6.1.2 Web-based WhoIs

ARI's web-based WhoIs service provides information consistent with that contained within the SRS.

The web-based WhoIs service contains an Image Verification Check (IVC) and query limits per IP address. These restrictions strike a balance between acceptable public usage and abusive use or data mining. The web-based WhoIs service can blacklist IP addresses or ranges to prevent abusive use of the service.

## 2.7 IDNs - Internationalised Domain Names

An Internationalised Domain Name (IDN) allows registrants to register domains in their native language and have it display correctly in IDN aware software.

This includes allowing a language to be read in the manner that would be common for its readers. For example, an Arabic domain would be presented right to left for an Arabic IDN aware browser.

The inclusion of IDNs into the TLD zones is supported by ARI. All the registry services, such as the EPP service, SRS Web Interface and RDPS (web and port 43), support IDNs. However there are some stability and security considerations related to IDNs which fall outside the general considerations applicable individually to those services.

#### 2.7.1 Stability Considerations Specific to IDN

To avoid the intentional or accidental registration of visually similar chars, and to avoid identity confusion between domains, there are several restrictions on the registration of IDNs.

##### 2.7.1.1 Prevent Cross Language Registrations

Domains registered within a particular language are restricted to only the chars of that language. This avoids the use of visually similar chars within one language which mimic the appearance of a label within another language, regardless of whether that label is already within the DNS or not.

##### 2.7.1.2 Inter-language and Intra-language Variants to Prevent Similar Registrations

ARI restricts child domains to a specific language and prevents registrations in one language being confused with a registration in another language, for example Cyrillic a (U+0430) and Latin a (U+0061).

#### 2.8 DNSSEC

DNSSEC provides a set of extensions to the DNS that allow an Internet user (normally the resolver acting on a user's behalf) to validate that the DNS responses they receive were not manipulated en-route.

This type of fraud, commonly called 'man in the middle', allows a malicious party to misdirect Internet users. DNSSEC allows a domain owner to sign their domain and to publish the signature, so that all DNS consumers who visit that domain can validate that the responses they receive are as the domain owner intended.

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

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

##### 2.8.1 Stability and Operational Considerations for DNSSEC

###### 2.8.1.1 DNSSEC Practice Statement

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

###### 2.8.1.2 Receipt of Public Keys from Registrars

The public key for a child domain is received by ARI from the Registrar via either the EPP or SRS Web Interface. ARI uses an SHA-256 digest to generate the DS Resource Record (RR) for inclusion into the zone file.

### 2.8.1.3 Resolution Stability

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

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

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

## 3 APPROACH TO SECURITY AND STABILITY

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

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

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

# Demonstration of Technical & Operational Capability

## 24. Shared Registration System (SRS) Performance

The Applicant has engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q24 - ARI Background & Roles.pdf'. This response describes the SRS as implemented by ARI.

### 1 INTRODUCTION

ARI has demonstrated delivery of an SRS with exceptional availability, performance and reliability. ARI are experienced running mission critical SRSs and have significant knowledge of the industry and building and supporting SRSs.

ARI's SRS has successfully supported a large group of Registrars for ASCII and IDN based TLDs. The system is proven to sustain high levels of concurrency, transaction load, and system uptime. ARI's SRS meets the following requirements:

- Resilient to wide range of security & availability threats

- Consistently exceeds performance & availability SLAs
- Allows capacity increase with minimal impact to service
- Provides fair & equitable provisioning for all Registrars

## 2 CAPACITY

ARI's SRS was built to sustain 20M domain names. Based on ARI's experience running a ccTLD registries and industry analysis, ARI were able to calculate the conservative characteristics of a registry this size.

Through conservative statistical analysis of the .au registry and data presented in the May 2011 ICANN reports for the .com & .net, .org, .mobi, .info, .biz and .asia [<http://www.icann.org/en/resources/registries/reports>] we know there is:

- An average of 70 SRS TPS per domain, per month
- A ratio of 3 query to 2 transform txs

This indicates an expected monthly transaction volume of 1,400M txs (840M query and 560M transforms).

Through statistical analysis of the .au registry and backed up by the data published in the .net RFP responses [<http://archive.icann.org/en/tlds/net-rfp/net-rfp-public-comments.htm>] we also know:

- The peak daily TPS is 6% of monthly total
- The peak 5 min is 5% of the peak day

Thus we expect a peak EPP tx rate of 14,000 TPS (5,600 transform TPS and 8,400 query TPS)

Through conservative statistical analysis of the .au registry we know:

- The avg no. contacts/domain is 3.76
- The avg no. hosts/domain is 2.28

This translates into a requirement to store 75.2M contacts and 45.6M hosts.

Finally through real world observations of the .au registry, which has a comprehensive web interface when compared to those offered by current gTLD registries, we know there is an avg of 0.5 HTTP requests/sec to the SRS web interface per Registrar. We also know that this behaviour is reasonably flat.

To support an estimated 1000 Registrars, would require 500 requests/second. For perspective on the conservativeness of this, the following was taken from data in the May 2011 ICANN reports referenced above:

- .info: ~7.8M names peaks at ~1,400 TPS (projected peak TPS of ~3,600 with 20M)
- .com: ~98M names peaks at ~41,000 TPS (projected peak TPS of ~8,300 TPS with 20M)
- .org: ~9.3M names, peaks at ~1,400 TPS (projected peak TPS of ~3,100 with 20M)

After performing this analysis the projected TPS for .com was still the largest value.

ARI understand the limitations of this method but it serves as a best estimate of probable tx load. ARI has built overcapacity of resources to account for limitations of this method, however as numbers are more conservative than real world observations, we are confident this capacity is sufficient.

This TLD is projected to reach 150000 domains at its peak volume and will generate 105 EPP TPS. This will consume 0,75% of the resources of the SRS infrastructure. As is evident ARI's SRS can easily accommodate this TLD's growth plans. See attachment 'Q24 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI expects to provide Registry services to 100 TLDs and a total of 12M domains by end of 2014. With all the TLDs and domains combined, ARI's SRS infrastructure will be 60% utilized. The SRS infrastructure capacity can be easily scaled as described in Q32

ARI benchmarked their SRS infrastructure and used the results to calculate the required computing resources for each of the tiers within the architecture; allowing ARI to accurately estimate the required CPU, IOPS, storage and memory requirements for each server, and the network bandwidth & packet throughput requirements for the anticipated traffic. These capacity numbers were then doubled to account for unanticipated traffic spikes, errors in predictions, and headroom for growth. Despite doubling numbers, effective estimated capacity is still reported as 20M. The technical resource allocations are explored in Q32.



### 3 SRS ARCHITECTURE

ARI's SRS has the following major components:

- Network Infrastructure
- EPP Application Servers
- SRS Web Interface Application Servers
- SRS Database

Attachment 'Q24 - SRS.pdf' shows the SRS systems architecture and data flows. Detail on this architecture is in our response to Q32. ARI provides two distinct interfaces to the SRS: EPP and SRS Web. Registrar SRS traffic enters the ARI network via the redundant Internet link and passes (via the firewall) to the relevant application server for the requested service (EPP or SRS Web). ARI's EPP interface sustains high volume and throughput domain provisioning transactions for a large number of concurrent Registrar connections. ARI's SRS Web interface provides an alternative to EPP with a presentation centric interface and provides reporting and verification features additional to those provided by the EPP interface.

#### 3.1 EPP

ARI's EPP application server is based on EPP as defined in RFCs 5730 - 5734. Registrars send XML based transactions to a load balanced EPP interface which forwards to one of the EPP application servers. The EPP application server then processes the XML and converts the request into database calls that retrieve or modify registry objects in the SRS database. The EPP application server tier comprises of three independent servers with dedicated connections to the registry database. Failure of any one of these servers will cause Registrar connections to automatically re-establish with one of the remaining servers. Additional EPP application servers can be added easily without any downtime. All EPP servers accept EPP both IPv4 & IPv6.

#### 3.2 SRS Web

The SRS Web application server is a Java web application. Registrars connect via the load balancer to a secure HTTP listener running on the web servers. The SRS web application converts HTTP requests into database calls which query or update objects in the SRS database. The SRS Web application server tier consists of two independent servers that connect to the database via JDBC. If one of these servers is unavailable the load balancer re-routes requests to the surviving server. Additional servers can be added easily without any downtime. These servers accept both IPv4 & IPv6.

#### 3.3 SRS Database

The SRS database provides persistent storage for domains and supporting objects. It offers a secure way of storing and retrieving objects provisioned within the SRS and is built on the Oracle 11g Enterprise Edition RDBMS. The SRS Database tier consists of four servers clustered using Oracle Real Application Clusters (RAC). In the event of failure of a database server, RAC will transparently transition its client connections to a surviving database host. Additional servers can be added easily without any downtime.

#### 3.4 Number of Servers

**EPP Servers** - The EPP cluster consists of 3 servers that can more than handle the anticipated 20M domains. This TLD will utilize 0,75% of this capacity at its peak volume. As the utilisation increases ARI will add additional servers ensuring the utilisation doesn't exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime.

**SRS Web Servers** - The SRS Web cluster consists of 2 servers that can more than handle the anticipated 20M domains. This TLD will utilize 0,75% of this capacity at its peak volume. As the utilisation increases ARI will add additional servers ensuring the utilisation doesn't exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime.

**SRS DB Servers** - The SRS DB cluster consists of 4 servers that can more than handle the anticipated 20M domains. This TLD will utilize 0,75% of this capacity at its peak volume. As the utilisation increases ARI will add additional servers ensuring the total utilisation doesn't exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime.

### 3.5 SRS Security

ARI adopts a multi-layered security solution to protect the SRS. An industry leading firewall is deployed behind the edge router and is configured to only allow traffic on the minimum required ports and protocols. Access to the ARI EPP service is restricted to a list of known Registrar IPs.

An Intrusion Detection device is in-line with the firewall to monitor and detect suspicious activity.

All servers are configured with restrictive host based firewalls, intrusion detection, and SELinux. Direct root access to these servers is disabled and all access is audited and logged centrally.

The SRS database is secured by removal of non-essential features and accounts, and ensuring all remaining accounts have strong passwords. All database accounts are assigned the minimum privileges required to execute their business function.

All operating system, database, and network device accounts are subject to strict password management controls such as validity & complexity requirements. Registrar access to the SRS via EPP or the Web interface is authenticated and secured with multi-factor authentication (NIST Level 3) and digital assertion as follows:

- Registrar's source IP must be allowed by the front-end firewalls. This source IP is received from the Registrar via a secure communication channel from within the SRS Web interface
- Registrar must use a digital certificate provided by ARI
- Registrar must use authentication credentials that are provided by encrypted email

All communication between the Registrar and the SRS is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57.

### 3.6 SRS High Availability

SRS availability is of paramount. Downtime is eliminated or minimised where possible. The infrastructure contains no single points of failure. N+1 redundancy is used as a minimum, which not only protects against unplanned downtime but also allows ARI to execute maintenance without impacting service. Redundancy is provided in the network with hot standby devices & multiple links between devices. Failure of any networking component is transparent to Registrar connections.

N+N redundancy is provided in the EPP and SRS Web application server tiers by the deployment of multiple independent servers grouped together as part of a load-balancing scheme. If a server fails the load balancer routes requests to the remaining servers.

N+N redundancy is provided in the database tier by the use of Oracle Real Application Cluster technology. This delivers active/active clustering via shared storage. This insulates Registrars from database server failure.

Complete SRS site failure is mitigated by the maintenance of a remote standby site - a duplicate of the primary site ready to be the primary if required. The standby site database is replicated using real time transaction replication from the main database using Oracle Data Guard physical standby. If required the Data Guard database can be activated quickly and service resumes at the standby site.

### 3.7 SRS Scalability

ARI's SRS scales efficiently. At the application server level, additional computing resource can be brought on-line rapidly by deploying a new server online. During benchmarking this has shown near linear.

The database can be scaled horizontally by adding a new cluster node into the RAC cluster online. This can be achieved without disruption to connections. The SRS has demonstrated over 80% scaling at the database level, but due to the distributed locking nature of Oracle RAC, returns are expected to diminish as the number of servers approaches double digits. To combat this ARI ensures that when the cluster is 'scaled' more powerful server equipment is added rather than that equal to the current members. Capacity can be added to the SAN at any time without downtime increasing storage and IOPs.

### 3.8 SRS Inter-operability and Data Synchronisation

The SRS interfaces with a number of related registry systems as part of normal operations.

#### 3.8.1 DNS Update

Changes made in the SRS are propagated to the DNS via an ARI proprietary DNS Update process. This process runs on the 'hidden' primary master nameserver and waits on a queue. It is notified when the business logic inserts changes into the queue for processing. The DNS Update process reads these queue entries and converts them into DNS update (RFC2136) commands that are sent to the nameserver. The process of synchronising changes to SRS data to the DNS occurs in real-time.

#### 3.8.2 WhoIs

The provisioned data supporting the SRS satisfies WhoIs queries. Thus the WhoIs and SRS share data sets and the WhoIs is instantaneously updated. Under normal operating conditions the WhoIs service is provided by the infrastructure at the secondary site in order to segregate the load and protect SRS from WhoIs demand (and vice versa). WhoIs queries that hit the standby site will query data stored in the standby database - maintained in near real-time using Oracle Active Data Guard. If complete site failure occurs WhoIs and SRS can temporarily share the same operations centre at the same site (capacity numbers are calculated for this).

#### 3.8.3 Escrow

A daily Escrow extract process executes on the database server via a dedicated database account with restricted read-only access. The results are then transferred to the local Escrow Communications server by SSH.

### 4 OPERATIONAL PLAN

ARI follow defined policies/procedures that have developed over time by running critical registry systems. Some principals captured by these are:

- Conduct all changes & upgrades under strict and well-practised change control procedures
- test, test and test again
- Maintain Staging environments as close as possible to production infrastructure/configuration
- Eliminate all single points of failure
- Conduct regular security reviews & audits
- Maintain team knowledge & experience via skills transfer/training
- Replace hardware when no longer supported by vendor
- Maintain spare hardware for all critical components
- Execute regular restore tests of all backups
- Conduct regular capacity planning exercises
- Monitor everything from multiple places but ensure monitoring is not 'chatty'
- Employ best of breed hardware & software products & frameworks (such as ITIL, ISO27001 and Prince2)
- Maintain two distinct OT&E environments to support pre-production testing for Registrars

### 5 SLA, RELIABILITY & COMPLIANCE

ARI's SRS adheres to and goes beyond the scope of Specification 6 and Specification 10 of the Registry Agreement. ARI's EPP service is XML compliant and XML Namespace aware. It complies with the EPP protocol defined in RFC5730, and the object mappings for domain, hosts & contacts are compliant with RFC 5731, 5732 & 5733 respectively. The transport over TCP is compliant with RFC5734. The service also complies with official extensions to support DNSSEC, RFC5910, & Redemption Grace Period, RFC 3915.

ARI's SRS is sized to sustain a peak transaction rate of 14,000 TPS while meeting strict internal Operational Level Agreements (OLAs). The monthly-based OLAs below are more stringent than those in Specification 10 (Section 2).

EPP Service Availability: 100%

EPP Session Command Round Trip Time (RTT): <=1000ms for 95% of commands

EPP Query Command Round Trip Time (RTT):  $\leq 500$ ms for 95% of commands  
EPP Transform Command Round Trip Time (RTT):  $\leq 1000$ ms for 95% of commands  
SRS Web Interface Service Availability: 99.9%

ARI measure the elapsed time of every query, transform and session EPP transaction, and calculate the percentage of commands that fall within OLA on a periodic basis. If percentage value falls below configured thresholds on-call personnel are alerted.

SRS availability is measured by ARI's monitoring system which polls both the EPP and SRS Web services status. These checks are implemented as full end to end monitoring scripts that mimic user interaction, providing a true representation of availability. These 'scripts' are executed from external locations on the Internet.

## 6 RESOURCES

This function will be performed by ARI. ARI staff are industry leading experts in domain name registries with the experience and knowledge to deliver outstanding SRS performance.

The SRS is designed, built, operated and supported by the following ARI departments:

- Products and Consulting Team (7 staff)
- Production Support Group (27 staff)
- Development Team (11 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided in attachment 'Q24 - ARI Background & Roles.pdf'. This attachment describes the functions of the teams and the number and nature of staff within. The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.

ARI provides registry backend services to 5 TLDs and has a vast experience in estimating the number of resources required to support a SRS.

Based on past experience ARI estimates that the existing staff is adequate to support an SRS that supporting at least 50M domains. Since this TLD projects 150000 domains, 0,3% of these resources are allocated to this TLD. See attachment 'Q24 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required, trained resources can be added to any of the teams with a 2 month lead time.

The Products and Consulting team is responsible for product management of the SRS solution including working with clients and the industry to identify new features or changes required. The team consists of:

- 1 Products and Consulting Manager
- 1 Product Manager
- 1 Technical Product Manager
- 4 Domain Name Industry Consultants

The Production Support Group (PSG) is responsible for the design, deployment and maintenance of the SRS infrastructure including capacity planning and monitoring as well as security aspects - ensuring the SRS services are available and performing at the appropriate level and operating correctly. The team consists of:

- Production Support Manager
- Service Desk:
  - 1 Level 1 Support Team Lead
  - 8 Customer Support Representatives (Level 1 support)
  - 1 Level 2 Support Team Lead
  - 4 Registry Specialists (Level 2 support)
- Operations (Level 3 support):
  - 1 Operations Team Lead
  - 2 Systems Administrators
  - 2 Database Administrators
  - 2 Network Engineers
- Implementation:

- 1 Project Manager
- 2 Systems Administrators
- 1 Database Administrator
- 1 Network Engineer

The development team is responsible for implementing changes and new features into the SRS as well as bug fixing and complex issue diagnosis. The team consists of:

- 1 Development Manager
- 2 Business Analysts
- 6 Developers
- 2 Quality Analysts

These resources sufficiently accommodate the needs of this TLD, and are included in ARI's fees as described in our Financial responses.

## 25. Extensible Provisioning Protocol (EPP)

The Applicant has engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q25 - ARI Background & Roles.pdf'. This response describes the Extensible Provisioning Protocol (EPP) interface as implemented by ARI.

### 1 INTRODUCTION

ARI's EPP service is XML compliant and XML Namespace aware. The service complies with the EPP protocol defined in RFC5730, and the object mappings for domain, hosts and contacts are compliant with RFC5731-3 respectively. The transport over TCP is implemented in compliance with RFC5734. The service also complies with the official extensions to support DNSSEC, RFC5910 and Redemption Grace Period, RFC3915. ARI implemented EPP draft version 0.6 in 2002, then migrated to EPP RFC 1.0 on its publishing in 2004. The system has operated live since 2002 in the .au ccTLD.

Descriptions in this response follow the terminology used in the EPP RFCs. When referring to the software involved in the process, ARI's EPP interface is called the server, and the software used by Registrars is called the client.

### 2 TRANSPORT LAYER

The ARI EPP service implements the RFC5734 - EPP Transport over TCP. Connections are allowed using TLSv1 encryption, optionally supporting SSLv2 Hello for compatibility with legacy clients. AES cipher suites for TLS as described in RFC3268 are the only ones allowed.

#### 2.1 Authentication

Registrar access to the EPP interface is authenticated and secured with multi-factor authentication (NIST Level 3) and digital assertion as follows.

Registrars must:

- present a certificate, during TLS negotiation, signed by the ARI Certificate Authority (CA). The server returns a certificate also signed by the ARI CA. Not presenting a valid certificate results in session termination. ARI requires that the Common Name in the subject field of the certificate identifies the Registrar.
- originate connections from an IP address that is known to be assigned to the Registrar with that Common Name.
- Registrar must use authentication credentials provided to the Registrar via encrypted email

- Registrars aren't able to exceed a fixed number of concurrent connections.

The connection limit is prearranged and designed to prevent abuse of

Registrars' systems from affecting the Registry. The limit is set to reasonable

levels for each Registrar, but can be increased to ensure legitimate traffic is unaffected. If any of the above conditions aren't met the connection is terminated.

All communication between the Registrars and the EPP service is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57.

### 2.3 Connection Close

The server may close the connection as a result of a logout, an error where the state of the connection is indeterminate, or after a timeout. Timeout occurs where no complete EPP message is received on the connection for 10 minutes.

## 3 EPP PROTOCOL

This section describes the interface relating to the EPP protocol described in RFC5730. This includes session management, poll message functionality and object mappings for domains, hosts and contacts.

### 3.1 Session Management

Session management refers to login and logout commands, used to authenticate and end a session with the SRS. The Login command is used to establish a session between the client and the server. This command succeeds when:

- The username supplied matches the Common Name in the digital certificate used in establishing the TLS session.
- The provided password is valid for the user.
- The user's access to the system isn't suspended.

The Logout command is used to end an active session. On processing a logout the server closes the underlying connection. The Hello command can be used as a session keep-alive mechanism.

### 3.2 Service Messages

Offline notifications pertaining to certain events are stored in a queue. The client is responsible for polling this queue for new messages and to acknowledge read messages. Messages include notification about server modification of sponsored objects, transfer operations, and balance thresholds.

## 4 EPP OBJECT MAPPINGS

This section covers the interface for the 3 core EPP objects; domain, host and contact objects, as per RFC5731, 5732, & 5733 respectively.

The EPP domain, contact and host object mapping describes an interface for the check, info, create, delete, renew (domain only), transfer (domain & contact only) and update commands. For domain objects the server doesn't support the use of host attributes as described by RFC5731, but rather uses host objects as described by RFC5731 and RFC5732. Details of each command are:

- check command: checks availability of 1 or more domain, contact or host objects in the SRS. Domain names will be shown as unavailable if in use, invalid or reserved, other objects will be unavailable if in use or invalid.
- info command: retrieves the information of an object provisioned in the SRS. Full information is returned to the sponsoring client or any client that provides authorisation information for the object. Non-sponsoring clients are returned partial information (no more than is available in the WhoIs).
- create command: provisions objects in the SRS. To ascertain whether an object is available for provisioning, the same rules for the check command apply.
- delete command: begins the process of removing an object from the SRS. Domain names transition into the redemption period and any applicable grace periods are applied. Domain names within the Add Grace Period are purged immediately. All other objects are purged immediately if they are not linked.
- renew command (domain only): extends the registration period of a domain name. The renewal period must be between 1 to 10 years inclusive and the current remaining registration period, plus the amount requested in the renewal mustn't exceed 10 years.
- transfer command (domain and contact only): provides several operations for

the management of the transfer of object sponsorship between clients. Clients that provide correct authorisation information for the object can request transfers. Domain names may be rejected from transfer within 60 days of creation or last transfer. The requesting client may cancel the transfer, or the sponsoring client may reject or approve the transfer. Both the gaining and losing clients may query the status of the current pending or last completed transfer.

- update command: updates authorisation information, delegation information (domains), and registration data pertaining to an object.

## 5 NON-PROPRIETARY EPP MAPPINGS

ARI's EPP service implements 2 non-proprietary EPP mappings, to support the required domain name lifecycle and to provide & manage DNSSEC information. The relevant schema documents aren't provided as they are published as RFCs in the RFC repository.

### 5.1 Grace Period Mapping

The Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (as per RFC 3915) is used to support the domain name lifecycle as per existing TLDs. The update command is extended by the restore command to facilitate the restoration of previously deleted domains in the redemption period. This command defines 2 operations, request & report, described here:

- Request operation: requests the restoration of a domain.
- Report operation: completes the restoration by specifying the information supporting the restoration of the domain. The restore report must include a copy of the WhoIs information at both the time the domain was deleted & restored, including the restore reason.

### 5.2 DNSSEC Mapping

The Domain Name System (DNS) Security Extensions Mapping for EPP, as per RFC5910, is used to support the provisioning of DNS Security Extensions. ARI requires clients use the Key Data interface. Clients may associate a maximum of 4 keys per domain. The registry system generates the corresponding DS data using the SHA-256 digest algorithm for the domain and any active variant domains.

ARI is aware of issues DNSSEC causes when transferring DNS providers - a transfer of Registrar usually means a change in DNS provider. DNSSEC key data won't be removed from the SRS or the DNS if a transfer occurs. It is the responsibility of and requires the cooperation of the registrant, Registrars, and DNS providers, to provide a seamless transition. ARI observes progress with this issue and implements industry agreed solutions as available. DNSSEC information is included in info responses when the secDNS namespace in login.

## 6 PROPRIETARY MAPPING

The registry system supports 3 additional EPP extensions where no published standard for the required functionality exists. Developed to conform to the requirements specified in RFC3735, these extensions include the provisioning of Internationalised Domain Names and domain name variants, and the association of arbitrary data with a domain name. These 3 extensions are introduced below, and further described in the attached schema documentation.

### 6.1 Internationalised Domain Names

ARI has developed an extension to facilitate the registration and management of Internationalised Domain Names as per RFCs 5890-5893 (collectively known as the IDNA 2008 protocol). This extension extends the domain create command and the info response.

The create command is extended to capture the language table identifier that identifies the corresponding IDN language table for the domain name.

Additionally the extension requires the Unicode form to avoid an inconsistency with DNS-form, as per RFC 5891.

The domain info command is extended to identify the language tag and Unicode form provided in the initial create command. This information is disclosed to

all querying clients that provided the extension namespace at login. This extension is documented in the attachment 'Q25 - idnadomain-1.0.pdf'.

### 6.2 Variant

ARI has developed an extension to facilitate the management of Domain Name variants. This extension extends the domain update command and the domain create and info responses. The domain update command is extended to allow the addition (activation) and removal (de-activation) of domain name variants subject to registry operator policy.

The domain create and info responses are extended to return the list of activated domain name variants. This information is disclosed to all querying clients that provided the extension namespace at login. The extension is documented in the attachment 'Q25 - variant-1.1.pdf'.

### 6.3 Key-Value

ARI has developed an extension to facilitate the transport of arbitrary data between clients and the SRS without the need for developing EPP Extensions for each specific use-case. This extension extends the domain create and domain update transform commands and the domain info query command. This extension is documented in the attachment 'Q25 - kv-1.0.pdf'.

## 7 ADDITIONAL SECURITY

The registry system provides additional mechanisms to support a robust interface. The use of command rate limiting enables the registry to respond to and withstand erroneous volumes of commands, while a user permission model provides fine-grained access to the EPP interface. These 2 mechanisms are described below.

### 7.1 Rate Limiting

The registry system supports command and global rate limits using a token-bucket algorithm. Limits apply to each connection to ensure fair and equitable use by all. Clients that exceed limits receive a command failed response message indicating breach of the limit.

### 7.2 User Permission Model

The registry system supports a fine-grained permission model controlling access to each specific command. By default, clients receive access to all functionality; however it is possible to remove access to a specific command in response to abuse or threat to stability of the system. Clients that attempt a command they have lost permission to execute, receive an EPP command failed response indicating loss of authorisation.

## 8 COMPLIANCE

Compliance with EPP RFCs is achieved through design and quality assurance (QA). The EPP interface was designed to validate all incoming messages against the respective XML Schema syntax. The XML Schema is copied directly from the relevant RFCs to avoid any ambiguity on version used. Inbound messages that are either malformed XML or invalid are rejected with a 2400 response. Outbound messages are validated against the XML Schema, and if an invalid response is generated, it is replaced with a known valid pre-composed 2400 response, and logged for later debugging.

A QA process provides confidence that changes don't result in regressions in the interface. Automated build processes execute test suites that ensure every facet of the EPP service (including malformed input, commands sequencing and synchronisation, and boundary values) is covered and compliant with RFCs and the EPP service specification. These tests are executed prior to committing code and automatically nightly. The final deliverable is packaged and tested again to ensure no defects were introduced in the packaging process.

New versions of the EPP Service follow a deployment schedule. The new version is deployed into an OT&E environment for Registrar integration testing.

Registrars are encouraged during this stage to test their systems operate correctly. After a fixed time in OT&E without issue, new versions are scheduled



for production deployment. This ensures incompatibilities with RFCs that made it through QA processes are detected in test environments prior reaching production.

ARI surveys Registrars for information about the EPP client toolkit. These surveys indicated that while many Registrars use ARI toolkits, several Registrars use either their own or that from another registry. The ability for Registrars to integrate with the ARI EPP service without using the supplied toolkit indicates the service is compliant with RFCs.

ARI is committed to providing an EPP service that integrates with third party toolkits and as such tests are conducted using said toolkits. Any issues identified during testing fall into the following categories:

- Third-party toolkit not compliant with EPP
- EPP service not compliant with EPP
- Both third-party toolkit and EPP service are compliant, however another operational issue causes an issue

Defects are raised and change management processes are followed. Change requests may also be raised to promote integration of third-party toolkits and to meet common practice.

## 9 CAPACITY

This TLD is projected to reach 150000 domains at its peak volume and will generate 105 EPP TPS. This will consume 0,75% of the EPP resources. ARI's SRS can easily accommodate this TLD. This was described in considerable detail in the capacity section of question 24.

## 10 RESOURCES

This function will be performed by ARI. ARI provides a technical support team to support Registrars and also provides Registrars with a tool kit (in Java and C++) implementing the EPP protocol. Normal operations for all registry services are managed by ARI's Production Support Group (PSG), who ensure the EPP server is available and performing appropriately.

Faults relating to connections with or functionality of the EPP server are managed by PSG. ARI monitors EPP availability and functionality as part of its monitoring practices, and ensures PSG staff are available to receive fault reports from Registrars any time. PSG has the appropriate network, Unix and application (EPP and load balancing) knowledge to ensure the EPP service remains accessible and performs as required. These ARI departments support EPP:

- Products and Consulting Team (7 staff)
- Production Support Group (27 staff)
- Development Team (11 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q25 - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system. Based on past experience ARI estimates that existing staff are adequate to support a registry system that supports in excess of 50M domains. Since this TLD projects 150000 domains, 0,3% of these resources are allocated to this TLD. See attachment 'Q25 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required, trained resources can be added to any of the above teams with a 2-month lead time.

### 10.1 Team Details

The products and consulting team is responsible for product management of the

EPP solution, and works with clients and industry to identify required system features or changes. The team consists of:

- 1 Products and Consulting Manager
- 1 Product Manager
- 1 Technical Product Manager
- 4 Domain Name Industry Consultants

The Production Support Group (PSG) is responsible for the design, deployment and maintenance of the EPP infrastructure including capacity planning, monitoring, and security. This team ensures the EPP services are available and performing appropriately. The team consists of:

- Production Support Manager
- Service Desk:
  - 1 Level 1 Support Team Lead
  - 8 Customer Support Representatives (Level 1 support)
  - 1 Level 2 Support Team Lead
  - 4 Registry Specialists (Level 2 support)
- Operations (Level 3 support):
  - 1 Operations Team Lead
  - 2 Systems Administrators
  - 2 Database Administrators
  - 2 Network Engineers
- Implementation:
  - 1 Project Manager
  - 2 Systems Administrators
  - 1 Database Administrator
  - 1 Network Engineer

The development team is responsible for EPP changes and features, bug fixes and issue diagnosis. The team consists of:

- 1 Development Manager
- 2 Business Analysts
- 6 Developers
- 2 Quality Analysts

These resources sufficiently accommodate the needs of this TLD, and are included in ARI's fees as described in our financial responses.

## 26. Whois

The Applicant has engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q26 - ARI Background & Roles.pdf'. This response describes the WhoIs interface as implemented by ARI.

### 1 INTRODUCTION

ARI's WhoIs service is for all domain names, contacts, nameservers and Registrars provisioned in the registry database. This response describes the port 43 and web interfaces of WhoIs, security controls to mitigate abuse, compliance with bulk access requirements for registration data, and the architecture delivering the service.

### 2 PORT 43 WHOIS SERVICE

WhoIs is on TCP port 43 in accordance with RFC3912. Requests are made in semi-free text format and ended by CR & LF. The server responds with a semi-free text format, terminating the response by connection close.

To support IDNs and Localised data we assume the query is encoded in UTF-8 and sends responses encoded in UTF-8. UTF-8 is backwards compatible with the ASCII charset and its use is consistent with the IETF policy on charsets as defined

in BCP 18 [<http://tools.ietf.org/html/bcp18>].

### 2.1 Query Format

By default WhoIs searches domains. To facilitate the queries of other objects keywords must be used. Supported keywords are:

- Domain
- Host/Nameserver
- Contact
- Registrar

Keywords are case-insensitive. The rest of the input is the search string. Wildcard chars may be used in search strings to match zero or more chars (%), or match exactly one char(\_). Wildcard chars must not be in the first 5 chars.

### 2.2 Response Format

The response follows a semi-structured format of object-specific data, followed by query-related meta-information, then a disclaimer.

The object-specific data is represented by key/value pairs, beginning with the key, followed by a colon and a space then the value terminated by an ASCII CR & LF. Where no object is found 'No Data Found' is returned.

The meta-information is used to identify data freshness and indicate when limits have been exceeded. It appears on one line within ' > > > ' and ' < < < ' chars.

The legal disclaimer is presented without leading comment marks wrapped at 72 chars. This format is consistent with that in the registry agreement.

### 2.3 Domain Data

Domain data is returned in response to a query with the keyword omitted, or with the 'domain' keyword. Domain queries return information on domains that are provisioned in the registry database.

The IDN domains may be specified in either the ASCII-compatible encoded form or the Unicode form. Clients are expected to perform any mappings, in conformance with relevant guidelines such as those specified in RFC5894 and UTS46.

Variant domains may be specified in the search string and WhoIs will match (using case-insensitive comparison) and return information for the primary registered domain.

For queries containing wildcard chars, if only one domain name is matched its details are returned, if more than one domain name is matched then the first 50 matched domain names are listed.

#### 2.3.1 Internationalised Domain Names

The WhoIs response format, prescribed in Specification 4, does not provide a mechanism to identify active variant domain names. ARI will include active variant domain names in WhoIs responses until a common approach for handling and display of variant names is determined.

#### 2.3.2 Reserved Domain Names

Domain names reserved from allocation will have a specific response that indicates the domain is not registered but also not available.

### 2.4 Nameserver Data

Nameserver data is returned in response to a query where the 'nameserver' or 'host' keywords have been used. Nameserver queries return information on hosts that are provisioned in the registry.

The search string for a nameserver query can be either a hostname or IP.

Queries using the hostname produce one result unless wildcards are used.

Queries using the IP produce one or more results depending on the number of hostnames that match that address. Queries for the hostname are matched case-insensitively.

The quad-dotted notation is expected for IPv4 and the RFC3513 - IPv6 Addressing Architecture format for IPv6. Wildcards cannot be used for IP queries.

### 2.5 Contact Data

Contact data is returned in response to a query where the 'contact' keyword was used. Contact queries return information on contacts that are provisioned in

the registry.

The search string for a contact query is the contact identifier. Contact identifiers are matched using a case-insensitive comparison. Wildcards cannot be used.

#### 2.6 Registrar Data

Registrar data is returned in response to a query where the 'Registrar' keyword was used. Registrar queries return information on Registrar objects that are provisioned in the registry.

The search string for a Registrar query can be name or IANA ID. Queries using the name or the IANA ID produce only one result. Queries for the name are matched using a case-insensitive comparison. Wildcards cannot be used.

#### 2.7 Non-standard Data

The SRS supports domain-related data beyond that above. It may include information used to claim eligibility to participate in the sunrise process, or other arbitrary data collected using the Key-Value Mapping to the EPP. This information will be included in the WhoIs response after the last object-specific data field and before the meta-information.

### 3 WEB-BASED WHOIS SERVICE

WhoIs is also available via port 80 using HTTP, known as Web-based WhoIs. This interface provides identical query capabilities to the port 43 interface via an HTML form.

### 4 SECURITY CONTROLS

WhoIs has an in-built mechanism to blacklist malicious users for a specified duration. Blacklisted users are blocked by source IP address and receive a specific blacklisted notification instead of the normal WhoIs response. Users may be blacklisted if ARI's monitoring system determines excessive use. A whitelist is used to facilitate legitimate use by law enforcement agencies and other reputable entities.

### 5 BULK ACCESS

The registry system complies with the requirements for the Periodic Access to Thin Registration Data and Exceptional Access to Thick Registration Data as described in Specification 4.

#### 5.1 Periodic Access to Thin Registration Data

ARI shall provide ICANN with Periodic Access to Thin Registration Data. The data will contain the following elements as specified by ICANN. The format of the data will be consistent with the format specified for Data Escrow. The Escrow Format prescribes an XML document encoded in UTF-8. The generated data will be verified to ensure that it is well formed and valid.

The data will be generated every Monday for transactions committed up to and on Sunday unless otherwise directed by ICANN. The generated file will be made available to ICANN using SFTP. Credentials, encryption material, and other parameters will be negotiated between ARI and ICANN using an out-of-band mechanism.

#### 5.2 Exceptional Access to Thick Registration Data

If requested by ICANN, ARI shall provide exceptional access to thick registration data for a specified Registrar. The data will contain full information for the following objects:

- Domain names sponsored by the Registrar
- Hosts sponsored by the Registrar
- Contacts sponsored by the Registrar
- Contacts linked from domain names sponsored by the Registrar

As above the format of the data will be consistent with the format specified for Data Escrow. And will be made available to ICANN using SFTP.

## 6 CAPACITY

ARI's WhoIs infrastructure is built to sustain 20M domain names. Based on ARI's experience running a high volume ccTLD registry (.au) and industry analysis, ARI were able to calculate the conservative characteristics of a registry of this size.

Through conservative statistical analysis of the .au registry and data presented in the May 2011 ICANN reports for the .com & .net, .org, .mobi, .info, .biz and .asia [<http://www.icann.org/en/resources/registries/reports>] we know there is:

- An average of 30 SRS txs per domain, per month.

Which indicates an expected monthly transaction volume of 600M txs?

Through statistical analysis of the .au registry and backed up by the data published in the .net RFP responses [<http://archive.icann.org/en/tlds/net-rfp/net-rfp-public-comments.htm>] we also know:

- The peak daily transactions is 6% of the monthly total
- The peak 5 min is 5% of the peak day

Thus we expect a peak WhoIs tx rate of WhoIs 6,000 TPS.

For perspective on the conservativeness of this, the following numbers were taken from data in the May 2011 ICANN reports referenced above:

- .info ~7.8M domain names, peaks at ~1,300 TPS (projected peak TPS of ~3,400 with 20M names).
- .mobi ~1M domain names, peaks at ~150 TPS (projected peak TPS of ~3,000 TPS with 20M names).
- .org ~9.3M domain names, peaks at ~1,300 TPS (projected peak TPS of ~2,800 with 20M names).

ARI understand the limitations of these calculations but they serve as a best estimate of probable transaction load. ARI has built overcapacity of resources to account for limitations of this method, however as conservative numbers were used and these are greater than real world observations, we are confident these capacity numbers are sufficient.

ARI benchmarked their WhoIs infrastructure and used the results to calculate the required computing resources for each of the tiers within the WhoIs architecture - allowing ARI to accurately estimate the required CPU, IOPS, storage and memory requirements for each server within the architecture, as well as the network bandwidth and packet throughput requirements for the anticipated WhoIs traffic. These capacity numbers were then doubled to account for unanticipated traffic spikes, errors in predictions and head room for growth. The technical resource allocations are explored in question 32.

This TLD is projected to reach 150000 domains at its peak volume and will generate 45 WhoIs transactions per second. This will consume 0,75% of the resources of the WhoIs infrastructure. As is evident ARI's WhoIs can easily accommodate this TLD's growth plans. See attachment 'Q26 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI expects to provide Registry services to 100 TLDs and a total of 12M domains by end of 2014. With all the TLDs and domains combined, ARI's WhoIs infrastructure will be only 60% utilized. The WhoIs infrastructure capacity can also be easily scaled as described in question 32

## 7 ARCHITECTURE

WhoIs uses a database separate from the SRS database as it operates from the secondary site such that network and database resources are decoupled from the operation of the SRS. Oracle Data Guard ensures the two databases are synchronised in real-time. The WhoIs service is operated live from the SRS 'failover' site, with the SRS 'primary' site serving as the 'failover' site for the WhoIs service. Both sites have enough capacity to run both services simultaneously, however by separating them, in normal operating modes headroom above the already over provisioned capacity is available. The architecture and data flow diagrams are described below and shown in the attachment 'Q26 - WhoIs.pdf'.

Traffic enters the network from the Internet through border routers and then firewalls. All traffic destined for this service except for TCP ports 43, 80 & 443 is blocked. Load balancers forward the request to one of the application

servers running ARI built WhoIs software. Each server is connected to the database cluster through another firewall further restricting access to the. Each server uses a restricted Oracle user that has read only access to the registry data and can only access the data that is relevant to the WhoIs queries. This ensures that in the unlikely event of an application server compromise the effects are limited.

All components are configured and provisioned to provide N+1 redundancy. Multiple Internet providers with separate upstream bandwidth suppliers are used. At least one additional component of all hardware exists, enabling maintenance without downtime. This configuration provides a service exceeding the availability requirements in Specification 10.

The use of load balancing allows addition of application servers with no downtime. From a database perspective, the ability to scale is enabled by utilising Oracle RAC database clustering. The entire service, including routers, firewalls and application is IPv6 compatible and WhoIs is offered on both IPv4 and IPv6. Detail about this architecture is available in our response to Question 32.

#### 7.1 Synchronisation

The WhoIs database is synchronised with the SRS database using Oracle Data Guard. Committed transactions in the SRS database are reflected in the WhoIs database in real-time. Should synchronisation break, WhoIs continues to operate with the latest available data until the issue is reconciled. The channel between the two sites consists of two independent dedicated point to point links as well as the Internet. Replication traffic flows via the dedicated links or if both links fail replication traffic flows over Internet tunnels.

#### 7.2. Interconnectivity with Other Services

The WhoIs service is not directly interconnected with other registry services or systems. The software has been developed to provide the WhoIs service exclusively and retrieve response information from a database physically separate to the SRS transactional database. This database is updated as described in 'Synchronisation' above. Although for smaller system the WhoIs and SRS can be configured to use the same data store. The WhoIs servers log every request to a central repository that is logically separate from the WhoIs database. This repository is used for query counts, detection of data mining and statistical analysis on query trends.

#### 7.3 IT and Infrastructure Resources

The WhoIs service is provided utilizing Cisco networking equipment, IBM servers & SAN. They are described in the attachment 'Q26 - WhoIs.pdf'. For more information on the architecture including server specifications and database capabilities please see Questions 32 & 33.

### 8 COMPLIANCE

Compliance with WhoIs RFCs is achieved through design and QA. The WhoIs interface was designed to conform to the RFCs as documented and independent test cases have been developed.

QA processes provide confidence that any changes to the service don't result in regression of the WhoIs. Automated build processes execute test suites that ensure every facet of the WhoIs service (including malformed input, commands sequencing and synchronisation, and boundary values) is covered and compliant with RFCs. These tests are executed prior to the committing of code and nightly. The final deliverable is packaged and tested again to ensure no defects were introduced in the packaging of the software.

New versions of the WhoIs follow a deployment schedule. The new version is deployed into an OT&E environment for Registrar integration testing. Registrars who rely on WhoIs functionality are encouraged during this stage to test their systems operate without change. After a fixed time in OT&E without issue, new versions are scheduled for production deployment. This ensures incompatibilities with RFCs that made it through QA processes are detected in test environments prior to reaching production.

ARI is committed to providing a WhoIs service that integrates with third party

tools and as such tests are conducted using these tools such as jWhoIs, a popular UNIX command line WhoIs client. Any issues identified during integration fall into 1 of the following categories:

- Third-party tool not compliant with the WhoIs specification
- WhoIs service not compliant
- Both third-party tool and WhoIs service are compliant, however another operational issue causes a problem

Defects are raised and follow the change management. Change requests may also be raised to promote integration of third-party tools and to meet common practice.

## 9 RESOURCES

This function will be performed by ARI. The WhoIs system is supported by a number of ARI departments:

- Products and Consulting Team (7 staff)
- Production Support Group (27 staff)
- Development Team (11 staff)
- Legal, Abuse and Compliance Team (6 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q26 - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system. Based on past experience ARI estimates that the existing staff is adequate to support a registry system that supports in excess of 50M domains. Since this TLD projects 150000 domains, 0,3% of these resources are allocated to this TLD. See attachment 'Q26 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

The products and consulting team is responsible for product management of the WhoIs solution including working with clients and the industry to identify new features or changes required to the system. The team consists of:

- 1 Products and Consulting Manager
- 1 Product Manager
- 1 Technical Product Manager
- 4 Domain Name Industry Consultants

ARI employ a development team responsible for the maintenance and continual improvement of the WhoIs software. The team consists of:

- 1 Development Manager
- 2 Business Analysts
- 6 Developers
- 2 Quality Analysts

ARI's Production Support Team ensures the successful operation of the WhoIs system. The team comprises Database Administrators, Systems Administrators and Network Administrators. This team routinely checks and monitors bandwidth, disk and CPU usages to plan and respond to expected increases in the volume of queries, and perform maintenance of the system including security patches and failover and recovery testing. The team consists of:

- Production Support Manager
- Service Desk:
  - 1 Level 1 Support Team Lead
  - 8 Customer Support Representatives (Level 1 support)
  - 1 Level 2 Support Team Lead
  - 4 Registry Specialists (Level 2 support)
- Operations (Level 3 support)

- 1 Operations Team Lead
- 2 Systems Administrators
- 2 Database Administrators
- 2 Network Engineers
- Implementation
  - 1 Project Manager
  - 2 Systems Administrators
  - 1 Database Administrators
  - 1 Network Engineers

ARI's registry provides abuse monitoring detection mechanisms to block data mining. ARI support staff may be contacted to remove blacklisted users during which they may be referred to the Legal, Abuse and Compliance Team for evaluation of their activities. Additionally the support team in conjunction with the Legal, Abuse and Compliance team administer requests for listing on the whitelist. The team consists of:

- 1 Legal Manager
- 1 Legal Counsel
- 4 Policy Compliance Officers

These resources sufficiently accommodate the needs of this TLD, and are included in ARI's fees as described in our Financial responses.

## 27. Registration Life Cycle

The Applicant has engaged ARI to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q27 - ARI Background & Roles.pdf'. This response describes the Registration Lifecycle as implemented by ARI.

### 1 INTRODUCTION

The lifecycle described matches current gTLD registries. All states, grace periods and transitions are supported by the EPP protocol as described in RFC5730 - 5734 & the Grace Period Mapping published in RFC3915. An overview is in attachment 'Q27 - Registration Lifecycle.pdf'.

### 2 REGISTRATION PERIODS

The registry supports registration up to 10 years and renewals for 1 to 10 years. The total current validity period can't exceed 10 years. Transfers under part A of the ICANN Policy on Transfer of Registrations between Registrars (Adopted 7 November 2008) extend registration by 1 year. The period truncates to 10 years if required.

### 3 STATES

The states that a domain can exist in are: Registered, Pending Transfer, Redemption, Pending Restore & Pending Delete.

All domain name statuses (RFC3915, 5730-5734 and 5910) are covered below

#### 3.1 Registered

EPP Status: ok

In DNS: Yes

Allowed Operations: Update, Renew, Transfer (request) & Delete

The default state of a domain - no pending operations. The sponsoring Registrar may update the domain.

#### 3.2 Pending Transfer

EPP Status: pendingTransfer



In DNS: Yes

Allowed Operations: Transfer (cancel, reject, approve)

Another Registrar has requested transfer of the domain and it is not yet completed. All transform operations, other than those to cancel, reject, or approve the transfer are rejected.

### 3.3 Redemption

EPP Status: pendingDelete

RGP Status: redemptionPeriod

In DNS: No

Allowed Operations: Restore (request)

Domain has been deleted. The sponsor may request restoration of the domain. The domain continues to be withheld from the DNS unless it is restored. No transform operations other than restore are allowed.

### 3.4 Pending Restore

EPP Status: pendingDelete

RGP Status: pendingRestore

In DNS: Yes

Allowed Operations: Restore (report)

A restore request is pending. The sponsor must submit a restore report. The domain is provisioned the DNS. No transform operations other than the restore report are allowed.

### 3.5 Pending Delete

EPP Status: pendingDelete

RGP Status: pendingDelete

In DNS: No

Allowed Operations: None

The Redemption Grace Period has lapsed and the domain is pending purge from the registry. This state prohibits the sponsor from updating, restoring or modifying the domain. This status applies for 5 days. At the end of this period the domain is purged from the database and made available for registration.

## 4 GRACE PERIODS

The registry system supports 4 grace periods: add, renew, auto-renew, and transfer, described below with consideration for overlap of grace periods. States described here are additional to those above.

### 4.1 Add Grace Period

Length: 5 days

RGP Status: addPeriod

Allows for the no-cost cancellation of a domain registrations resulting from typing mistakes and other errors by Registrars and registrants - beginning on the creation of a domain and lasting for 5 days. When the following operations are performed during this period these rules apply:

- Delete: the sponsoring Registrar, who must have created the domain, may delete the domain and receive a refund. The domain is deleted with immediate effect. The refund is subject to the Add Grace Period Limits consensus policy. Excess deletions over 50 or 10% of creates (whichever is greater), are not subject to a refund, except in extraordinary circumstances.

- Renew: the sponsor may renew the domain but does not receive any refund for the initial registration fee. The Registrar is charged for the renewal operation. The total period for the domain is the sum of the initial period in the create and any renewal term, limited to a 10 year maximum.

- Transfer: Under ICANN policy a transfer can't occur during the Add Grace Period or at any other time in the first 60 days after the initial registration. The registry system enforces this, rejecting such requests.

- Bulk Transfers: Under Part B of the ICANN Policy on Transfer of Registrations between Registrars, a bulk transfer can occur during the Add Grace Period. Any bulk transfer causes the Add Grace Period to not apply.

The Add Grace Period does not have any impact on other commands.

#### 4.2 Renew Grace Period

Length: 5 days

RGP Status: renewPeriod

Allows the sponsoring Registrar to undo a renewal via the deletion of a domain - beginning on the receipt of a renewal command and lasting for 5 days. If any of the following operations are performed during this period these rules apply:

- Delete: the sponsoring Registrar, who must have initiated the renewal, may delete the domain and receive a renewal fee refund. The extension to the registration period caused by the preceding renew is reversed and unless the domain is also in the Add Grace Period, the domain enters the Redemption state. If also in the Add Grace Period it is deleted with immediate effect and availability for registration.

- Renew: the sponsoring Registrar, who must have performed the initial renew, can subsequently renew the domain again, causing a second independent Renewal Grace Period to start. The Registrar is charged for the operation and the total registration period for the domain is extended by the renewal term, limited to the 10 year maximum.

- Transfer: an approved transfer command ends the current Renew Grace Period without a refund and begins a Transfer Grace Period.

- Bulk Transfers: bulk transfers cause the Renew Grace Period to end without a refund, consequently registration periods are not changed.

The Renew Grace Period has no impact on other commands.

#### 4.3 Auto-Renew Grace Period

Length: 45 days

RGP Status: autoRenewPeriod

Auto-Renew Grace Period allows for domains to remain in the DNS past registration expiration while giving adequate time for the sponsoring Registrar to obtain intention of renewal from the registrant.

This period begins on the expiration of the domain and lasts for 45 days. If any of the following are performed during this period these rules apply:

- Delete: the sponsoring Registrar, who must be the sponsor when the Auto-Renew Grace Period commenced, may delete the domain and receive an auto-renew fee refund. The registration period auto-renew extension is reversed and the domain enters the Redemption state.

- Renew: the sponsoring Registrar, who must be the sponsor when the auto-renew occurred, can renew the domain again causing an independent Renewal Grace Period to begin. The Registrar is charged and the registration period is extended by the renewal term, limited to the 10 year maximum.

- Transfer: an approved transfer command ends the current Auto-Renew Grace Period with a refund to the losing Registrar and begins a Transfer Grace Period. The registration period auto-renew extension is reversed and the registration is extended by the period specified in the transfer.

- Bulk Transfers: bulk transfers cause the Auto-Renew Grace Period to end without a refund consequently registration periods are not changed.

The Auto-Renew Grace Period does not have any impact on other commands.

#### 4.4 Transfer Grace Period

Length: 5 days

RGP Status: transferPeriod

Transfer Grace Period allows the sponsoring Registrar to undo the registration period extension (due to a transfer command), via the deletion of a domain.

This period begins on a transfer completion and lasts for 5 calendar days. If the following are performed during the period these rules apply:

- Delete: the sponsoring Registrar, who must have initiated the transfer, may delete the domain and receive a transfer fee refund. The extension to the registration period of the preceding transfer is reversed and the Redemption state is entered.

- Renew: the sponsoring Registrar can renew the domain thus causing an independent Renewal Grace Period to begin. The Registrar is charged and the registration period for the domain is extended by the renewal term, limited to the 10 year maximum.

- Transfer: under Part A of the ICANN Policy on Transfer of Registrations between Registrars a transfer may not occur during the 60 day period after

transfer (except in special circumstances). The registry system enforces this - effects of transfer do not require consideration. Should a special situation require transfer back to the losing Registrar, this is dealt with by taking into account the specific situation. The registry system does not allow this without intervention by registry staff.

- Bulk Transfers: bulk transfers cause the Transfer Grace Period to end without a refund; consequently registration periods are not changed. The Transfer Grace Period does not have any impact on other commands.

#### 4.5 Redemption Grace Period

Length: 30 days

RGP Status: as described in Redemption state

Redemption Grace Period refers to the period of time the domain spends in the Redemption state, starting after a domain is deleted. The Redemption state description provides information on operations during this period.

#### 4.6 Overlap of Grace Periods

The 4 possible overlapping grace periods are:

- Add Grace Period with 1 or more Renew Grace Periods.
- Renew Grace Period with 1 or more other Renew Grace Periods.
- Transfer Grace Period with 1 or more Renew Grace Periods.
- Auto-Renew Grace Period with 1 or more Renew Grace Periods.

These are treated independently with respect to timelines however action that is taken has the combined effects of all grace periods still current.

##### 4.6.1 Transfer Clarification

If several billable operations, including a transfer, are performed on a domain and it is deleted in the operations' grace periods, only those operations performed after/including the latest transfer are eligible for refund.

## 5 TRANSITIONS

### 5.1 Available > Registered

Triggered by the receipt of a create command to register the domain. The sponsoring Registrar is charged for the creation amount. This transition begins the Add Grace Period.

### 5.2 Registered > Pending Transfer

Triggered by the receipt of a request transfer command. The transfer must result in domain registration extension - the gaining Registrar is charged for the transfer. Requests to transfer the domain within 60 days of creation or a previous transfer are rejected. As per '4.4 Transfer Grace Period', exceptions specified in ICANN's Transfer Policy apply - dealt with individually.

### 5.3 Pending Transfer > Registered

Triggered by 1 of 4 operations:

- Operation 1 (Cancel): during the Pending Transfer period the gaining Registrar may cancel the transfer by issuing a cancel transfer command. The gaining Registrar is refunded the transfer fee, the registration period remains unchanged and all existing grace periods at the time of transfer request remain in effect.
- Operation 2 (Reject): during the Pending Transfer period the losing Registrar may reject the transfer by issuing a reject transfer command. The gaining Registrar is refunded the transfer. The registration period remains unchanged and all grace periods existing at the time of transfer request remain in effect if not elapsed.
- Operation 3 (Approve): During the Pending Transfer period the losing Registrar may approve the transfer by issuing an approve transfer command. If the transfer was requested during the Auto-Renew Grace Period, the extension to the registration period is reversed and the losing Registrar is refunded the auto-renew. The registration period is extended by the amount specified in the transfer request. This begins the Transfer Grace Period.
- Operation 4 (Auto-Approve): If after 5 days, no action has been taken, the system approves the transfer. If the transfer was requested during the Auto-

Renew Grace Period the extension to the registration period is reversed and the losing Registrar is refunded the auto-renew. The registration period is extended by the amount specified in the transfer request. This begins the Transfer Grace Period.

#### 5.4 Registered ) Deleted

On receipt of a delete command if the domain is in the Add Grace Period, it is purged from the Database and immediately available for registration. Renew Grace Period may also be in effect.

#### 5.5 Registered ) Redemption

On receipt of a delete command if the domain is not in the Add Grace Period, it transitions to the Redemption Period state and all grace periods in effect are considered.

#### 5.6 Redemption ) Pending Restore

On receipt of a restore command if the Redemption Period has not lapsed, the domain transitions to the Pending Restore state. The domain is provisioned in the DNS. The sponsoring Registrar is charged a fee for the restore request.

#### 5.7 Pending Restore ) Registered

During the Pending Restore period the sponsoring Registrar may complete the restore via a restore report containing the WhoIs information - submitted prior to the deletion, the WhoIs information at the time of the report, and the reason for the restoration.

#### 5.8 Pending Restore ) Redemption

Seven calendar days after the transition to the Pending Restore state, if no restore report is received the domain transitions to the Redemption state, which begins a new redemption period. The domain is removed from the DNS. The restore has no refund.

#### 5.9 Redemption ) Pending Delete

Thirty calendar days after the transition to the Redemption state, if no restore request is received the domain transitions to the Pending Delete state.

#### 5.10 Pending Delete ) Deleted

Five calendar days after the transition to the Pending Delete state, the domain is removed from the Database and is immediately available for registration.

## 6 LOCKS

Locks may be applied to the domain to prevent specific operations occurring. The sponsoring Registrar may set the locks prefixed with 'client' while locks prefixed with 'server' are added and removed by the registry operator. Locks are added and removed independently but they can be combined to facilitate the enforcement of higher processes, such as 'Registrar Lock', and outcomes required as part of UDRP. All locks are compatible with EPP RFCs. The available locks are:

- clientDeleteProhibited, serverDeleteProhibited - Requests to delete the object are rejected
- clientHold, serverHold - DNS information is not published
- clientRenewProhibited, serverRenewProhibited - Requests to renew the object are rejected. Auto-renew is allowed
- clientTransferProhibited, serverTransferProhibited - Requests to transfer the object are rejected
- clientUpdateProhibited, serverUpdateProhibited - Requests to update the object are rejected, unless the update removes this status

## 7 SPECIAL CONSIDERATIONS

### 7.1 ICANN-Approved Bulk Transfers

ICANN-Approved Bulk Transfers do not follow the typical transfer lifecycle. Existing grace periods are invalidated and no refunds are credited to the

losing Registrar. The prohibition of transfer period on domains created or transferred within 60 days does not apply.

## 7.2 Uniform Rapid Suspension

In the Uniform Rapid Suspension (URS) process, as described in the 'gTLD Applicant Guidebook' 11th January 2012, the following modification to the above processes is required.

Remedy allows for the addition of a year to the registration period, limited to the 10 year maximum. During this time no transform operations may be performed other than to restore the domain as allowed by Appeal. At the expiration of the registration period the domain is not automatically renewed, but proceeds to the Redemption state as per the lifecycle described above, and it is not eligible for restoration.

## 8 UPDATE/DNS

The update command does not impact the state of the domain through the Registration Lifecycle, however the command can be used to add and remove delegation information, which changes the DNS state of the domain. A domain is required to have 2 or more nameservers published in the DNS. An update that results in a domain having less than 2 nameservers removes the domain from the DNS. An exception is when 1 nameserver remains assigned to a domain due to deletion of its other nameservers due to purge of their parent domain. The next update that modifies delegation information ends the exception and from then on the domain requires 2 nameservers be in the DNS.

## 9 RESOURCES

This function will be performed by ARI. ARI's registry performs all time-based transitions automatically and enforces all other business rules - without requiring human resources for normal operation. If changes to the automatic behaviours or restrictions enforced by the policy system are required, ARI has a development team for this.

Domain Name Lifecycle aspects requiring human resources to manage are included in the ARI outsourcing include:

- Processing Add Grace Period exemptions as requested by Registrars.
- Processing restore reports provided by Registrars.
- Meeting the registry operator's obligations under ICANN's Transfer Dispute Policy.
- Performing exception processing in the case of approved transfers during the 60 day transfer prohibition window.

The Registration Lifecycle is designed, built, operated and supported by these ARI departments:

- Products and Consulting Team (7 staff)
- Legal, Abuse and Compliance Team (6 staff)
- Development Team (11 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q27 - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system. Based on past experience ARI estimates that the existing staff is adequate to support a registry system that supports in excess of 50M domains. Since this TLD projects 150000 domains, 0,3% of these resources are allocated to this TLD. See attachment 'Q27 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams

with a 2 month lead time.

The Products and Consulting team is responsible for product management of the Registration Lifecycle, including working with clients and the industry to identify new features or changes required to the system. The team consists of:

- 1 Products and Consulting Manager
- 1 Product Manager
- 1 Technical Product Manager
- 4 Domain Name Industry Consultants

Most manual tasks fall to the Legal, Abuse and Compliance team, with staff experienced in development of policy for policy rich TLD environments. They have the required legal and industry background to perform this function. The team consists of:

- 1 Legal Manager
- 1 Legal Counsel
- 4 Policy Compliance Officers

The automated aspects of the Registration lifecycle are supported by ARI's Domain Name Registry software. ARI has a development team for maintenance and improvement of the software. The team consist of:

- 1 Development Manager
- 2 Business Analysts
- 6 Developers
- 2 Quality Analysts

Information on these roles is in Resources in our response to Question 31.

These resources sufficiently accommodate the needs of this TLD, and are included in ARI's fees as described in our Financial responses.

## 28. Abuse Prevention and Mitigation

The Applicant has engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q28 - ARI Background & Roles.pdf'.

### 1 INTRODUCTION

The efforts that will be undertaken in this TLD to minimise abusive registrations and other activities that have a negative impact on Internet users are described below. We will be utilising the Anti-Abuse Service of our managed registry service provider, ARI. This service includes the implementation of our comprehensive Anti-Abuse Policy. This policy, developed in consultation with ARI, clearly defines abusive behaviour and identifies particular types of abusive behaviour and the mitigation response to such behaviour.

### 2 OVERVIEW

We have engaged ARI to deliver registry services for this TLD. ARI will, owing to their extensive industry experience and established anti-abuse operations, implement and manage on our behalf various procedures and measures adopted to mitigate the potential for abuse, identify abuse and handle identified abuse. ARI will forward to us all matters requiring determination by the registry operator which fall beyond the scope of ARI's Anti-Abuse Service. This is described below in the context of the implementation of our Anti-Abuse Policy. Despite utilisation of ARI's Anti-Abuse Service, we are nonetheless cognisant of our responsibility to minimise abusive registrations and other activities that have a negative impact on Internet users in the TLD. In recognition of this responsibility, we will play an instrumental role in overseeing the implementation of the Anti-Abuse Service by ARI. We will also have contractual commitments in the form of SLA's in place to ensure that ARI's delivery of the

Anti-Abuse Service is aligned with our strong commitment to minimise abuse in our TLD.

That strong commitment is further demonstrated by our adoption of many of the requirements proposed in the '2011 Proposed Security, Stability and Resiliency Requirements for Financial TLDs' (at <http://www.icann.org/en/news/correspondence/aba-bits-to-beckstrom-crocker-20dec11-en.pdf>) (the 'BITS Requirements'). We acknowledge that these requirements were developed by the financial services sector in relation to financial TLDs, but nevertheless believe that their adoption in this TLD (which is not financial-related) results in a more robust approach to combating abuse.

Consistent with Requirement 6 of the BITS Requirements, we will certify to ICANN on an annual basis our compliance with our Registry Agreement.

Please note that the various policies and practices that we have implemented to minimise abusive registrations and other activities that affect the rights of trademark holders are specifically described in our response to Question 29.

### 3 POLICY

In consultation with ARI we have developed a comprehensive Anti-Abuse Policy, which is the main instrument that captures our strategy in relation to abuse in the TLD.

#### 3.1 Definition of Abuse

Abusive behaviour in a TLD may relate to the core domain name-related activities performed by Registrars and registries including, but not limited to:

- The allocation of registered domain names.
- The maintenance of and access to registration information.
- The transfer, deletion, and reallocation of domain names.
- The manner in which the registrant uses the domain name upon creation.

Challenges arise in attempting to define abusive behaviour in the TLD due to its broad scope. Defining abusive behaviour by reference to the stage in the domain name lifecycle in which the behaviour occurs presents difficulty given that a particular type of abuse may occur at various stages of the life cycle. With this in mind, ARI has fully adopted the definition of abuse developed by the Registration Abuse Policies Working Group (Registration Abuse Policies Working Group Final Report 2010, at <http://gnso.icann.org/issues/rap/rap-wg-final-report-29may10-en.pdf>), which does not focus on any particular stage in the domain name life cycle.

Abusive behaviour in a TLD may be defined as an action that:

- causes actual and substantial harm, or is a material predicate of such harm.
- is illegal or illegitimate, or is otherwise considered contrary to the intention and design of the mission/purpose of the TLD.

In applying this definition the following must be noted:

1. The party or parties harmed, and the severity and immediacy of the abuse, should be identified in relation to the specific alleged abuse.
2. The term "harm" is not intended to shield a party from fair market competition.

3. A predicate is a related action or enabler. There must be a clear link between the predicate and the abuse, and justification enough to address the abuse by addressing the predicate (enabling action).

For example, WhoIs data can be used in ways that cause harm to domain name registrants, intellectual property (IP) rights holders and Internet users. Harmful actions may include the generation of spam, the abuse of personal data, IP infringement, loss of reputation or identity theft, loss of data, phishing and other cybercrime-related exploits, harassment, stalking, or other activity with negative personal or economic consequences. Examples of predicates to these harmful actions are automated email harvesting, domain name registration by proxy/privacy services to aid wrongful activity, support of false or misleading registrant data, and the use of WhoIs data to develop large email lists for commercial purposes. The misuse of WhoIs data is therefore considered abusive because it is contrary to the intention and design of the stated legitimate purpose of WhoIs data.

### 3.2 Aims and Overview of Our Anti-Abuse Policy

Our Anti-Abuse Policy will put registrants on notice of the ways in which we will identify and respond to abuse and serve as a deterrent to those seeking to register and use domain names for abusive purposes. The policy will be made easily accessible on the Abuse page of our registry website which will be accessible and have clear links from the home page along with FAQs and contact information for reporting abuse.

Consistent with Requirements 15 and 16 of the BITS Requirements, our policy:

- Defines abusive behaviour in our TLD.
- Identifies types of actions that constitute abusive behaviour, consistent with our adoption of the RAPWG definition of 'abuse'.
- Classifies abusive behaviours based on the severity and immediacy of the harm caused.
- Identifies how abusive behaviour can be notified to us and the steps that we will take to determine whether the notified behaviour is abusive.
- Identifies the actions that we may take in response to behaviour determined to be abusive.

Our RRA will oblige all Registrars to do the following in relation to the Anti-Abuse Policy:

- comply with the Anti-Abuse Policy; and
- include in their registration agreement with each registrant an obligation for registrants to comply with the Anti-Abuse Policy and each of the following requirements:

'operational standards, policies, procedures, and practices for the TLD established from time to time by the registry operator in a non-arbitrary manner and applicable to all Registrars, including affiliates of the registry operator, and consistent with ICANN's standards, policies, procedures, and practices and the registry operator's Registry Agreement with ICANN. Additional or revised registry operator operational standards, policies, procedures, and practices for the TLD shall be effective upon thirty days notice by the registry operator to the Registrar. If there is a discrepancy between the terms required by this Agreement and the terms of the Registrar's registration agreement, the terms of this Agreement shall supersede those of the Registrar's registration agreement'.

Our RRA will additionally incorporate the following BITS Requirements:

- Requirement 7: Registrars must certify annually to ICANN and us compliance with ICANN's Registrar Accreditation Agreement (RAA) our Registry-Registrar Agreement (RRA).
- Requirement 9: Registrars must provide and maintain valid primary contact information (name, email address, and phone number) on their website.
- Requirement 14: Registrars must notify us immediately regarding any investigation or compliance action, including the nature of the investigation or compliance action by ICANN or any outside party (eg law enforcement, etc.) along with the TLD impacted.
- Requirement 19: Registrars must disclose registration requirements on their website.

We will re-validate our RRAs at least annually, consistent with Requirement 10.

### 3.3 Anti-Abuse Policy

Our Anti-Abuse Policy is as follows:

#### Anti-Abuse Policy

##### Introduction:

The abusive registration and use of domain names in the TLD is not tolerated given that the inherent nature of such abuses creates security and stability issues for all participants in the Internet environment.

##### Definition of Abusive Behaviour:

Abusive behaviour is an action that:

- causes actual and substantial harm, or is a material predicate of such harm;
- or
- is illegal or illegitimate, or is otherwise considered contrary to the intention and design of the mission/purpose of the TLD.

A 'predicate' is an action or enabler of harm.



'Material' means that something is consequential or significant.

Examples of abusive behaviour falling within this definition:

- Spam: the use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of web sites and Internet forums. An example, for purposes of illustration, would be the use of email in denial-of-service attacks.
- Phishing: the use of a fraudulently presented web site to deceive Internet users into divulging sensitive information such as usernames, passwords or financial data.
- Pharming: the redirecting of unknowing users to fraudulent web sites or services, typically through DNS hijacking or poisoning, in order to deceive Internet users into divulging sensitive information such as usernames, passwords or financial data.
- Wilful distribution of malware: the dissemination of software designed to infiltrate or cause damage to devices or to collect confidential data from users without the owner's informed consent.
- Fast Flux hosting: the use of DNS to frequently change the location on the Internet to which the domain name of an Internet host or nameserver resolves in order to disguise the location of web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast flux hosting may only be used with prior permission of the registry operator.
- Botnet command and control: 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.
- Distribution of child pornography: the storage, publication, display and/or dissemination of pornographic materials depicting individuals under the age of majority in the relevant jurisdiction.
- Illegal access to other computers or networks: the illegal accessing of computers, accounts, or networks belonging to another party, or attempt to penetrate security measures of another individual's system (hacking). Also, any activity that might be used as a precursor to an attempted system penetration.

Detection of Abusive Behaviour:

Abusive behaviour in the TLD may be detected in the following ways:

- By us through our on-going monitoring activities and industry participation.
- By third parties (general public, law enforcement, government agencies, industry partners) through notification submitted to the abuse point of contact on our website, or industry alerts.

Reports of abusive behaviour will be notified immediately to the Registrar of record.

Handling of abusive behaviour:

When abusive behaviour is detected in our TLD through notification by a third party, a preliminary assessment will be performed in order to determine whether the notification is legitimately made. Applying the definitions of types of abusive behaviours identified in this policy, we will classify each incidence of legitimately reported abuse into one of two categories based on the probable severity and immediacy of harm to registrants and Internet users. These categories are provided below and are defined by reference to the action that may be taken by us. The examples of types of abusive behaviour falling within each category are illustrative only.

Category 1:

Probable Severity or Immediacy of Harm: Low

Examples of types of abusive behaviour: Spam, Malware

Mitigation steps:

1. Investigate
2. Notify registrant

Category 2:

Probable Severity or Immediacy of Harm: Medium to High

Examples of types of abusive behaviour: Fast Flux Hosting, Phishing, Illegal Access to other Computers or Networks, Pharming, Botnet command and control

Mitigation steps:

1. Suspend domain name
2. Investigate
3. Restore or terminate domain name

In the event that we receive specific instructions regarding a domain name from a law enforcement agency, government or quasi-governmental agency utilising the expedited process for such agencies, our mitigation steps will be in accordance with those instructions provided that they do not result in the contravention of applicable law. In addition, we will take all reasonable efforts to notify law enforcement agencies of abusive behaviour in our TLD which we believe may constitute evidence of a commission of a crime, eg distribution of child pornography.

Note that these expected actions are intended to provide a guide to our response to abusive behaviour rather than any guarantee that a particular action will be taken.

The identification of abusive behaviour in the TLD, as defined above, shall give us the right, but not the obligation, to take such actions in accordance with the following text in the RRA, which provides that the registry operator: '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, or instruct Registrars to take such an action as we deem necessary in our discretion to;

1. protect the integrity and stability of the registry;
2. comply with any applicable laws, government rules or requirements, requests of law enforcement, or dispute resolution process;
3. avoid any liability, civil or criminal, on the part of the registry operator, as well as its affiliates, subsidiaries, officers, directors, and employees, per the terms of the registration agreement; and
4. correct mistakes made by the registry operator or any Registrar in connection with a domain name registration.

We reserve the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

We also reserve the right to deny registration of a domain name to a registrant who has repeatedly engaged in abusive behaviour in our TLD or any other TLD. Registrars only and not Resellers may offer proxy registration services to private individuals using the domain name for non-commercial purposes. We may amend or otherwise modify this policy to keep abreast of changes in consensus policy or new and emerging types of abusive behaviour in the Internet.

Registrar's failure to comply with this Anti-Abuse Policy shall constitute a material breach of the RRA, and shall give rise to the rights and remedies available to us under the RRA.

#### 4 ABUSE PREVENTION AND MITIGATION

This section describes the implementation of our abuse related processes regarding:

- Building awareness of the Anti-Abuse Policy.
- Mitigating the potential for abusive behaviour.
- Identifying abusive behaviour.
- Handling abusive behaviour.

##### 4.1. Awareness of Policy

The Anti-Abuse Policy will be published on the Abuse page of our registry website, which will be accessible and have clear links from the home page. In addition, the URL to the Abuse page will be included in all email correspondence to the registrant, thereby placing all registrants on notice of the applicability of the Anti-Abuse Policy to all domain names registered in our TLD. The Abuse page will, consistent with Requirement 8 of the BITS Requirements, provide registry contact information (name, email address, and phone number) to enable the public to communicate with us about TLD policies. The Abuse page will emphasise and evidence our commitment to combating abusive registrations by clearly identifying what our policy on abuse is and what effect our implementation of the policy may have on registrants. We anticipate that this clear message, which communicates our commitment to combating abusive

registrations, will serve to minimise abusive registrations in our TLD.

#### 4.2 Pre-emptive - Mitigating of the Potential for Abuse

The following practices and procedures will be adopted to mitigate the potential for abusive behaviour in our TLD.

##### 4.2.1 ICANN Prescribed Measures

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

- DNSSEC deployment, which reduces the opportunity for pharming and other man-in-the-middle attacks. We will encourage Registrars and Internet Service Providers to deploy DNSSEC capable resolvers in addition to encouraging DNS hosting providers to deploy DNSSEC in an easy-to-use manner in order to facilitate deployment by registrants. DNSSEC deployment is further discussed in the context of our response to Question 43.
- Prohibition on Wild Carding as required by section 2.2 of Specification 6 of the Registry Agreement.
- Removal of Orphan Glue records (discussed below in '4.2.8 Orphan Glue Record Management').

##### 4.2.2 Increasing Registrant Security Awareness

In accordance with our commitment to operating a secure and reliable TLD, we will attempt to improve registrant awareness of the threats of domain name hijacking, registrant impersonation and fraud, and emphasise the need for and responsibility of registrants to keep registration (including WhoIs) information accurate. Awareness will be raised by:

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

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

##### 4.2.3 Mitigating the Potential for Abusive Registrations that Affect the Legal Rights of Others

Many of the examples of abusive behaviour identified in our Anti-Abuse Policy may affect the rights of trademark holders. While our Anti-Abuse Policy addresses abusive behaviour in a general sense, we have additionally developed specific policies and procedures to combat behaviours that affect the rights of trademark holders at start-up and on an ongoing basis. These include the implementation of a trademark claims service and a sunrise registration service at start-up and implementation of the UDRP, URS and PDDRP on an ongoing basis. The implementation of these policies and procedures serves to mitigate the potential for abuse in the TLD by ensuring that domain names are allocated to those who hold a corresponding trademark.

These policies and procedures are described in detail in our response to Question 29.

##### 4.2.4 Safeguards Against Allowing for Unqualified Registrations

The eligibility restrictions for this TLD are outlined in our response to Question 18.

Eligibility restrictions will be implemented contractually through our RRA, which will require Registrars to include the following in their Registration Agreements:

- Registrant warrants that it satisfies eligibility requirements.

Where applicable, eligibility restrictions will be enforced through the

adoption of the Charter Eligibility Dispute Resolution Policy or a similar policy, and Registrars will be obliged to require in their registration agreements that registrants agree to be bound by such policy and acknowledge that a registration may be cancelled in the event that a challenge against it under such policy is successful.

Providing an administrative process for enforcing eligibility criteria and taking action when notified of eligibility violations mitigates the potential for abuse. This is achieved through the risk of cancellation in the event that it is determined in a challenge procedure that eligibility criteria are not satisfied.

#### 4.2.5 Registrant Disqualification

As specified in our Anti-Abuse Policy, we reserve the right to deny registration of a domain name to a registrant who has repeatedly engaged in abusive behaviour in our TLD or any other TLD.

Registrants, their agents or affiliates found through the application of our Anti-Abuse Policy to have repeatedly engaged in abusive registration will be disqualified from maintaining any registrations or making future registrations. This will be triggered when our records indicate that a registrant has had action taken against it an unusual number of times through the application of our Anti-Abuse Policy. Registrant disqualification provides an additional disincentive for qualified registrants to maintain abusive registrations in that it puts at risk even otherwise non-abusive registrations, through the possible loss of all registrations.

In addition, nameservers that are found to be associated only with fraudulent registrations will be added to a local blacklist and any existing or new registration that uses such fraudulent NS record will be investigated.

The disqualification of 'bad actors' and the creation of blacklists mitigates the potential for abuse by preventing individuals known to partake in such behaviour from registering domain names.

#### 4.2.6 Restrictions on Proxy Registration Services

Whilst it is understood that implementing measures to promote WhoIs accuracy is necessary to ensure that the registrant may be tracked down, it is recognised that some registrants may wish to utilise a proxy registration service to protect their privacy. In the event that Registrars elect to offer such services, the following conditions apply:

- Proxy registration services may only be offered by Registrars and NOT resellers.
- Registrars must ensure that the actual WhoIs data is obtained from the registrant and must maintain accurate records of such data.
- Registrars must provide Law Enforcement Agencies (LEA) with the actual WhoIs data upon receipt of a verified request.
- Proxy registration services may only be made available to private individuals using the domain name for non-commercial purposes.

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

#### 4.2.7 Registry Lock

Certain mission-critical domain names such as transactional sites, email systems and site supporting applications may warrant a higher level of security. Whilst we will take efforts to promote the awareness of security amongst registrants, it is recognised that an added level of security may be

provided to registrants by 'registry locking' the domain name thereby prohibiting any updates at the registry operator level. The registry lock service will be offered to all Registrars who may request this service on behalf of their registrants in order to prevent unintentional transfer, modification or deletion of the domain name. This service mitigates the potential for abuse by prohibiting any unauthorised updates that may be associated with fraudulent behaviour. For example, an attacker may update nameservers of a mission-critical domain name, thereby redirecting customers to an illegitimate website without actually transferring control of the domain name.

Upon receipt of a list of domain names to be placed on registry lock by an authorised representative from a Registrar, ARI will:

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

#### 4.2.8 Orphan Glue Record Management

The ARI registry SRS database does not allow orphan records. Glue records are removed when the delegation point NS record is removed. Other domains that need the glue record for correct DNS operation may become unreachable or less reachable depending on their overall DNS service architecture. It is the registrant's responsibility to ensure that their domain name does not rely on a glue record that has been removed and that it is delegated to a valid nameserver. The removal of glue records upon removal of the delegation point NS record mitigates the potential for use of orphan glue records in an abusive manner.

#### 4.2.9 Promoting WhoIs Accuracy

Inaccurate WhoIs information significantly hampers the ability to enforce policies in relation to abuse in the TLD by allowing the registrant to remain anonymous. In addition, LEAs rely on the integrity and accuracy of WhoIs information in their investigative processes to identify and locate wrongdoers. In recognition of this, we will implement a range of measures to promote the accuracy of WhoIs information in our TLD including:

- Random monthly audits: registrants of randomly selected domain names are contacted by telephone using the provided WhoIs information by a member of the ARI Abuse and Compliance Team in order to verify all WhoIs information. Where the registrant is not contactable by telephone, alternative contact details (email, postal address) will be used to contact the registrant, who must then provide a contact number that is verified by the member of the ARI Policy Compliance team. In the event that the registrant is not able to be contacted by any of the methods provided in WhoIs, the domain name will be cancelled following five contact attempts or one month after the initial contact attempt (based on the premise that a failure to respond is indicative of inaccurate WhoIs information and is grounds for terminating the registration agreement).
  - Semi-annual audits: to identify incomplete WhoIs information. Registrants will be contacted using provided WhoIs information and requested to provide missing information. In the event that the registrant fails to provide missing information as requested, the domain name will be cancelled following five contact attempts or one month after the initial contact attempt.
  - Email reminders: to update WhoIs information to be sent to registrants every 6 months.
  - Reporting system: a web-based submission service for reporting WhoIs accuracy issues available on the Abuse page of our registry website.
  - Analysis of registry data: to identify patterns and correlations indicative of inaccurate WhoIs (eg repetitive use of fraudulent details).
- Registrants will continually be made aware, through the registry website and email reminders, of their responsibility to provide and maintain accurate WhoIs information and the ramifications of a failure to do so or respond to requests

to do so, including termination of the Registration Agreement.

The measures to promote WhoIs accuracy described above strike a balance between the need to maintain the integrity of the WhoIs service, which facilitates the identification of those taking part in illegal or fraudulent behaviour, and the operating practices of the registry operator and Registrars, which aim to offer domain names to registrants in an efficient and timely manner.

Awareness by registrants that we will actively take steps to maintain the accuracy of WhoIs information mitigates the potential for abuse in the TLD by discouraging abusive behaviour given that registrants may be identified, located and held liable for all actions in relation to their domain name.

#### 4.3 Reactive - Identification

The methods by which abusive behaviour in our TLD may be identified are described below. These include detection by ARI and notification from third parties. These methods serve to merely identify and not determine whether abuse actually exists. Upon identification of abuse, the behaviour will be handled in accordance with '4.4 Abuse Handling'.

Any abusive behaviour identified through one of the methods below will, in accordance with Requirement 13 of the BITS Requirements, be notified immediately to relevant Registrars.

##### 4.3.1 Detection - Analysis of Data

ARI will routinely analyse registry data in order to identify abusive domain names by searching for behaviours typically indicative of abuse. The following are examples of the data variables that will serve as indicators of a suspicious domain name and may trigger further action by the ARI Abuse and Compliance Team:

- Unusual Domain Name Registration Practices: practices such as registering hundreds of domains at a time, registering domains which are unusually long or complex or include an obvious series of numbers tied to a random word (abuse40, abuse50, abuse60) may, when considered as a whole, be indicative of abuse.
- Domains or IP addresses identified as members of a Fast Flux Service Network (FFSN): ARI uses the formula developed by the University of Mannheim and tested by participants of the Fast Flux PDP WG to determine members of this list. IP addresses appearing within identified FFSN domains, as either NS or A records shall be added to this list.
- An Unusual Number of Changes to the NS record: the use of fast-flux techniques to disguise the location of web sites or other Internet services, to avoid detection and mitigation efforts, or to host illegal activities is considered abusive in the TLD. Fast flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or nameserver resolves. As such an unusual number of changes to the NS record may be indicative of the use of fast-flux techniques given that there is little, if any, legitimate need to change the NS record for a domain name more than a few times a month.
- Results of WhoIs audits: The audits conducted to promote WhoIs accuracy described above are not limited to serving that purpose but may also be used to identify abusive behaviour given the strong correlation between inaccurate WhoIs data and abuse.
- Analysis of cross-validation of registrant WhoIs data against WhoIs data known to be fraudulent.
- Analysis of Domain Names belonging to a registrant subject to action under the Anti-Abuse Policy: in cases where action is taken against a registrant through the application of the Anti-Abuse Policy, we will also investigate other domain names by the same registrant (same name, nameserver IP address, email address, postal address etc).

##### 4.3.2 Abuse Reported by Third Parties

Whilst we are confident in our abilities to detect abusive behaviour in the TLD owing to our robust ongoing monitoring activities, we recognise the value of notification from third parties to identify abuse. To this end, we will incorporate notifications from the following third parties in our efforts to identify abusive behaviour:

- Industry partners through ARI's participation in industry forums which

facilitate the sharing of information.

- LEA through a single abuse point of contact (our Abuse page on the registry website, as discussed in detail below) and an expedited process (described in detail in '4.4 Abuse Handling') specifically for LEA.
- Members of the general public through a single abuse point of contact (our Abuse page on the registry website).

#### 4.3.2.1 Industry Participation and Information Sharing

ARI is a member of the Registry Internet Safety Group (RISG), whose mission is to facilitate data exchange and promulgate best practices to address Internet identity theft, especially phishing and malware distribution. In addition, ARI coordinates with the Anti-Phishing Working Group (APWG) and other DNS abuse organisations and is subscribed to the NXdomain mailing list. ARI's strong participation in the industry facilitates collaboration with relevant organisations on abuse-related issues and ensures that ARI is responsive to new and emerging domain name abuses.

The information shared as a result of this industry participation will be used to identify domain names registered or used for abusive purposes. Information shared may include a list of registrants known to partake in abusive behaviour in other TLDs. Whilst presence on such lists will not constitute grounds for registrant disqualification, ARI will investigate domain names registered to those listed registrants and take action in accordance with the Anti-Abuse Policy. In addition, information shared regarding practices indicative of abuse will facilitate detection of abuse by our own monitoring activities.

#### 4.3.2.2 Single Abuse Point of Contact on Website

In accordance with section 4.1 of Specification 6 of the Registry Agreement, we will establish a single abuse point of contact (SAPOC) responsible for addressing and providing a timely response to abuse complaints concerning all names registered in the TLD through all Registrars of record, including those involving a reseller. Complaints may be received from members of the general public, other registries, Registrars, LEA, government and quasi-governmental agencies and recognised members of the anti-abuse community.

The SAPOC's accurate contact details (email and mailing address as well as a primary contact for handling inquiries related to abuse in the TLD) will be provided to ICANN and published on the Abuse page of our registry website, which will also include:

- All public facing policies in relation to the TLD, including the Anti-Abuse Policy.
- A web-based submission service for reporting inaccuracies in WhoIs information.
- Registrant Best Practices.
- Conditions that apply to proxy registration services and direction to the SAPOC to report domain names that violate the conditions.

As such, the SAPOC may receive complaints regarding a range of matters including but not limited to:

- Violations of the Anti-Abuse Policy.
- Inaccurate WhoIs information.
- Violation of the restriction of proxy registration services to individuals.

The SAPOC will be the primary method by which we will receive notification of abusive behaviour from third parties. It must be emphasised that the SAPOC will be the initial point of contact following which other processes will be triggered depending on the identity of the reporting organisation. Accordingly, separate processes for identifying abuse exist for reports by LEA/government and quasi-governmental agencies and members of the general public. These processes will be described in turn below.

##### 4.3.2.2.1 Notification by LEA of Abuse

We recognise that LEA, governmental and quasi-governmental agencies may be privy to information beyond the reach of others which may prove critical in the identification of abusive behaviour in our TLD. As such, we will provide an expedited process which serves as a channel of communication for LEA, government and quasi-governmental agencies to, amongst other things, report illegal conduct in connection with the use of the TLD.

The process will involve prioritisation and prompt investigation of reports identifying abuse from those organisations. The steps in the expedited process are summarised as follows:

1. ARI's Abuse and Compliance Team will identify relevant LEA, government and quasi-governmental agencies who may take part in the expedited process, depending on the mission/purpose and jurisdiction of our TLD. A means of verification will be established with each of the identified agencies in order to verify the identity of a reporting agency utilising the expedited process.
2. We will publish contact details on the Abuse page of the registry website for the SAPOC to be utilised by only those taking part in the expedited process.
3. All calls to this number will be responded to by the ARI Service Desk on a 24/7 basis. All calls will result in the generation of a ticket in ARI's case management system (CMS).
4. The identity of the reporting agency will be identified using the established means of verification (ARI's Security Policy has strict guidelines regarding the verification of external parties over the telephone). If no means of verification has been established, the report will be immediately escalated to the ARI Abuse and Compliance Team. Results of verification will be recorded against the relevant CMS ticket.
6. Upon verification of the reporting agency, the ARI Service Desk will obtain the details necessary to adequately investigate the report of abusive behaviour in the TLD. This information will be recorded against the relevant CMS ticket.
7. Reports from verified agencies may be provided in the Incident Object Description Exchange Format (IODEF) as defined in RFC 5070. Provision of information in the IODEF will improve our ability to resolve complaints by simplifying collaboration and data sharing.
8. Tickets will then be forwarded to the ARI Abuse and Compliance Team to be dealt with in accordance with '4.4 Abuse Handling'.

#### 4.3.2.2.2 Notification by General Public of Abuse

Abusive behaviour in the TLD may also be identified by members of the general public including but not limited to other registries, Registrars or security researchers. The steps in this notification process are summarised as follows:

1. We will publish contact details on the Abuse page of the registry website for the SAPOC (note that these contact details are not the same as those provided for the expedited process).
2. All calls to this number will be responded to by the ARI Service Desk on a 24/7 basis. All calls will result in the generation of a CMS ticket.
3. The details of the report identifying abuse will be documented in the CMS ticket using a standard information gathering template.
4. Tickets will be forwarded to the ARI Abuse and Compliance Team, to be dealt with in accordance with '4.4 Abuse Handling'.

#### 4.4 Abuse Handling

Upon being made aware of abuse in the TLD, whether by ongoing monitoring activities or notification from third parties, the ARI Abuse and Compliance Team will perform the following functions:

##### 4.4.1 Preliminary Assessment and Categorisation

Each report of purported abuse will undergo an initial preliminary assessment by the ARI Abuse and Compliance Team to determine the legitimacy of the report. This step may involve simply visiting the offending website and is intended to weed out spurious reports, and will not involve the in-depth investigation needed to make a determination as to whether the reported behaviour is abusive. Where the report is assessed as being legitimate, the type of activity reported will be classified as one of the types of abusive behaviour as found in the Anti-Abuse Policy by the application of the definitions provided. In order to make this classification, the ARI Abuse and Compliance Team must establish a clear link between the activity reported and the alleged type of abusive behaviour such that addressing the reported activity will address the abusive behaviour.

While we recognise that each incident of abuse represents a unique security threat and should be mitigated accordingly, we also recognise that prompt



action justified by objective criteria are key to ensuring that mitigation efforts are effective. With this in mind, we have categorised the actions that we may take in response to various types of abuse by reference to the severity and immediacy of harm. This categorisation will be applied to each validated report of abuse and actions will be taken in accordance with the table below. It must be emphasised that the actions to mitigate the identified type of abuse in the table are merely intended to provide a rough guideline and may vary upon further investigation.

#### Category 1

Probable Severity or Immediacy of Harm: Low

Examples of types of abusive behaviour: Spam, Malware

Mitigation steps:

1. Investigate
2. Notify registrant

#### Category 2

Probable Severity or Immediacy of Harm: Medium to High

Examples of types of abusive behaviour: Fast Flux Hosting, Phishing, Illegal Access to other Computers or Networks, Pharming, Botnet command and control

Mitigation steps:

1. Suspend domain name
2. Investigate
3. Restore or terminate domain name

The mitigation steps for each category will now be described:

#### 4.4.2 Investigation - Category 1

Types of abusive behaviour that fall into this category include those that represent a low severity or immediacy of harm to registrants and Internet users. These generally include behaviours that result in the dissemination of unsolicited information or the publication of illegitimate information. While undesirable, these activities do not generally present such an immediate threat as to justify suspension of the domain name in question. We will contact the registrant to instruct that the breach of the Anti-Abuse Policy be rectified. If the ARI Abuse and Compliance Team's investigation reveals that the severity or immediacy of harm is greater than originally anticipated, the abusive behaviour will be escalated to Category 2 and mitigated in accordance with the applicable steps. These are described below. The assessment made and actions taken will be recorded against the relevant CMS ticket.

#### 4.4.3 Suspension - Category 2

Types of abusive behaviour that fall into this category include those that represent a medium to high severity or immediacy of harm to registrants and Internet users. These generally include behaviours that result in intrusion into other computers' networks and systems or financial gain by fraudulent means. Following notification of the existence of such behaviours, the ARI Abuse and Compliance Team will suspend the domain name pending further investigation to determine whether the domain name should be restored or cancelled. Cancellation will result if, upon further investigation, the behaviour is determined to be one of the types of abuse defined in the Anti-Abuse Policy. Restoration of the domain name will result where further investigation determines that abusive behaviour, as defined by the Anti-Abuse Policy, does not exist. Due to the higher severity or immediacy of harm attributed to types of abusive behaviour in this category, ARI will, in accordance with their contractual commitment to us in the form of SLA's, carry out the mitigation response within 24 hours by either restoring or cancelling the domain name. The assessment made and actions taken will be recorded against the relevant CMS ticket.

Phishing is considered to be a serious violation of the Anti-Abuse Policy owing to its fraudulent exploitation of consumer vulnerabilities for the purposes of financial gain. Given the direct relationship between phishing uptime and extent of harm caused, we recognise the urgency required to execute processes that handle phish domain termination in a timely and cost effective manner. Accordingly, the ARI Abuse and Compliance Team will prioritise all reports of phishing from brand owners, anti-phishing providers or otherwise and carry out

the appropriate mitigation response within 12 hours in accordance with the SLA's in place between us and ARI. In addition, since a majority of phish domains are subdomains, we believe it is necessary to ensure that subdomains do not represent an unregulated domain space to which phishers are known to gravitate. Regulation of the subdomain space is achieved by holding the registrant of the parent domain liable for any actions that may occur in relation to subdomains. In reality, this means that where a subdomain determined to be used for phishing is identified, the parent domain may be suspended and possibly cancelled, thus effectively neutralising every subdomain hosted on the parent. In our RRA we will require that Registrars ensure that their Registration Agreements reflect our ability to address phish subdomains in this manner.

#### 4.4.4 Executing LEA Instructions

We understand the importance of our role as a registry operator in addressing consumer vulnerabilities and are cognisant of our obligations to assist LEAs, government and quasi-governmental agencies in the execution of their responsibilities. As such, we will make all reasonable efforts to ensure the integration of these agencies into our processes for the identification and handling of abuse by, amongst other things:

1. Providing expedited channels of communication (discussed above).
2. Notifying LEA of abusive behaviour believed to constitute evidence of a commission of a crime eg distribution of child pornography.
3. Sharing all available information upon request from LEA utilising the expedited process, including results of our investigation.
4. Providing bulk WhoIs information upon request from LEA utilising the expedited process.
5. Acting on instructions from a verified reporting agency.

It is anticipated that these actions will assist agencies in the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties. The relevant agencies are not limited to those enforcing criminal matters but may also include those enforcing civil matters in order to eliminate consumer vulnerabilities.

Upon notification of abusive behaviour by LEA, government or quasi-governmental agencies through the expedited process and verification of the reporting agency, a matter will be immediately communicated to us for our consideration. If we do not instruct ARI to refer the matter to us for our resolution, the CMS ticket will be forwarded to the ARI Abuse and Compliance Team, which will take one of the following actions:

1. The reported behaviour will be subject to preliminary assessment and categorisation as described above. The reported behaviour will then be mitigated based on the results of the categorisation. A report describing the manner in which the notification from the agency was handled will be provided to the agency within 24 hours. This report will be recorded against the relevant CMS ticket.

OR

2. Where specific instructions are received from the reporting agency in the required format, ARI will act in accordance with those instructions provided that they do not result in the contravention of applicable law. ARI will, in accordance with their contractual commitment to us in the form of SLA's, execute such instructions within 12 hours. The following criteria must be satisfied by the reporting agency at this stage:

- a. The request must be made in writing to ARI using a Pro Forma document on the agency's letterhead. The Pro Forma document will be sent to the verified agency upon request.
- b. The Pro Forma document must be delivered to ARI by fax.
- c. The Pro Forma document must:
  - i. Describe in sufficient detail the actions the agency seeks ARI to take.
  - ii. Provide the domain name/s affected.
  - iii. Certify that the agency is an 'enforcement body' for the purposes of the Privacy Act 1988 (Cth) or local equivalent.
  - iv. Certify that the requested actions are required for the investigation and/or enforcement of relevant legislation which must be specified.
  - v. Certify that the requested actions are necessary for the agency to

effectively carry out its functions.

Following prompt execution of the request, a report will be provided to the agency in a timely manner. This report will be recorded against the relevant CMS ticket.

Finally, whilst we do not anticipate the occurrence of a security situation owing to our robust systems and processes deployed to combat abuse, we are aware of the availability of the Expedited Registry Security Request Process to inform ICANN of a present or imminent security situation and to request a contractual waiver for actions we might take or have taken to mitigate or eliminate the security concern.

## 5 RESOURCES

This function will be performed by ARI. Abuse services are supported by the following departments:

- Abuse and Compliance Team (6 staff)
- Development Team (11 staff)
- Service Desk (14 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q28 - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system. Based on past experience ARI estimates that the existing staff is adequate to support a registry system that supports in excess of 50M domains. Since this TLD projects 150000 domains, 0,3% of these resources are allocated to this TLD. See attachment 'Q28 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required.

ARI's Anti-Abuse Service serves to prevent and mitigate abusive behaviour in the TLD as well as activities that may infringe trademarks. These responsibilities will be undertaken by three teams. ARI's Development Team will be responsible for developing the technical platforms and meeting technical requirements needed to implement the procedures and measures adopted to mitigate the potential for abuse, identify abuse and handle identified abuse. ARI's Abuse and Compliance Team will be responsible for the ongoing implementation of measures to minimise abusive registrations and other activities that have a negative impact on Internet users. ARI's Service Desk will be responsible for responding to reports of abuse received through the abuse point of contact on the registry's website and logging these in a ticket in ARI's case management system.

The responsibilities of these teams relevant to the initial implementation and ongoing maintenance of our measures to minimise abusive registrations and other activities that affect the rights of trademark holders are described in our response to Question 29.

All of the responsibilities undertaken by ARI's Development Team, Abuse and Compliance Team, and Service Desk are inclusive in ARI's Managed TLD Registry services fee, which is accounted for as an outsourcing cost in our response to Question 47. The resources needs of these teams have been determined by applying the conservative growth projections for our TLD (which are identified in our response to Question 48) to the team's responsibilities at start-up and on an ongoing basis.

### 5.1 ARI Development Team

All tools and systems needed to support the initial and ongoing implementation of measures adopted to mitigate the potential for abuse, identify abuse and handle identified abuse will be developed and maintained by ARI. ARI has a software development department dedicated to this purpose which will ensure that the tools are fit for purpose and adjusted as requirements change.

ARI's Development Team participate actively in the industry; this facilitates collaboration with relevant organisations on abuse related issues and ensures that the ARI Development Team is responsive to new and emerging domain name abuses and the tools and systems required to be built to address these abuses.

This team consists of:

- 1 Development Manager
- 2 Business Analysts
- 6 Developers
- 2 Quality Analysts

## 5.2 ARI Abuse and Compliance Team

ARI's Abuse and Compliance Team will be staffed by six full-time equivalent positions. These roles will entail the following:

**Policy Compliance Officers:** A principal responsibility of the Policy Compliance Officers will be handling notifications of abuse through the SAPOC. This will involve managing the expedited process, identifying and categorising suspected abuse according to our Anti-Abuse Policy, and carrying out the appropriate mitigation response for all categorised abuses. When abuse is identified, Policy Compliance Officers will investigate other domain names held by a registrant whose domain name is subject to a mitigation response. They will maintain a list of and disqualify registrants found to have repeatedly engaged in abusive behaviour. They will also be responsible for analysing registry data in search of behaviours indicative of abuse, reviewing industry lists in search of data that may identify abuse in the TLD.

Another key responsibility of Policy Compliance Officers will be implementing measures to promote WhoIs accuracy (including managing and addressing all reports of inaccurate WhoIs information received from the web submission service) and verifying the physical address provided by a registrant against various databases for format and content requirements for the region. Policy Compliance Officers will act on the instructions of verified LEA and Dispute Resolution Providers and participate in ICANN and industry groups involved in the promulgation of policies and best practices to address abusive behaviour. They will escalate complaints and issues to the Legal Manager when necessary and communicate with all relevant stakeholders (Registrars, registrants, LEA, general public) as needed in fulfilling these responsibilities. This role will be provided on a 24/7 basis, supported outside of ordinary business hours by ARI's Service Desk.

Policy Compliance Officers will be required to have the following skills/qualifications: customer service/fault handling experience, comprehensive knowledge of abusive behaviour in a TLD and related policies, Internet industry knowledge, relevant post-secondary qualification, excellent communication and professional skills, accurate data entry skills, high-level problem solving skills, and high-level computer skills.

**Legal Manager:** The Legal Manager will be responsible for handling all potential disputes arising in connection with the implementation of ARI's Anti-Abuse service and related policies. This will involve assessing escalated complaints and issues, liaising with Legal Counsel and the registry operator, resolving disputes and communicating with all relevant stakeholders (Registrars, registrants, LEA, general public) as needed in fulfilling these responsibilities. The Legal Manager will be responsible for forwarding all matters requiring determination by the registry operator which fall outside the scope of ARI's Anti-Abuse functions. The Legal Manager will be required to have the following skills/qualifications: legal background (in particular, intellectual property/information technology law) or experience with relevant tertiary or post-graduate qualifications, dispute resolution experience, Internet industry experience, strong negotiation skills, excellent communication and professional skills, good computer skills, high-level problem solving skills.

**Legal Counsel:** A qualified lawyer who will be responsible for all in-house

legal advice, including responding to LEA and dealing with abusive behaviour.

The team consists of:

- 4 Policy Compliance Officers
- 1 Legal Manager
- 1 Legal Counsel

### 5.3 ARI Service Desk

ARI's Service Desk will be staffed by 14 full-time equivalent positions. Responsibilities of Service Desk relevant to ARI's Anti-Abuse Service include the following: responding to notifications of abuse through the abuse point of contact and expedited process for LEA, logging notifications as a ticket in ARI's case management system, notifying us of a report received through the expedited process for LEA, government and quasi-governmental agencies, and forwarding tickets to ARI's Abuse and Compliance team for resolution in accordance with the Anti-Abuse Policy.

For more information on the skills and responsibilities of these roles please see the in-depth resources section in response to Question 31.

Based on the projections and the experience of ARI, the resources described here are more than sufficient to accommodate the needs of this TLD.

The use of these resources and the services they enable is included in the fees paid to ARI which are described in the financial responses.

## 29. Rights Protection Mechanisms

The Applicant has engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q29 - ARI Background & Roles.pdf'.

### 1 INTRODUCTION

This response is organised by first addressing the RPMs that we will apply during start-up of our TLD (sunrise and trademark claims service) and then by addressing the RPMs that we will apply on an ongoing basis (URS, UDRP and efforts to avoid infringement trademark infringement including implementation of and compliance with the Trademark PDDRP). Each measure is described and the technological and contractual steps needed for its implementation are identified.

The abusive behaviour primarily targeted by these RPMs is cybersquatting, which is the registration of names constituting trademarks by registrants lacking rights in such trademarks. Cybersquatting is one of the many forms of abuse we will seek to minimise in our TLD. Our approach to combating abusive behaviours other than cybersquatting is described in our response to Question 28. Some overlap between the responses to Questions 28 and Question 29 is inherent because the prevention of cybersquatting can also serve to minimise other abusive behaviours such as phishing and pharming. By implementing the RPMs discussed below we thus aim to minimise not only cybersquatting but also some of the abusive behaviours identified in the response to Question 28. The registration policy of our TLD is described in our response to Question 18. We acknowledge that the legal rights protected by ICANN-mandated RPMs are limited to trademarks. Different RPMs define the scope of protectable trademarks slightly differently; we therefore clearly identify the scope of protectable marks as respects each RPM.

In addition to the RPMs mandated by the Applicant Guidebook, we have also adopted certain requirements proposed in the '2011 Proposed Security, Stability and Resiliency Requirements for Financial TLDs' (at <http://www.icann.org/en/news/correspondence/aba-bits-to-beckstrom-crocker-20dec11-en.pdf>) (the 'BITS Requirements'). We acknowledge that these requirements were developed by the financial services sector in relation to financial TLDs, but nevertheless believe that their adoption in this TLD (which

is not financial-related) results in a more robust approach to combating abuse.

In particular, we will adopt the following:

Requirement 6: we will certify annually to ICANN our compliance with our Registry Agreement.

Requirement 8: we will provide and maintain valid primary contact information (name, email address, and phone number) on our registry website.

Requirement 10: we will re-validate our Registry-Registrar Agreements at least annually.

Requirement 13: we will notify Registrars immediately regarding any RPM investigation or compliance action including the nature of the investigation or compliance action by ICANN or any outside party (eg, law enforcement etc).

We will additionally require through our Registry-Registrar Agreement (RRA) that Registrars comply with the following:

Requirement 7: Registrars must certify annually to ICANN their compliance with ICANN's Registrar Accreditation Agreement (RAA).

Requirement 9: Registrars must provide and maintain valid primary contact information (name, email address, and phone number) on their website.

Requirement 19: Registrars must disclose registration requirements on their website.

## 2 START-UP RPMS

Below we identify our start-up RPM timeline and describe our implementation of:

- A sunrise period.
- The trademark claims service ('TM claims service') during a landrush period.

### 2.1 Start-up RPMS Timeline

The timeline for start-up RPMS in our TLD is as follows:

Day 1: Single sunrise round opens

Day 30: Sunrise round closes

Day 31: Sunrise allocation begins

Day 40: Landrush (including TM claims service) opens

Day 100: Landrush closes

Day 101: Landrush allocation begins

Day 110: General availability begins

### 2.2 Sunrise Registration Service

Our sunrise will provide trademark holders with a 30-day priority period in which to register their trademarks as domain names.

The following stakeholders are involved in implementation of the sunrise registration service:

- TMCH Service Provider/s
- Trademark owner prospective domain name registrants
- Registrars
- Registry operator
- Auction provider

The role played by these stakeholders is described below by reference to:

- A summary of our Sunrise Policy and Sunrise Dispute Resolution Policy (SDRP)
- Our Sunrise Implementation Plan
- Our SDRP Implementation Plan
- Our implementation of sunrise and SDRP through contractual relationships

#### 2.2.1 Sunrise Policy Summary and SDRP Summary

Through our Sunrise Policy we will offer a single, 30-day sunrise round in which trademark holders satisfying (i), (iii) and (iv) of the Sunrise Eligibility Requirements (SERs) and any general eligibility requirements (as identified in our response to Question 18) proposed in the Applicant Guidebook at Trademark Clearinghouse s6.2.3 will be eligible to apply for a domain name. Our Sunrise Policy will specify that applications satisfying the SERs received by a Registrar within the 30-day sunrise period will be accepted for participation in the sunrise. This will be the first opportunity for registration in our TLD.

Our Sunrise Policy will mandate that the trademarks upon which sunrise

applications are based must fall within s7.2 of the Applicant Guidebook (Trademark Clearinghouse) and be supported by an entry in the TMCH. Consistent with Requirement 2 of the BITS Requirements, our Sunrise Policy will describe how we will allocate domain names applied for during the sunrise period, as follows: allocation will start at the end of the 30-day sunrise period. Where only one validated application is received for a domain name, that domain will be allocated to the applicant during the 10-day period between the close of the sunrise applications period and start of the landrush. Where multiple validated applications are received for a domain name, applicants will be invited to participate in an auction to determine the party to which the domain will be allocated. Our Sunrise Policy will specify that by making a sunrise application (or, where relevant, by agreeing to participate in an auction), the applicant agrees to purchase the domain if it is allocated to the applicant. Domain names registered during the sunrise period will have a term of one year from the date of registration.

We will adopt an SDRP to allow any party to raise a challenge on the four grounds identified in the Applicant Guidebook at Trademark Clearinghouse, s6.2.4. The remedy will be cancellation or deletion of a successfully challenged domain. All registrants will be required to submit to proceedings under the SDRP. Our SDRP will specify that SDRP claims may be raised after registration of a sunrise domain and will require that complaints clearly identify the challenger, the challenged domain, and the grounds on which the complaint is based.

If a TMCH service provider is not able to receive challenges directly as part of its undertaking to 'maintain the SERs, validate and authenticate marks, as applicable, and hear challenges' (Applicant Guidebook at Trademark Clearinghouse, s6.2.5), ARI will receive SDRP challenges and communicate these to the SDRP provider.

#### 2.2.2 Implementation

Our Sunrise and SDRP Implementation Plan are set out below followed by a description of the implementation that will take place through contractual relationships.

##### 2.2.2.1 Sunrise Implementation Plan

1. Prior to or during our 30-day sunrise period, trademark holders can apply for validation of marks by the TMCH and inclusion of validated marks in the TMCH database.
2. ARI will develop a website and make available on that website our Sunrise Policy and SDRP.
3. A trademark holder warranting satisfaction of the SERs in our Sunrise Policy (as described above) will submit to an ICANN-accredited Registrar its application to register a domain corresponding to its TMCH entry with evidence of the TMCH entry. A non-refundable sunrise application/validation fee will be payable by the applicant to the Registrar on submitting the application.
4. Registrars will be required through our RRA to communicate sunrise application information to ARI. On receipt of this information, ARI will charge the sunrise application/validation fee to the submitting Registrar.
5. ARI will perform standard checks (including IDN validity checks where relevant, reserved and restricted words in accordance with the Registry Agreement, composition requirements, etc) to ensure that the domain being applied for is technically valid; an error message will be returned to the Registrar if the domain fails any of these checks. If the domain passes these checks, ARI will hold the application for allocation.
6. Allocation will commence upon conclusion of the 30-day sunrise period. As an initial step, ARI will compile a list of applied-for names and reserve these from registration in landrush and general availability.
7. Through an interface with the TMCH, ARI will identify all sunrise applications constituting an 'Identical Match' (as defined in the Applicant Guidebook at Trademark Clearinghouse s6.1.5) with a TMCH entry and provide notice to the holders of those marks of the filing of a corresponding sunrise application.
8. Where a single application exists for a particular domain, between the end of the sunrise application period and start of the landrush period ARI will

enable the sponsoring Registrar to CREATE (using EPP or the SRS web interface) the domain and charge the sunrise registration fee to the Registrar, who will collect this fee from the registrant.

9. Where multiple sunrise applications exist for an identical domain name, ARI will compile and communicate to a third-party auction services provider a list of competing applicants, who will be invited to participate in an auction.

10. The auction services provider will facilitate the auction process and upon its completion will notify all participants of the outcome and collect the auction payment from the winning participant.

11. Upon payment of the auction bid, the auction services provider will communicate to ARI the details of the winning auction participant and submit the revenue collected to ARI.

12. ARI will validate the communication from the auction services provider and enable the sponsoring Registrar to CREATE (using EPP or the SRS web interface) the domain name. ARI will charge the sunrise registration fee to the auction winner's Registrar, who will collect this fee from the registrant.

#### 2.2.2.2 SDRP Implementation Plan

1. If a TMCH service provider is not able to directly receive complaints under our SDRP, we will specify in our SDRP the email address to which SDRP filings must be sent. This email address will be monitored by ARI's Abuse and Compliance Team.

2. ARI will develop a process of manual or automatic interface with the TMCH to communicate the SERs and any SDRP challenges received by ARI. This interface will also enable the TMCH Service Provider to notify ARI of successful SDRP challenges.

3. Upon notification from a TMCH service provider of a successful SDRP challenge, ARI will cancel or delete the successfully challenged domain.

#### 2.2.2.3 Implementation through Contractual Relationships

The following features of the Sunrise and SDRP implementation plan described above will be executed by inclusion of corresponding clauses in our RRA, which will require inclusion in Registrars' Registration Agreements:

- By making a sunrise application (or, where relevant, by agreeing to participate in an auction), applicant agrees to purchase the domain name if that name is allocated to the applicant.
- The sunrise application fee is non-refundable.
- All sunrise applicants must submit to proceedings under the SDRP.

#### 2.3 TM Claims Service During Landrush

Ten days after the day that sunrise allocations begin, a 60-day landrush period will commence during which we will offer the TM claims service. This is a service whereby prospective domain name registrants receive notice of existing trademark rights matching their applied-for domain and trademark owners receive notice of domain name registrations matching their trademark. In accordance with the Applicant Guidebook, our TM claims service will be supported exclusively by the TMCH and will recognise and honour all word marks falling within the Applicant Guidebook at Trademark Clearinghouse s7.1.

The following stakeholders are involved in implementation of the TM claims service:

- TMCH Service Provider/s
- Trademark owners
- Landrush domain name applicants
- Landrush domain name registrants
- Registrars
- Registry operator

The role played by these stakeholders is described below by reference to:

- Our Landrush/TM Claims Service Implementation Plan
- Our implementation of Landrush/TM Claims Service through contractual relationships

Consistent with Requirement 2 of the BITS Requirements, the Landrush/TM Claims Service Implementation Plan identifies how we will allocate domain names applied for during the landrush.



### 2.3.1 Implementation

Our Landrush™ Claims Service Implementation Plan is set out below followed by a description of the implementation that will take place through contractual relationships.

#### 2.3.1.1 Landrush™ Claims Service Implementation Plan

1. Prior to or during our 60-day landrush period trademark holders can apply for validation of their marks by the TMCH and inclusion of validated marks in the TMCH database. This will enable provision of notice to landrush applicants of entries in the TMCH and provision of notice to trademark holders of registrations matching TMCH entries (how and by whom this will be achieved is detailed in subsequent steps of this implementation plan).
2. An applicant warranting compliance with the registration policies in this TLD (as described in our response to Question 18) will make an application to an ICANN-accredited Registrar for a domain name during the 60-day landrush period. A non-refundable landrush application/validation fee will be payable by the applicant to the Registrar on submitting the application.
3. Registrars will be required through our RRA to communicate landrush application information to ARI. On receipt of this information, ARI will charge the landrush application/validation fee to the submitting Registrar.
4. Registrars will be required through our RRA to interface with the TMCH to determine whether an applied-for domain constitutes an 'Identical Match' with a mark in the TMCH. If an 'Identical Match' is identified, the Registrar will provide to the landrush applicant a TM Claims Notice in the form prescribed by the Applicant Guidebook. Following receipt of this notice a landrush applicant must communicate to the Registrar its decision either to proceed with or abandon the application. If the applied-for name does not constitute an 'Identical Match' with a trademark in the TMCH, no TM Claims Notice will be generated.
5. ARI will utilise the manual or automatic interface it establishes for implementation of the SDRP (described above in 'Implementation Plan') to facilitate reporting by the TMCH of attempts to register domains that are an 'Identical Match' with a trademark (within the scope of the Applicant Guidebook at Trademark Clearinghouse s7.1) in the TMCH database.
6. ARI will perform standard checks (including IDN validity checks where relevant, reserved and restricted words in accordance with the Registry Agreement, composition requirements, etc) on all landrush applications (irrespective of whether they have generated a TM Claims Notice) to ensure that the domain being applied for is technically valid and an error message will be returned to the Registrar if the domain fails any of these checks. If the domain passes these checks, ARI will hold the application for allocation.
7. Allocation of landrush applications will commence on conclusion of the 60-day landrush application period. Where a single landrush application exists for a particular domain, between the end of the landrush application period and start of general availability, ARI will enable the sponsoring Registrar to CREATE (using EPP or the SRS web interface) the domain and charge the landrush registration fee to the Registrar, who will collect this fee from the registrant.
8. Where multiple landrush applications exist for an identical domain, ARI will compile and communicate to a third-party auction services provider a list of competing applicants, who will be invited to participate in an auction for the domain name.
9. The auction services provider will facilitate the auction process and on its completion will notify all participants of the outcome and collect payment from the winning participant.
10. Upon payment of the auction bid the auction services provider will communicate to ARI the details of the winning participant and will submit the revenue collected to ARI.
11. ARI will validate the communication from the auction services provider and enable the auction winner's Registrar to CREATE (using EPP or the SRS web interface) the domain name. ARI will charge the landrush registration fee to the Registrar, who will collect this fee from the registrant.
12. The Registrar will be required through our RRA to interface with the TMCH to promptly notify relevant mark holders of the registration of a domain

constituting an 'Identical Match' to their TMCH entry.

13. Ten days after the start of the landrush allocation period, general availability of domain names (at first-come, first-served allocation) will commence.

#### 2.3.1.2 Implementation through Contractual Relationships

The following features of our Landrush™ Claims Service Implementation Plan described above will additionally be executed by the inclusion of corresponding clauses in our RRA:

- Registrars must use the TMCH as required by ICANN and the TMCH Service Provider/s.
- Registrars must not in their provision of the TM Claims Service make use of any trademark information aggregation, notification or validation service other than the TMCH.
- In order to prevent a chilling effect on registration, Registrars must ensure that landrush applicants are not prevented from registering domains considered an 'Identical Match' with a mark in the TMCH.
- Registrars must provide clear notice in the specific form provided by the Applicant Guidebook to the prospective registrant of relevant entries in the TMCH.
- The landrush application fee is non-refundable. Registrars must also include this in their Registration Agreements.

### 3 ONGOING RPMS

Below we describe the way in which we will implement on an ongoing basis the URS and UDRP and address issues related to the Trademark PDDRP. These RPMS serve to mitigate not only cybersquatting but other types of abuse that frequently occur in conjunction with cybersquatting, such as phishing and pharming.

#### 3.1 URS

The URS is a new RPM the implementation of which is mandated in all new gTLDs. The URS is targeted at providing a rapid takedown solution to clear-cut cases of cybersquatting. It is intended to have a deterrent effect and reduce the number of UDRP disputes.

The URS is intended to supplement and not replace the UDRP, and the Applicant Guidebook foreshadows (at URS ss8.6 and 13) the likelihood of URS claimants also commencing UDRP claims. For this reason, we have considered in our URS Implementation Plan the potential interaction between URS stakeholders and UDRP stakeholders.

The following stakeholders are involved in implementation of the URS:

- URS claimants (holders of valid and enforceable trade or service marks)
- Registrants
- Registrars
- Registry operator
- URS provider/s
- URS Examiner

The role played by these stakeholders is described below by reference to:

- Our URS Implementation Plan
- Our implementation of the URS through contractual relationships

Our URS Implementation Plan identifies certain aspects of implementation that are not clearly addressed in the Applicant Guidebook. For example, the Guidebook does not specify how, from an operational perspective, suspension of a domain name will transform to another domain name status (eg the transfer of a domain following a successful UDRP challenge); we assume that such a status change would only occur upon expiry of the registration, but acknowledge the potential for further development of URS policy to allow for change of status as a result of a subsequent UDRP decision.

In addition to identifying such gaps, our URS Implementation Plan identifies our proposed method of addressing these. Furthermore, understanding that a fundamental aim of the URS is expediency, all of the steps in our Implementation Plan below will be undertaken as soon as practical but without

compromising security or accuracy.

### 3.1.1 Implementation

Our URS Implementation Plan is set out below followed by a description of the implementation that will take place through contractual relationships.

#### 3.1.1.1 URS Implementation Plan

1. As an initial step, ARI will notify to each URS provider an email address for all URS-related correspondence. On an ongoing basis, ARI's Abuse and Compliance Team will monitor this address for communications from URS providers, including the Notice of Complaint, Notice of Default, URS Determination, Notice of Appeal and Appeal Panel Findings.
2. ARI will validate correspondence from a URS provider to ensure that it originates from the URS Provider.
3. ARI will within 24 hours of receipt of a URS Notice of Complaint lock the domain name/s the subject of complaint by restricting all changes to the registration data, including transfer and deletion of the domain. The domain will continue to resolve while in this locked status.
4. ARI will immediately notify the URS provider in the manner requested by the URS provider once the domain name/s have been locked.
5. Upon receipt of a favourable URS Determination ARI will lock the domain name the subject of the Determination for the balance of the registration period and redirect the nameservers to an informational web page provided by the URS provider. While a domain name is locked, ARI will continue to display all of the WhoIs information of the original registrant except for the redirection of the nameservers and (subject to future policy development taking into account the transfer of a URS-locked domain name following a successful UDRP challenge) the additional statement that the domain will not be able to be transferred, deleted or modified for the life of the registration.
6. Upon receipt of notification from the URS provider of termination of a URS proceeding ARI will promptly unlock the domain and return full control to the registrant.
7. Where a default has occurred (because a registrant has not submitted an answer to a URS complaint in accordance with the Applicant Guidebook at URS s6.1) and a Determination has been made in favour of the complainant, in the event that ARI receives notice from a URS provider that a Response has been filed in accordance with the Applicant Guidebook at URS s6.4, ARI will as soon as practical restore a domain to resolve to the original IP address while preserving its locked status until a Determination from de novo review is notified to ARI.
8. ARI will ensure that no changes are made to the resolution of a registration the subject of a successful URS Determination until expiry of the registration or the additional registration year unless otherwise instructed by UDRP provider.
9. ARI will make available to successful URS complainants an optional extension of the registration period for one additional year at commercial rates. We understand that this requirement has been based on the provision in the Expired Domain Deletion Policy (3.7.5.7 of the 2009 RAA), under which there is no requirement of notification to the complainant that a name is due to expire. From this we conclude that there is likewise no requirement in the operation of our TLD that ARI notify a successful URS complainant that a name is due to expire.
10. The Applicant Guidebook specifies that renewal must be offered 'at commercial rates' but it does not specify how and to whom payment for renewal should be made. If payment is to be made to a stakeholder other than the registry operator, it is not clear how this will be received by the registry operator. ARI's Abuse and Compliance Team will be prepared and have the expertise and flexibility necessary to develop the technical and financial interfaces necessary to facilitate the receipt of renewal fees by ARI.

#### 3.1.1.2 Implementation of the URS through Contractual Relationships

The following features of our URS Implementation Plan described above will be executed by inclusion of corresponding clauses in our RRA:

- In the event that a registrant does not submit an answer to a URS complaint

in accordance with the Applicant Guidebook at URS s6.1 (default), Registrars must prevent registrants from making changes to the WhoIs information of a registration while it is in default.

- Registrars must prevent changes to a domain it is in locked status to ensure that both the Registrar's systems and registry's systems contain the same information for the locked domain.
- Registrars must not take any action relating to a URS proceeding except as in accordance with a validated communication from ARI or URS provider.

### 3.2 UDRP

The UDRP is applicable to domain name registrations in all new gTLDs. It is available to parties with rights in valid and enforceable trade or service marks and is actionable on proof of all of the following three grounds:

- i. The registrant's domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights.
- ii. The registrant has no rights or legitimate interests in respect of the domain name.
- iii. The registrant's domain name has been registered and is being used in bad faith.

Available remedies are cancellation of a domain or transfer of a domain to a successful UDRP claimant.

The following stakeholders are involved in implementation of the UDRP:

- UDRP claimants
- Registrants
- Registrar
- Registry operator
- UDRP providers

The role played by these stakeholders is described below by reference to:

- Our UDRP Implementation Plan
- Our implementation of the UDRP through contractual relationships

Our UDRP Implementation Plan considers the potential overlap between URS implementation and UDRP implementation because we consider it likely that URS complainants may commence UDRP claims as a second recourse or simultaneously. We note that neither policy prohibits complainants from commencing proceedings simultaneously.

#### 3.2.1 Implementation

Our UDRP Implementation Plan is set out below followed by a description of the implementation that will take place through contractual relationships.

##### 3.2.1.1 UDRP Implementation Plan

Our UDRP Implementation Plan focuses on interaction with Registrars because there is currently no interaction between existing gTLD registry operators and UDRP providers. On this basis we anticipate ARI has two responsibilities to facilitate Registrars' implementation of the UDRP.

1. ARI's Development Team (as described in '4 RESOURCES') will maintain awareness of UDRP requirements and be capable of taking action when required and sufficiently skilled and flexible to respond to any changes to UDRP policy.
2. ARI will provide EPP and the SRS web interface to enable Registrars to perform required UDRP functions in accordance with the Policy on Transfer of Registrations between Registrars.

##### 3.2.1.2 Implementation of the UDRP through Contractual Relationships

The UDRP is applicable to domain name registrations in all new gTLDs by force of a contractual obligation (Registry Agreement Art. 2.9) on registry operators to use only ICANN-accredited Registrars, who in turn are contractually required (RAA, 21 May 2009, at s3.8) to incorporate the UDRP in their Registration Agreements.

### 3.3 Preventing Trademark Infringement in Operating the Registry

We take seriously our responsibilities in running a registry and understand that while offering a sunrise registration service and TM Claims Service during start-up of our TLD and the URS and UDRP on an ongoing basis serves to minimise abuse, this does not necessarily serve to minimise trademark infringement in

our operation of the TLD. This responsibility is now clearly placed on registry operators through the new Trademark PDDRP, which targets infringement arising from the registry operator's manner of operation or use of its TLD.

While we will as required by the Registry Agreement agree to participate in all Trademark PDDRP procedures and be bound by resulting determinations, we will also have in place procedures to identify and address potential conflicts before they escalate to the stage of a Trademark PDDRP claim.

The following stakeholders are involved in our implementation of measures to prevent trademark infringement in operation of the TLD:

- Trademark holders
- Registry operator
- Trademark PDDRP provider/s

The role played by these stakeholders is described below by reference to:

- Our Trademark PDDRP Implementation Plan
- Our implementation of our Trademark PDDRP through contractual relationships

### 3.3.1 Implementation

Our Trademark PDDRP Implementation Plan is set out below followed by a description of the implementation that will take place through contractual relationships.

#### 3.3.1.1 Trademark PDDRP Implementation Plan

1. ARI will notify to the Trademark PDDRP provider/s contact details for all communications regarding the Trademark PDDRP.

2. As described in our response to Question 28, ARI will publish our Anti-Abuse Policy on a website dedicated to abuse handling in our TLD. Consistent with Requirement 8 of the BITS Requirements, this website will include information necessary to enable trademark holders to raise concerns regarding infringement of their trademarks and resultant harm caused by our operation or use of our TLD.

3. Using the single abuse point of contact (SAPOC) discussed in our response to Question 28, a complainant can notify ARI's Service Desk of its belief that one or more of its marks have been infringed and harm caused by our operation or use of our TLD. The complainant will be required to provide the following information:

- Name of the complainant
- Contact details
- Trademark name
- Jurisdiction
- Registration date
- Registration number
- Nature of entitlement to trademark
- Explanation of why complainant believes that its mark has been infringed and harm caused by our operation or use of the TLD

4. ARI's Service Desk will receive complaints submitted through the SAPOC on a 24/7 basis and generate a ticket in ARI's case management system (CMS). The details of the complaint (which will at a minimum include the information above) will be documented using a standard information gathering template and forwarded to ARI's Abuse and Compliance Team.

5. Upon receipt of a complaint, the Abuse and Compliance Team will conduct a preliminary assessment to ensure that a complaint is not spurious. If it is determined that a complaint is not spurious, a member of the team will use the contact details provided in the complaint to acknowledge receipt of the complaint and commence investigation of the subject matter of the complaint and good faith negotiations with the complainant in accordance with the Applicant Guidebook at Trademark PDDRP s7.2.3(d). The results of this preliminary assessment and subsequent actions taken will be recorded against the CMS ticket.

6. On an ongoing basis, ARI's Abuse and Compliance Team will monitor the email address notified to the Trademark PDDRP provider/s for all communications from the Trademark PDDRP provider, including threshold determination, Trademark PDDRP complaint, complainant's reply, notice of default, expert panel determination, notice of appeal and determination of an appeal panel.

7. In the event that a complaint cannot be resolved and a Trademark PDDRP claim

is made, ARI's Abuse and Compliance Team will do the following:

- File a response to the complaint in accordance with the Applicant Guidebook at Trademark PDDRP s10 thus avoiding (whenever possible) default.
- Where appropriate, undertake discovery in compliance with the Applicant Guidebook at Trademark PDDRP s15, attend hearings raised under s16 if required, and gather evidence in compliance with ss20.5 and 20.6.

8. ARI's Abuse and Compliance Team will upon notification of an Expert Panel finding in favour of the Claimant (Applicant Guidebook at Trademark PDDRP s14.3), reimburse the Claimant.

9. ARI will implement any remedial measures recommended by the expert panel pursuant to the Applicant Guidebook at Trademark PDDRP s18.3.1 and take all steps necessary to cure violations found by the expert panel (s18.3.2) and notified by ICANN (s21.3).

### 3.3.2 Implementation of Trademark PDDRP through Contractual Relationships

All new gTLD registry operators are bound to comply with the Trademark PDDRP by Specification 7, cl 2 of the Registry Agreement. In accordance with Requirement 6 of the BITS Requirements, we will certify annually to ICANN our compliance with our Registry Agreement.

## 4 RESOURCES

ARI's abuse services are supported by the following departments:

- Abuse and Compliance Team (6 staff)
- Development Team (11 staff)
- Service Desk (14 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q29 - ARI Background & Roles.pdf'. This attachment describes the functions of these teams and the exact number and nature of staff within.

The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system. Based on past experience ARI estimates that the existing staff is adequate to support a registry system that supports in excess of 50M domains. Since this TLD projects 150000 domains, 0,3% of these resources are allocated to this TLD. See attachment 'Q29 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required.

The measures described in the context of the responses to Question 28 and Question 29 - which serve to prevent and mitigate abusive behaviour in the TLD as well as activities that may infringe trademarks - will be implemented and managed by ARI on our behalf. These responsibilities will be undertaken by two teams. ARI's Development Team will be responsible for developing the technical platforms and meeting technical requirements needed to implement the RPMs discussed above. ARI's Abuse and Compliance Team will be responsible for the ongoing operations of measures to minimise abusive registrations and other activities that affect trademark rights recognised through RPMs. ARI's Service Desk will be responsible for responding to reports of trademark infringement received through the abuse point of contact on the Registry's website and logging these in a ticket in ARI's case management system.

The responsibilities of these teams relevant to the initial implementation and ongoing maintenance for our measures to minimise the potential in our TLD for abuse not specifically affecting trademark rights are described in our response to Question 28.

All of the responsibilities undertaken by ARI's Development Team, Abuse and Compliance Team, and Service Desk are inclusive in ARI's Managed TLD Registry services fee, which is accounted for as an outsourcing cost in our response to Question 47. The resource needs of these teams have been determined by applying

the conservative growth projections for our TLD (as identified in our response to Question 48) to the teams' responsibilities at startup and on an ongoing basis.

#### 4.1 ARI Development Team

All tools and systems used for the transmission and receipt of information related to RPMs will be developed and maintained by ARI. ARI has a Development Team dedicated to this purpose which will ensure that the tools are fit for purpose and adjusted as requirements change.

ARI will ensure that systems and tools will be compliant with the appropriate processes for dealing with Registrars, the TMCH, URS and Trademark PDDRP providers as these processes are defined. ARI has been and will remain active in the formulating of these processes, using its resources to remain current with the approved measures for exchange of any material relevant to RPMs, whether during sunrise, landrush or on an ongoing basis. This team consists of:

- 1 Development Manager
- 2 Business Analysts
- 6 Developers
- 2 Quality Analysts

#### 4.2 ARI Abuse and Compliance Team

ARI's Abuse and Compliance Team will be staffed by five full-time equivalent positions:

- 4 Policy Compliance Officers
- 1 Legal Manager

Policy Compliance Officers will be responsible for managing sunrise and landrush applications, supporting the SDRP, TM Claims Service, URS, UDRP and Trademark PDDRP, managing communications with the TMCH, receiving, assessing and managing trademark infringement complaints received through the single abuse point of contact, escalating complaints and issues to the Legal Manager when necessary and communicating with all relevant stakeholders (Registrars, registrants, trademark holders, general public) as needed in fulfilling these responsibilities. This role will be provided on a 24/7 basis supported outside of ordinary business hours by ARI's Service Desk. Policy Compliance Officers will be required to have the following skills/qualifications: customer service/fault handling experience, complete knowledge of all RPMs offered by the TLD and related policies, Internet industry knowledge, relevant post-secondary qualification, excellent communication and professional skills, accurate data entry skills, high-level problem solving skills, and high-level computer skills.

The Legal Manager will be responsible for handling all potential disputes arising in connection with RPMs and related policies. This will involve assessing complaints and issues, liaising with legal counsel and management, resolving disputes and communicating with all relevant stakeholders (Registrars, registrants, trademark holders, general public) as needed in fulfilling these responsibilities. The Legal Manager will be required to have the following skills/qualifications: legal background (in particular, intellectual property/information technology law) or experience with relevant tertiary or post-graduate qualifications, dispute resolution experience, Internet industry experience, excellent communication, negotiation, problem solving and professional skills and good computer skills.

For more information on the skills and responsibilities of these roles, please see the in-depth resources section in response to Question 31.

Based on the projections and the experience of ARI, the resources described here are more than sufficient to accommodate the needs of this TLD.

The use of these resources and the services they enable is included in the fees paid to ARI, which are described in response to Question 47.

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

The Applicant has engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q30a - ARI Background & Roles.pdf'. This response describes Security as implemented by ARI under direction from the registry operator taking into account any specific needs for this TLD.

#### 1 SECURITY POLICY SUMMARY

ARI operates an ISO27001 compliant Information Security Management System (ISMS) for Domain Name Registry Operations; see attachment 'Q30a - SAI Global Certificate of Compliance.pdf'. The ISMS is an organisation-wide system encompassing all levels of Information Security policy, procedure, standards, and records. Full details of all the policies and procedures included in the ISMS are included in the attachment to Question 30b.

##### 1.1 The ISMS

ARI's ISMS's governing policy:

- Defines the scope of operations to be managed (Domain Name Registry Operations).
- Designates the responsible parties (COO, CTO and Information Security Officer) for governance, Production Support Group for implementation and maintenance, and other departments for supporting services.
- Requires a complete Risk Assessment (a developed Security Threat Profile for the Service - in this case registry services for the TLD - and a Risk Analysis tracing threats and vulnerabilities through to Risks) and Risk Treatment Plan (each major risk in the Risk Assessment references the Statement of Applicability indicating controls to be implemented, responsible parties, and the effectiveness metrics for each).
- Includes a series of major sub policies governing security, which include but are not limited to:
  - ICT acceptable use policy and physical security policies.
  - PSG Security Policy which outlines the registry operations policies, the management of end-user devices, classification of networks and servers according to the classification of information they contain, networking, server & database configuration and maintenance guidelines, vulnerability and patch management, data integrity controls, access management, penetration testing, third party management, logging and monitoring, and cryptography.
- Requires ongoing review:
  - Of risks, threats, the Risk Treatment Plan, client requirements and commitments, process and policy compliance, process and policy effectiveness, user etc.
  - Regular internal and external penetration testing & vulnerability scanning.
  - Ad-hoc review raised during normal operations, common sources being change management processes, scheduled maintenance or project debriefs, and security incidents.
  - Yearly review cycle which includes both internal and external audits, including external surveillance audits for compliance.
  - Additional yearly security controls assessment reviews, which include analysis of the security control implementations themselves (rather than compliance with any particular standard).
  - At 24 month intervals, external penetration testing of selected production services.
  - periodic ISO reaccreditation

ARI's ISMS encompasses the following ARI standards:

- Configuration standards for operating systems, networking devices and databases based on several key publications, including those released by NIST (eg SP800-123, SP800-44v2, SP-800-40, SP800-41) and the NSA, staff testing and experience, and vendor supplied standards.



- Security Incident Classification, which identifies the various classifications of security incidents and events to ensure that events that qualify as security incidents.
- Information Classification and Handling which specifies the information classification scheme and the specific requirements of handling, labelling, management and destruction for each level of classification.

## 1.2 SECURITY PROCESSES

Processes are used to implement the policies. These include, but are not limited to:

### 1.2.1 Change Management

This includes change management and its sub-processes for access management, software deployment, release of small changes and scheduled maintenance. This process includes:

- The classification of changes and the flow into sub processes by classification.
- The release and deployment process for change control into production environments, outlining peer review, testing steps, approval points, checklist sets, staging requirements and communication requirements.
- The software release and deployment process with its specific testing and staged rollout requirements.
- The scheduled maintenance process and its various review points.

### 1.2.2 Incident Management

This includes incident management process and its sub-process for unplanned outages. These outline:

- How incidents are managed through escalation points, recording requirements, communication requirements etc.
- The unplanned outage procedure which applies directly to situations where the registry itself or other critical services are unexpectedly offline.

### 1.2.3 Problem Management

The goal of problem management is to drive long term resolution of underlying causes of incidents. This process centres on finding and resolving the root causes of incidents. It defines escalation points to third parties or other ARI departments such as Development, as well as verification of the solution prior to problem closure.

### 1.2.4 Security Incident Management

This process deals with the specific handling of security incidents. It outlines the requirements and decision points for managing security incidents. Decision points, escalation points to senior management and authorities are defined, along with evidence-gathering requirements, classification of incidents and incident logging.

### 1.2.5 Access Management

This process handles all access changes to systems. HR must authorize new users, and access changes are authorized by departmental managers and approved by the Information Security Officer.

When staff leave or significantly change roles, a separation process is followed which ensures all access that may have been granted during their employment (not just their initially granted access) is checked and where appropriate, revoked.

Finally, quarterly review of all access is undertaken by the ISO, reviewing and approving or rejecting (with an action ticket) as appropriate.

## 2 ARI'S SECURITY INFRASTRUCTURE SOLUTIONS

ARI has developed a layered approach to IT security infrastructure. At a high level, some of the layers are as follows:

- DDoS countermeasures are employed outside ARI networks. These include routing traps for DDoS attacks, upstream provider intervention, private peering links and third party filtering services.

- Routing controls at the edge of the network at a minimum ensures that only traffic with valid routing passes into ARI networks.
- Overprovisioning and burstable network capabilities help protect against DoS and DDoS attacks.
- Network firewalls filter any traffic not pre-defined by network engineering staff as valid.
- Application layer firewalls then analyse application level traffic and filter any suspicious traffic. Examples of these would be an attempt at SQL injection, script injection, cross-site scripting, or session hijacking.
- Server firewalls on front-end servers again filter out any traffic that is not strictly defined by systems administrators during configuration as valid traffic.
- Only applications strictly necessary for services are running on the servers.
- These applications are kept up-to-date with the latest security patches, as are all of the security infrastructure components that protect them or that they run on.
- ARI infrastructure is penetration-tested by external tools and contracted security professionals for vulnerabilities to known exploits.
- ARI applications are designed, coded and tested to security standards such as OWASP and penetration-tested for vulnerabilities to common classes of exploits by external tools and contracted security professionals.
- ARI configures SELinux on its production servers. Specific details of this configuration is confidential; essentially any compromised application is extremely limited in what it can do.
- Monitoring is used to detect security incidents at all layers of the security model. Specifically:
  - Network Intrusion Detection systems are employed to monitor ARI networks for suspicious traffic.
  - ARI maintains its own host-based Intrusion Detection system based on tripwire, which has now undergone four years of development. Specific details are confidential, but in summary, the system can detect any unusual activity with respect to configuration, program files, program processes, users, or network traffic.
  - More generic monitoring systems are used as indicators of security incidents. Any behaviour outside the norm across over 1,100 individual application, database, systems, network and environmental checks is investigated.
- Capacity management components of the monitoring suite are also used to detect and classify security incidents. Some examples are:
  - Network traffic counts, packet counts and specific application query counts.
  - Long term trend data on network traffic vs. specific incident windows.
  - CPU, Storage, Memory and Process monitors on servers.
- A second layer of hardware firewalling separates application and middle tier servers from database servers.
- Applications only have as much access to database information as is required to perform their function.
- Finally, database servers have their own security standards, including server-based firewalls, vulnerability management for operating system and RDBMS software, and encryption of critical data.

### 2.1 Physical Security Infrastructure

ARI maintains a series of physical security infrastructure measures including but not limited to biometric and physical key access control to secured areas and security camera recording, alarm systems and monitoring.

### 3 COMMITMENTS TO REGISTRANTS

We commit to the following:

- Safeguarding the confidentiality, integrity and availability of registrant's data.
- Compliance with the relevant regulation and legislation with respect to privacy.
- Working with law enforcement where appropriate in response to illegal activity or at the request of law enforcement agencies.

- Maintaining a best practice information security management system that continues to be ISO27001-compliant.
- Validating requests from external parties requesting data or changes to the registry to ensure the identity of these parties and that their request is appropriate. This includes requests from ICANN.
- That access to DNS and contact administrative facilities requires multi-factor authentication by the Registrar on behalf of the registrant.- That Registry data cannot be manipulated in any fashion other than those permitted to authenticated Registrars using the EPP or the SRS web interface. Authenticated Registrars can only access Registry data of domain names sponsored by them.
- A Domain transfer can only be done by utilizing the AUTH CODE provided to the Domain Registrant.
- Those emergency procedures are in place and tested to respond to extraordinary events affecting the integrity, confidentiality or availability of data within the registry.

#### 4 AUGMENTED LEVEL OF SECURITY

This TLD is a generic TLD and as such requires security considerations that are commensurate with its purpose. Our goal with this TLD is to provide registrants with adequate protections against unauthorized changes to their names, without making the registration process too onerous and thus increasing costs.

The following attributes describe the security with respect to the TLD:

- ARI, follows the highest security standards with respect to its Registry Operations. ARI is ISO 27001 certified and has been in the business of providing a Registry backend for 10 years. ARI have confirmed their adherence to all of the security standards as described in this application. As per recommendation 24 this ensures that the technical implementations do not compromise elevated security standards
  - Registrant will only be permitted to make changes to their domain name after a authenticating to their Registrar.
  - Registrants will only be able to access all interfaces for domain registration and management via HTTPS. A reputed digital certificate vendor will provide the SSL certificate of the secure site.
  - Registrar identity will be manually verified before they are accredited within this TLD. This will include verification of corporate identity, identity of individuals involved / mentioned, and verification of contact information
  - Registrars will only be permitted to connect with the SRS via EPP after a multi-factor authentication that validates their digital identity. This is described further ahead.
  - Registrars will only be permitted to use a certificate signed by ARI to connect with the Registry systems. Self-signed certificates will not be permitted.
- The Registry is DNSSEC enabled and the TLD zone will be DNSSEC enabled. This is described in detail in our response to question 43. The following additional requirements will exist for Registrars who want to get accredited to sell this TLD:
  - Registrars must support DNSSEC capabilities within its control panels.
  - If the Registrar provides Managed DNS services to Registrants within this TLD they must provide the option for DNSSEC. This ensures that DNSSEC is deployed at each zone and subsequent sub-zones at Registry, Registrar and Registrant level as per recommendation 26.
  - Registrar access to all Registry Systems will be via TLS and secured with multi-factor authentication as per recommendation 27. This is described in detail in our responses to Question 24 and Question 25.
  - Registrant access to all Registrar and Registry Systems will be via TLS and secured with multi-factor authentication as per recommendation 28. This is described in detail in our response to Question 25, Question 27 and Question 29.
  - All communication between the Registrar or the Registrars systems and the registry system is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57. This includes the following communication:

- Secure websites and control panels provided by the Registrar to the Registrant.
- Ticketing systems provided by the Registrar to the Registrant.
- Web and EPP interfaces provided by ARI to the Registrars.
- Ticketing systems provided by ARI to the Registrar.
- Any communication between the Registrant, Registrar and Registry that is deemed as critical or contains credentials or sensitive information.

Where these requirements put controls on Registrars these will be enforced through the RRA.

## 5 RESOURCES

This function will be performed by ARI. The following resources are allocated to performing the tasks required to deliver the services described:

- Executive Management Team (4 staff)
- Production Support Group (27 staff)

ARI has ten years' experience designing, developing, deploying, securing and operating critical Registry systems, as well as TLD consulting and technology leadership.

As a technology company, ARI's senior management are technology and methodology leaders in their respective fields who ensure the organisation maintains a focus on technical excellence and hiring, training and staff management. Executive Management is heavily involved in ensuring security standards are met and that continued review and improvement is constantly undertaken. This includes the:

- Chief Operations Officer
- Chief Technology Officer

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q30a - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system. Based on past experience ARI estimates that the existing staff is adequate to support a registry system that supports in excess of 50M domains. Since this TLD projects 150000 domains, 0,3% of these resources are allocated to this TLD. See attachment 'Q30a - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

The Production Support Group is responsible for the deployment and operation of TLD registries.

The group consists of:

- Production Support Manager (also the ISO)
- Service Desk:
  - 1 Level 1 Support Team Lead
  - 8 Customer Support Representatives (Level 1 support)
  - 1 Level 2 Support Team Lead
  - 4 Registry Specialists (Level 2 support)
- Operations (Level 3 support):
  - 1 Operations Team Lead
  - 2 Systems Administrators
  - 2 Database Administrators
  - 2 Network Engineers
- Implementation:
  - 1 Project Manager
  - 2 Systems Administrators

- 1 Database Administrators
- 1 Network Engineers

ARI employs a rigorous hiring process and screening (Police background checks for technical staff and Australian Federal Government 'Protected' level security clearances for registry operations staff).

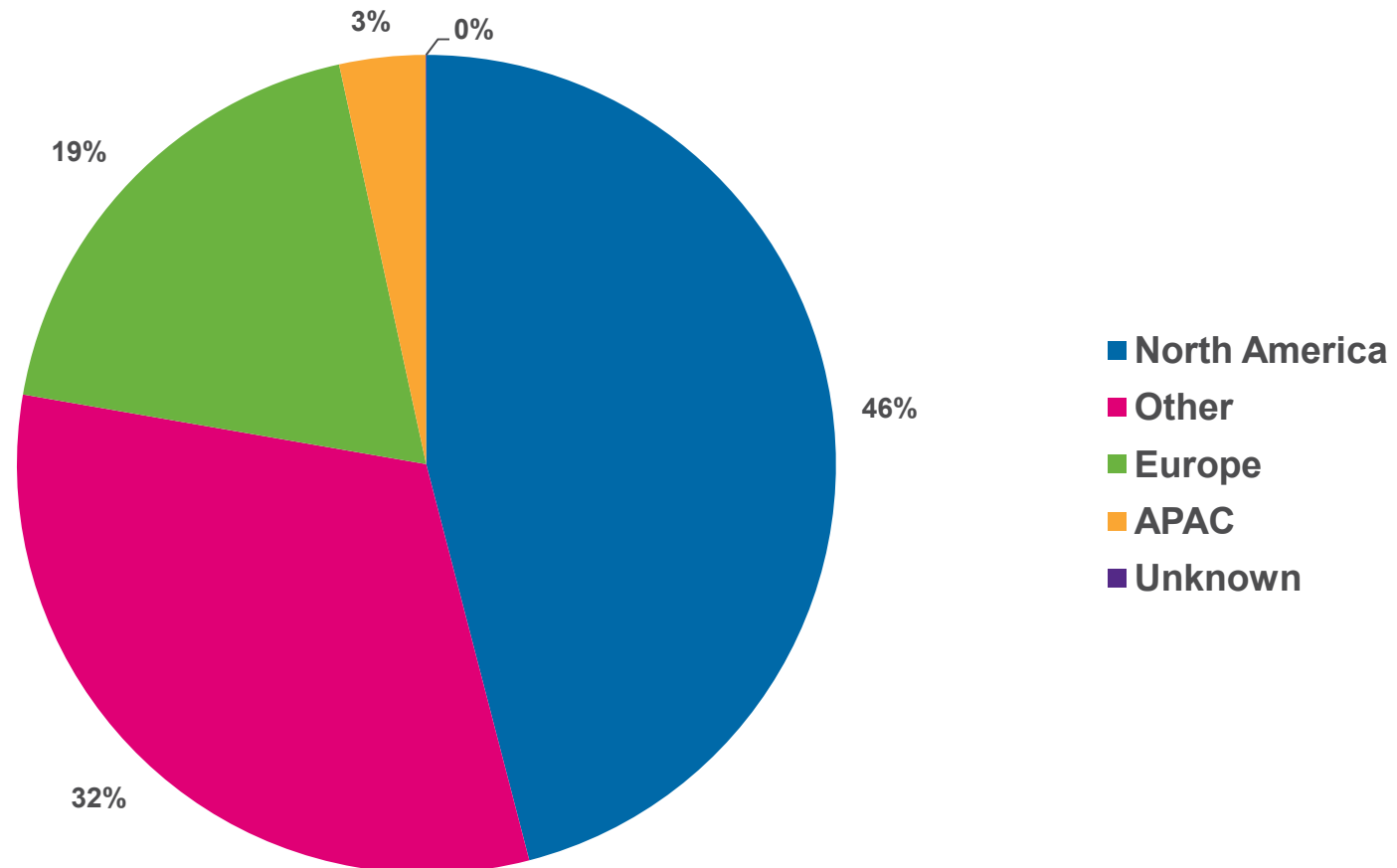
© *Internet Corporation For Assigned Names and Numbers.*



# **Annex 2.**

# Geographical Split

## *Active Websites By Region*







# **Annex 3.**



## **New gTLD Application Submitted to ICANN by: Web.com Group, Inc.**

**String: web**

**Originally Posted: 13 June 2012**

**Application ID: 1-1009-97005**

### **Applicant Information**

#### **1. Full legal name**

Web.com Group, Inc.

#### **2. Address of the principal place of business**

Contact Information Redacted

#### **3. Phone number**

Contact Information Redacted

#### **4. Fax number**

Contact Information Redacted

## 5. If applicable, website or URL

<http://www.web.com>

## Primary Contact

### 6(a). Name

Mr. Robert Conant Wiegand

### 6(b). Title

Senior Vice President

### 6(c). Address

### 6(d). Phone Number

Contact Information Redacted

### 6(e). Fax Number

### 6(f). Email Address

Contact Information Redacted

## Secondary Contact

### 7(a). Name

Mr. Matthew Patrick McClure

**7(b). Title**

Chief Legal Officer

**7(c). Address**

**7(d). Phone Number**

Contact Information Redacted

**7(e). Fax Number**

**7(f). Email Address**

Contact Information Redacted

**Proof of Legal Establishment**

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

Corporation

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

General Corporation Law of the State of Delaware

**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.**

NASDAQ; WWWW

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

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

## Applicant Background

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

Anton J. Levy	Director
David L. Brown	Chairman of the Board
Deborah H. Quazzo	Director
Hugh M. Durden	Director
Phillip J. Facchina	Director
Robert S. McCoy	Director
Timothy I. Maudlin	Director

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

David L. Brown	CEO & President
Jason M. Teichman	EVP and Chief Marketing Officer
Kevin M. Carney	EVP and Chief Financial Officer
Matthew P. McClure	Chief Legal Officer & Secretary
Roseann Duran	EVP and Chief People Officer

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

NWS Holdings	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.**

web

**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.**

Web.com Group, Inc. ("Web.com") has taken a number of steps, including consulting with Verisign, our registry services provider to ensure that there are no known operational or rendering problems concerning the .web gTLD string.

Many software applications conduct software validity checks. Applications like web browsers and desktop software will validate the use of URLs either by a validation of the known gTLDs and/or the length of the string. The gTLDs delegated during the 2004 round experienced universal acceptance issues that for the most part are resolved today.

Upon delegation of .web, Web.com intends to conduct thorough integration testing with all major software applications. Further, Web.com intends to assist customers of the .web gTLD as issues arise. Web.com understands that these items cannot be remedied alone, but Web.com will collaborate with software vendors about issues as they are discovered to ensure seamless adoption.

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

## **Mission/Purpose**

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

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

Web.com Group, Inc ("Web.com") has been in the business of helping our customers establish their online presence for over 15 years. Following our acquisition of Register.com in July 2010 and the subsequent acquisition of Network Solutions, LLC, the oldest ICANN accredited registrar, in October 2011, we have become one of the largest domain name registrars in the world with approximately 3 million customers. Web.com offers a variety of TLDs and a full suite of domain-name services, including registration, management, renewal, expiration protection and privacy services.



The creation of a .web gTLD will help to fulfill ICANN's mission of providing more competition in the online marketplace and Web.com is the perfect candidate for operating .web given its experience, global reach, and brand recognition.

Why .web?

Web.com knows from years of experience that the .com gTLD has played a revolutionary role in the advancement of global commerce and culture. In addition, the .com gTLD has had a powerful and democratizing impact, providing avenues for anyone to participate in online discourse and a growing market. There are, however, a finite number of useful second-level domains that can be applied for in .com, as ICANN knows and understands. Often other gTLDs, such as .org, .info, .biz and others either are unavailable or are not a good fit for a potential second-level domain.

In looking to expand the gTLD landscape beyond the existing robustness of gTLD offerings, an easy-to-remember and intuitively logical gTLD such as .web is a relevant addition. Consumers will instantly understand that a .web domain is an Internet website thereby ensuring quick adoption by users. Due to its ubiquitous nature, .web will compete directly with all gTLDs, both existing ones and others to be approved by ICANN. It has universal appeal to anyone looking to operate on the World Wide Web. Not only will .web introduce a new and previously unavailable range of domain choices to businesses and individuals around the world but it could also serve as a platform for a number of innovative domain-based services.

The .web gTLD will help customers launch and leverage their presence on the Internet. As a leading global provider of online marketing services to small businesses, Web.com recognizes that finding a relevant and memorable domain name can be challenging. Since many keywords and descriptive phrases associated with existing TLDs have already been registered, it is often difficult to pinpoint a domain name which contains an acceptable number of characters. Consequently, prospective registrants are many times unable to secure a unique and adequate name.

The availability of .web domains will spark competition across all industries engaging customers online by providing more opportunities for registrants to secure easily found domains. Consumer choice will increase, and in doing so, online operators will seek ways to differentiate themselves from their competition with proactive steps to build consumer trust and confidence.

Introducing .web as a gTLD choice also will inject additional inventory into the domain name marketplace. As such, it will increase competition within the Internet registry space, as well as provide avenues for increased registrar competition.

Why Web.com?

As the sole owner of the Web.com® Trademark--issued by the U.S. Patent and Trademark Office-- Web.com seeks to be the sole registry operator for the .web gTLD. Historically, Web.com has offered and will continue to provide pre-registration service for the .web gTLD through [www.register.web.com](http://www.register.web.com). We remain committed to promoting .web as a new gTLD and to expanding the competitive landscape that permeates the Internet.

Founded in 1997 as Atlantic Teleservices, Web.com has evolved to become a leading provider of Internet services for small- to medium-sized businesses ("SMBs"). Web.com is the parent company of two global domain name registrars, and further meets the Internet needs of consumers and businesses throughout their lifecycle with affordable value-added services. These services include domain-name registration; website design; search engine optimization; search engine marketing; social media and mobile products; local sales leads; ecommerce solutions; and call center services.

Headquartered in Jacksonville, FL, USA, Web.com is a publicly traded company (Nasdaq: WWWW) serving nearly three million customers, with more than 1,700 global employees in fourteen locations in North America, South America and the United Kingdom. In recognition of its rapid progress, Web.com has appeared on Deloitte's Technology Fast 500™ list in each of the past two years.

One of our primary corporate goals is to provide a broad range of online services and products that enable SMBs to establish, maintain, promote, and optimize their web presence. By providing a comprehensive and best-in-class suite of services, we are able to deliver solutions that enable small and medium-sized businesses to compete and succeed online. Customers can choose to purchase 'a la carte' solutions for specific issues, or subscribe to bundled products that meet a variety of needs.

Web.com brings a wealth of experience in providing a seamless process for customers from the first point of registration through the growth of their Internet properties. Following our acquisition of Register.com in July 2010 and the subsequent acquisition of Network Solutions in October 2011, we have become one of the largest domain name registrars in the world. Web.com offers a variety of TLDs and a full suite of domain-name services, including registration, management, renewal, expiration protection and privacy services. Web.com is also a prominent player in the Internet community through participation in numerous working groups and organizations including the Certificate Authentication Board, Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet standards development community.

Additionally, since the .web gTLD mirrors the Web.com brand, trademarks, and the character string associated with our corporate website address (www.web.com), we believe that Web.com should be the sole operator and administrator of the .web gTLD. The issuance of the .web gTLD to anyone other than Web.com would infringe on the trademark rights in Web.com and be confusingly similar to domains currently in use by Web.com such as www.register.web.com and www.dot.web.com.

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

18(b). How proposed gTLD will benefit registrants, Internet users, and others.

The .web gTLD will benefit registrants, Internet users, and others in a number of ways:

- **Increase the domain-name extension inventory:** An expanding global population results in more Internet users, coupled with increasing demand for domain name choices. The .web gTLD provides alternatives in every possible imagining of a website, from ecommerce to promotion of free expression.
- **Increased availability of generic word domain names.** For the first time in decades, generic names that have been locked down by registrants in existing gTLDs will be available in a new and easy-to-remember gTLD, which increases competition and benefits Internet users.
- **Increase online innovation:** New online properties with the .web gTLD will spur competitors to innovate in ways that will empower consumers, enabling communication instantaneously with others in their own communities and worldwide, at a low cost relative to traditional forms of media. The Internet's unique attributes create new opportunities to collaborate, exchange ideas, and promote scientific, cultural, and economic progress. These opportunities will increase when .web is introduced by ICANN and implemented and operated by Web.com.

Web.com is committed to providing best-in-class service to customers by maintaining our position as an industry leader. Our goal is to enable online users to expand their web presence and we are committed to offering a greater choice in top level domain extensions.

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

Many gTLDs introduced by ICANN will, by their nature, appeal only to certain segments of the online population, whether those communities are industries, ethnicities, or other collections of like-minded individuals and organizations. We are hopeful that the .web gTLD will have the same popularity as that of .com.

Web.com has the scalability and processes required to meet the challenges anticipated with the .web gTLD. Today we manage over 8 million domain names across hundreds of TLDs. We are committed to servicing and/or providing domain-name resolution services that adhere to industry standards. Following our existing standards of industry benchmark performance, we will continuously monitor and proactively defend the .web infrastructure and associated services in order to provide reliable services for each registrant in areas of specialty, service levels, and reputation:

- **Specialty:** As the first domain-name ICANN-accredited registrar, Web.com's Network Solutions subsidiary brings an unprecedented 25 years of domain industry experience to the community as a whole. The .web gTLD will be the baseline by which customers can incorporate new generation web-based technologies, enabling their web presence to be a highly efficient and effective communication mechanism. The experience and trust associated with Web.com will help ensure that outcome.
- **Service Levels:** Web.com has a long history of succeeding in its mission of providing world-class domain registration services. Our longstanding commitment to the highest service levels will be replicated with .web. Furthermore, we will meet or exceed the service levels mandated within the Registry Agreement enforced by ICANN as it pertains, but not limited, to the registration and resolution of the .web gTLD zone. Web.com is pleased to be working with Verisign, one of the leading Internet infrastructure companies, to launch .web. Verisign's unmatched performance in the operation of existing TLDs will ensure a high degree of service, stability and reliability.
- **Reputation:** Given our success over the course of the last 15 years, we are confident that Web.com will continue to serve customers with the best in class service as it pertains to the .web gTLD. Given the proactive safeguards we incorporate, and will continue to incorporate within the .web gTLD, we believe potential customers will register a .web gTLD in order to be associated with a secure, reliable and scalable gTLD. At Web.com, we believe that a website is only as good as the services and support behind it. With the .web gTLD, we have the opportunity to bring this same level of commitment to a gTLD.

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

As stated in 18(a) above, the .web gTLD will have a dramatic impact by increasing competition, providing more differentiation for customers and consumers, while driving innovation.

- **Competition:** The addition of a .web gTLD will increase competition across all vertical online platforms. Registrars will compete to offer .web and meet the high demand for .web second-level TLDs. Vendors in the online marketplace will seek to expand their existing footprint or pioneer new products and services with a fresh .web website. The universal appeal of a .web

URL will provide competition to every TLD, both broad-based existing ones--such as .com, .org, .biz and .info--as well as others that will be approved by ICANN, whether broad-based or narrowly targeted. Internet users will benefit from the dramatically accelerated competitive environment resulting from ICANN's adoption of .web operated by Web.com.

- **Differentiation:** The .web gTLD will quickly become as ubiquitous as .com. The .web gTLD will be the most versatile gTLD on the World Wide Web. A brand name company might choose .com; a non-profit .org; a start-up .biz; a resource site .info; and so on. But every one of those organizations' sites would be perfectly compatible with a .web second-level domain. More narrow gTLDs will provide differentiation in certain niches and markets; .web will do so in every conceivable area on the Internet, from commerce to information to community-building. The introduction of generics under a new gTLD also will provide differentiated approaches to reaching Internet users.

- **Innovation:** There is little room for continued innovation by .com registrants seeking to compete with and differentiate themselves from other .com registrants. That is not a negative reflection on .com, but rather the fact that there are a finite number of short and memorable second-level domains. With many keywords and descriptive phrases already registered, incentives to innovate decrease with each year. A land rush of .web addresses will reverse that decline and drive new innovation in web delivery and customer service.

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

Web.com will provide rewarding user experiences on two levels:

- **Registrants:** Web.com will incorporate the ability to allow various segments of the market to take advantage of registering the desired .web domain name. This includes providing the IP community with the ability to secure the .web domains affiliated or associated with their brands during a proposed Sunrise period, prior to making registrations publicly available to all. This registrant service is a natural extension of decades of experience on the part of Web.com and its holdings. Web.com may also enable registrants who have already purchased domains in other gTLDs the ability to register those domains in the .web gTLD. For registrants who are looking to improve their domain name or looking to purchase a new one, having .web will open up a new swath of choices in a gTLD that is new, fresh and directly tied to their goals of establishing their web presence. Upon enabling registrations to the general public, Web.com will incorporate a Go to Market Launch plan that will focus on ease of use, perspective registrant outreach program, and proactive communication associated with turn-key customer service. We intend to maintain our leading position that includes the lowest churn rates in the industry, which will be critical to the rollout of .web and its long-term success as a vibrant gTLD.

- **Internet users:** For users of .web gTLD websites, our enhanced efforts to prevent abusive behavior to protect the rights of others will result in a user experience that is more stable and secure than what they currently experience in other gTLDs. We fully recognize that eliminating abusive and fraudulent behavior is a difficult challenge but it is one that we will stress as we develop our plans to launch .web. Web.com plans to vigorously enforce all provisions we have outlined in the responses to Questions 28 and 29 to ensure a positive experience for all users of the .web gTLD.

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

Web.com takes its responsibilities in the operation of the .web gTLD very seriously. We have implemented a series of measures that, when taken together, will ensure that registrants have the ability to register names of their choice while ensuring that policies are in place to prevent and mitigate abusive

behavior as well as protect the rights of others.

These registration policies include:

- An Acceptable Use Policy (AUP) that clearly defines what is considered abuse and what registrants may and may not do with their .web domain names
- A name selection policy that ensures compliance with ICANN mandated restrictions on second level domains
- Support for Uniform Rapid Suspension (URS) and Uniform Domain-Name Dispute-Resolution Policy (UDRP) to mitigate trademark infringement

The gTLD will be launched in multiple phases, ensuring a stable, secure, and controlled introduction:

- Sunrise A: This initial phase will allow the trademark community the ability to secure the .web domains associated with their brands for a 60-day period - double the ICANN minimum.
- Possible Sunrise B: We are also considering a second phase which might be available for previously registered names in other gTLDs.
- Landrush: Following the Sunrise phases, this phase will allow domain registrants to register domains at a premium price point. Multiple submissions will be auctioned, with the auction provider to be named at a later date.
- General Availability: This final phase will be open to the general public. Domains may be registered on a first-come/first-serve basis.

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

Web.com respects the privacy of its customers and the visitors and users of its websites. The .web gTLD will be governed by a strict Privacy Policy to ensure the privacy of information for registrants as well as users. Web.com is an industry leader in providing transparent and rigorous policies on how sensitive information will be used, as well as preventing unauthorized access to information through vigilant use of the latest technological innovations. We will continue our commitment to privacy for our customers and website users by publicly posting our privacy policies on the registry website. Web.com will ensure compliance with all laws and regulations that govern privacy issues.

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

Web.com enables regular dialogue with its registrants by establishing and maintaining clear and secure channels of communication. Web.com has every incentive to ensure that potential and existing .web registrants understand privacy and security measures to protect their information and to assist in their adherence to the AUP in their efforts to protect Internet users.

No other registry is better equipped to deal with the communication challenges inherent in the rollout and maintenance of a gTLD with the appeal and anticipated popularity of .web.

To ensure the success of the .web launch, the company will undertake a global marketing and advertising campaign to create customer awareness and interest in the features and benefits of the .web gTLD.

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

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

As stated earlier, we take our responsibilities in this area very seriously. To demonstrate our commitment to make the .web gTLD more resistant to abusive behavior than other gTLDs that currently exist, Web.com has explored various mechanisms to help prevent abusive registrations. We were particularly impressed with the set of 31 Proposed Security, Stability and Resiliency Requirements for Financial TLDs that were developed by the Security Standards Working Group (SSWG) under the guidance of the financial services industry. Following their recommendation that all potential applicants look at these standards for their own TLDs, Web.com has completed a thorough review to determine which ones might enhance the .web gTLD experience. While not all of the proposed standards are applicable to the .web gTLD, we will endeavor to implement several of them to aid in our efforts to prevent and mitigate abusive registrations. In addition to the mechanisms described in 18 (b)(iv), we will undertake the following efforts:

- An Acceptable Use policy that clearly defines what is considered abuse and what registrants may and may not do with their domain names
- A seasoned abuse mitigation team that has years of experience in dealing with these issues
- Technological measures for removal of orphan glue records
- Efforts and measures to promote accurate and complete 'Whois'
- Requirements for .web accredited registrars to enact measures in support of these efforts
- Extended Sunrise services
- Extended trademark claims service
- Name Selection Policy
- Acceptable Use Policy
- Support for URS and UDRP
- PDDRP
- Rapid takedown or suspension where necessary
- Anti-Abuse Process
- Enhanced Authentication
- Malware Code Identification
- DNSSEC signing service
- Biannual 'WHOIS' Verification
- Participation in anti-abuse community activities

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

Web.com will launch the .web gTLD in the following phases:

- Sunrise A: This initial phase will allow the trademark community the ability to secure the .web domains associated with their brands for a 60-day period.
- Possible Sunrise B: This second phase could be available for previously registered names in other gTLDs.
- Landrush: Following the Sunrise phases, Landrush will allow registrants to register domains at a premium price point. Multiple submissions for the same domain name will be resolved through auction, with an auction provider to be named at a later date.
- General Availability: This final phase will be open to the general

public. Domains may be registered on a first-come/first-serve basis.

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

Web.com, like ICANN, has every incentive to see the .web gTLD become a ubiquitous online presence, serving Internet users globally and spurring online innovation. As such, we will institute necessary incentives to encourage rapid rollout and growing adoption of the .web gTLD, with policies to be developed and adopted in the future as necessary.

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

Web.com intends to price its domains competitively to maximize sales, while at the same time ensuring profitable, secure, and sustainable operations. It is premature to elaborate on specific policies at this stage in the process, but we intend to be responsive to market demands and share ICANN's desire to ensure a rapid spread and adoption of .web. Web.com will fully comply with all necessary and recommended notification requirements in the event that price increases are necessary.

## 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.**

In order to comply with ICANN requirements and GAC recommendations regarding the protection of geographic names, Web.com Group, Inc. ("Web.com") has developed and will implement the following measures to protect geographical names at the second and all other levels in the .web gTLD:

1. Rules for Reserving Geographical Names

Web.com will comply with Specification 5 "Schedule of Reserved Names at the Second Level in gTLD Registries" Section 5 titled "Country and Territory Names." The country and territory names contained in the following internationally recognized lists shall be initially reserved at the second level and at all other levels within the .web gTLD at which the Web.com provides for registrations:

- a. the short form (in English) of all country and territory names contained on the ISO 3166-1 list, as updated from time to time, including the European Union, which is exceptionally reserved on the ISO 3166-1 list, and its scope extended in August 1999 to any application needing to represent the name European Union;
- b. the United Nations Group of Experts on Geographical Names, Technical



Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World; and

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

2. Incorporation of GAC recommendation regarding second level geographic domains

Web.com will review and seriously consider suggestions from global government entities, public authorities and the IGO's regarding additional names with national or geographic significant at the second level.

Web.com will consider any claims of abuse, including abuse of names with national or geographic significance as serious offenses. The Abuse Prevention and Mitigation Procedures for the .web gTLD will ensure that governments, public authorities or IGO's have the ability to raise cases of concern.

3. Rules for registration and employment of geographical names.

If a decision is made by Web.com to release names reserved in Section 1 above, Web.com will follow the policy and procedures outlined in Specification 5 of the Registry agreement and will work effectively to reach agreement with the applicable government(s), provided, further, that Web.com may also propose release of these reservations, subject to review by ICANN's Governmental Advisory Committee and approval by ICANN.

## Registry Services

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

1 CUSTOMARY REGISTRY SERVICES

Please note; all figures, tables and diagrams referenced in the following response can be found in attachment titled "Attachment dot web Q23."

As Web.com Group, Inc.'s ("Web.com") selected provider of backend registry services, Verisign provides a comprehensive system and physical security solution that is designed to ensure a TLD is protected from unauthorized disclosure, alteration, insertion, or destruction of registry data. Verisign's system addresses all areas of security including information and policies, security procedures, the systems development lifecycle, physical security, system hacks, break-ins, data tampering, and other disruptions to operations. Verisign's operational environments not only meet the security criteria specified in its customer contractual agreements, thereby preventing unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with applicable standards, but also are subject to multiple independent assessments as detailed in the response to Question 30, Security Policy. Verisign's physical and system security methodology follows a mature, ongoing lifecycle that was developed and implemented many years before the development of the industry standards with which Verisign currently complies. Please see the response to Question 30, Security Policy, for details of the security features of Verisign's registry services.

Verisign's registry services fully comply with relevant standards and best current practice RFCs published by the Internet Engineering Task Force (IETF), including all successor standards, modifications, or additions relating to the DNS and name server operations including without limitation RFCs 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 3901, 4343, and 4472. Moreover, Verisign's Shared Registration System (SRS) supports the following IETF Extensible Provisioning Protocol (EPP) specifications, where the Extensible Markup Language (XML) templates and XML schemas are defined in RFC 3915, 5730, 5731, 5732, 5733, and 5734. By strictly adhering to these RFCs, Verisign helps to ensure its registry services do not create a condition that adversely affects the throughput, response time, consistency, or coherence of responses to Internet servers or end systems. Besides its leadership in authoring RFCs for EPP, Domain Name System Security Extensions (DNSSEC), and other DNS services, Verisign has created and contributed to several now well-established IETF standards and is a regular and long-standing participant in key Internet standards forums.

Figure 23-1 summarizes the technical and business components of those registry services, customarily offered by a registry operator (i.e., Verisign), that support this application. These services are currently operational and support both large and small Verisign-managed registries. Customary registry services are provided in the same manner as Verisign provides these services for its existing gTLDs.

Through these established registry services, Verisign has proven its ability to operate a reliable and low-risk registry that supports millions of transactions per day. Verisign is unaware of any potential security or stability concern related to any of these services.

Registry services defined by this application are not intended to be offered in a manner unique to the new generic top-level domain (gTLD) nor are any proposed services unique to this application's registry.

As further evidence of Verisign's compliance with ICANN mandated security and stability requirements, Verisign allocates the applicable RFCs to each of the five customary registry services (items A - E above). For each registry service, Verisign also provides evidence in Figure 23-2 of Verisign's RFC compliance and includes relevant ICANN prior-service approval actions.

#### 1.1 Critical Operations of the Registry

##### i. Receipt of Data from Registrars Concerning Registration of Domain Names and Name Servers

See Item A in Figure 23-1 and Figure 23-2.

##### ii. Provision to Registrars Status Information Relating to the Zone Servers

Verisign is Web.com's selected provider of backend registry services. Verisign registry services provisions to registrars status information relating to zone servers for the gTLD. The services also allow a domain name to be updated with clientHold, serverHold status, which removes the domain name server details from zone files. This ensures that DNS queries of the domain name are not resolved temporarily. When these hold statuses are removed, the name server details are written back to zone files and DNS queries are again resolved. Figure 23-3 describes the domain name status information and zone insertion indicator provided to registrars. The zone insertion indicator determines whether the name server details of the domain name exist in the zone file for a given domain name status. Verisign also has the capability to withdraw domain names from the zone file in near real time by changing the domain name statuses upon request by customers, courts, or legal authorities as required.

##### iii. Dissemination of TLD Zone Files

See Item B in Figure 23-1 and Figure 23-2.

#### iv. Operation of the Registry Zone Servers

Verisign is Web.com's selected provider of backend registry services. Verisign, as a company, operates zone servers and serves DNS resolution from 76 geographically distributed resolution sites located in North America, South America, Africa, Europe, Asia, and Australia. Currently, 17 DNS locations are designated primary sites, offering greater capacity than smaller sites comprising the remainder of the Verisign constellation. Verisign also uses Anycast techniques and regional Internet resolution sites to expand coverage, accommodate emergency or surge capacity, and support system availability during maintenance procedures. Verisign plans to operate Web.com's .web gTLD from a minimum of eight of its primary sites (two on the East Coast of the United States, two on the West Coast of the United States, two in Europe, and two in Asia) and expand resolution sites based on traffic volume and patterns. Further details of the geographic diversity of Verisign's zone servers are provided in the response to Question 34, Geographic Diversity. Moreover, additional details of Verisign's zone servers are provided in the response to Question 32, Architecture and the response to Question 35, DNS Service.

#### v. Dissemination of Contact and Other Information Concerning Domain Name Server Registrations

See Item C in Figure 23-1 and Figure 23-2.

#### 2 OTHER PRODUCTS OR SERVICES THE REGISTRY OPERATOR IS REQUIRED TO PROVIDE BECAUSE OF THE ESTABLISHMENT OF A CONSENSUS POLICY

Verisign, Web.com's selected provider of backend registry services, is a proven supporter of ICANN's consensus-driven, bottom-up policy development process whereby community members identify a problem, initiate policy discussions, and generate a solution that produces effective and sustained results. Verisign currently provides all of the products or services (collectively referred to as services) that the registry operator is required to provide because of the establishment of a Consensus Policy. For the .web gTLD, Verisign implements these services using the same proven processes and procedures currently in-place for all registries under Verisign's management. Furthermore, Verisign executes these services on computing platforms comparable to those of other registries under Verisign's management. Verisign's extensive experience with consensus policy required services and its proven processes to implement these services greatly minimize any potential risk to Internet security or stability. Details of these services are provided in the following subsections. It shall be noted that consensus policy services required of registrars (e.g., Whois Reminder, Expired Domain) are not included in this response. This exclusion is in accordance with the direction provided in the question's Notes column to address registry operator services.

##### 2.1 Inter-Registrar Transfer Policy (IRTP)

Technical Component: In compliance with the IRTP consensus policy, Verisign, Web.com's selected provider of backend registry services, has designed its registration systems to systematically restrict the transfer of domain names within 60 days of the initial create date. In addition, Verisign has implemented EPP and "AuthInfo" code functionality, which is used to further authenticate transfer requests. The registration system has been designed to enable compliance with the five-day transfer grace period and includes the following functionality:

- Allows the losing registrar to proactively 'ACK' or acknowledge a transfer prior to the expiration of the five-day transfer grace period
- Allows the losing registrar to proactively 'NACK' or not acknowledge a transfer prior to the expiration of the five-day transfer grace period
- Allows the system to automatically ACK the transfer request once the five-day transfer grace period has passed if the losing registrar has not proactively ACK'd or NACK'd the transfer request.

Business Component: All requests to transfer a domain name to a new registrar are handled according to the procedures detailed in the IRTP. Dispute proceedings arising from a registrar's alleged failure to abide by this policy

may be initiated by any ICANN-accredited registrar under the Transfer Dispute Resolution Policy. Web.com's compliance office serves as the first level dispute resolution provider pursuant to the associated Transfer Dispute Resolution Policy. As needed Verisign is available to offer policy guidance as issues arise.

**Security and Stability Concerns:** Verisign is unaware of any impact caused by the service on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems. By implementing the IRTP in accordance with ICANN policy, security is enhanced as all transfer commands are authenticated using the AuthInfo code prior to processing.

**ICANN Prior Approval:** Verisign has been in compliance with the IRTP since November 2004 and is available to support Web.com in a consulting capacity as needed.

**Unique to the TLD:** This service is not provided in a manner unique to the .web gTLD.

## 2.2 Add Grace Period (AGP) Limits Policy

**Technical Component:** Verisign's registry system monitors registrars' Add grace period deletion activity and provides reporting that permits Web.com to assess registration fees upon registrars that have exceeded the AGP thresholds stipulated in the AGP Limits Policy. Further, Web.com accepts and evaluates all exemption requests received from registrars and determines whether the exemption request meets the exemption criteria. Web.com maintains all AGP Limits Policy exemption request activity so that this material may be included within Web.com's Monthly Registry Operator Report to ICANN.

Registrars that exceed the limits established by the policy may submit exemption requests to Web.com for consideration. Web.com's compliance office reviews these exemption requests in accordance with the AGP Limits Policy and renders a decision. Upon request, Web.com submits associated reporting on exemption request activity to support reporting in accordance with established ICANN requirements.

**Business Component:** The Add grace period (AGP) is restricted for any gTLD operator that has implemented an AGP. Specifically, for each operator:

- During any given month, an operator may not offer any refund to an ICANN-accredited registrar for any domain names deleted during the AGP that exceed (i) 10% of that registrar's net new registrations (calculated as the total number of net adds of one-year through ten-year registrations as defined in the monthly reporting requirement of Operator Agreements) in that month, or (ii) fifty (50) domain names, whichever is greater, unless an exemption has been granted by an operator.

- Upon the documented demonstration of extraordinary circumstances, a registrar may seek from an operator an exemption from such restrictions in a specific month. The registrar must confirm in writing to the operator how, at the time the names were deleted, these extraordinary circumstances were not known, reasonably could not have been known, and were outside the registrar's control. Acceptance of any exemption will be at the sole and reasonable discretion of the operator; however "extraordinary circumstances" that reoccur regularly for the same registrar will not be deemed extraordinary.

In addition to all other reporting requirements to ICANN, Web.com identifies each registrar that has sought an exemption, along with a brief description of the type of extraordinary circumstance and the action, approval, or denial taken by the operator.

**Security and Stability Concerns:** Verisign is unaware of any impact, caused by the policy, on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems.

ICANN Prior Approval: Verisign, Web.com's backend registry services provider, has had experience with this policy since its implementation in April 2009 and is available to support Web.com in a consulting capacity as needed.

Unique to the TLD: This service is not provided in a manner unique to the .web gTLD.

### 2.3 Registry Services Evaluation Policy (RSEP)

Technical Component: Verisign, Web.com's selected provider of backend registry services, adheres to all RSEP submission requirements. Verisign has followed the process many times and is fully aware of the submission procedures, the type of documentation required, and the evaluation process that ICANN adheres to.

Business Component: In accordance with ICANN procedures detailed on the ICANN RSEP website (<http://www.icann.org/en/registries/rsep/>), all gTLD registry operators are required to follow this policy when submitting a request for new registry services.

Security and Stability Concerns: As part of the RSEP submission process, Verisign, Web.com's backend registry services provider, identifies any potential security and stability concerns in accordance with RSEP stability and security requirements. Verisign never launches services without satisfactory completion of the RSEP process and resulting approval.

ICANN Prior Approval: Not applicable.

Unique to the TLD: gTLD RSEP procedures are not implemented in a manner unique to the .web gTLD.

## 3 PRODUCTS OR SERVICES ONLY A REGISTRY OPERATOR IS CAPABLE OF PROVIDING BY REASON OF ITS DESIGNATION AS THE REGISTRY OPERATOR

Web.com plans to implement a Premium Name Service as part of launch plans for the .web gTLD. Work is still proceeding on this effort but it will be modeled after similar offerings during recent TLD launches and the reserved Premium Domain Name list will comply with all necessary ICANN regulations related to such efforts. This list will be authoritative and these names will not be available during Sunrise A&B or Landrush.

Verisign, Web.com's selected backend registry services provider, has developed a Registry-Registrar Two-Factor Authentication Service that complements traditional registration and resolution registry services. In accordance with direction provided in Question 23, Verisign details below the technical and business components of the service, identifies any potential threat to registry security or stability, and lists previous interactions with ICANN to approve the operation of the service. The Two-Factor Authentication Service is currently operational, supporting multiple registries under ICANN's purview.

Web.com is unaware of any competition issue that may require the registry service(s) listed in this response to be referred to the appropriate governmental competition authority or authorities with applicable jurisdiction. ICANN previously approved the service(s), at which time it was determined that either the service(s) raised no competitive concerns or any applicable concerns related to competition were satisfactorily addressed.

### 3.1 Two-Factor Authentication Service

Technical Component: The Registry-Registrar Two-Factor Authentication Service is designed to improve domain name security and assist registrars in protecting the accounts they manage. As part of the service, dynamic one-time passwords augment the user names and passwords currently used to process update, transfer, and/or deletion requests. These one-time passwords enable transaction processing to be based on requests that are validated both by "what users

know" (i.e., their user name and password) and "what users have" (i.e., a two-factor authentication credential with a one-time-password).

Registrars can use the one-time-password when communicating directly with Verisign's Customer Service department as well as when using the registrar portal to make manual updates, transfers, and/or deletion transactions. The Two-Factor Authentication Service is an optional service offered to registrars that execute the Registry-Registrar Two-Factor Authentication Service Agreement.

**Business Component:** There is no charge for the Registry-Registrar Two-Factor Authentication Service. It is enabled only for registrars that wish to take advantage of the added security provided by the service.

**Security and Stability Concerns:** Verisign is unaware of any impact, caused by the service, on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems. The service is intended to enhance domain name security, resulting in increased confidence and trust by registrants.

**ICANN Prior Approval:** ICANN approved the same Two-Factor Authentication Service for Verisign's use on .com and .net on 10 July 2009 (RSEP Proposal 2009004) and for .name on 16 February 2011 (RSEP Proposal 2011001).

**Unique to the TLD:** This service is not provided in a manner unique to the .web gTLD.

## Demonstration of Technical & Operational Capability

### 24. Shared Registration System (SRS) Performance

#### 1 ROBUST PLAN FOR OPERATING A RELIABLE SRS

Please note; all figures, tables and diagrams referenced in the following response can be found in attachment titled "Attachment dot web Q24."

1.1 High-Level Shared Registration System (SRS) System Description  
Verisign, Web.com Group, Inc.'s ("Web.com") selected provider of backend registry services, provides and operates a robust and reliable SRS that enables multiple registrars to provide domain name registration services in the top-level domain (TLD). Verisign's proven reliable SRS serves approximately 915 registrars, and Verisign, as a company, has averaged more than 140 million registration transactions per day. The SRS provides a scalable, fault-tolerant platform for the delivery of gTLDs through the use of a central customer database, a web interface, a standard provisioning protocol (i.e., Extensible Provisioning Protocol, EPP), and a transport protocol (i.e., Secure Sockets Layer, SSL).

The SRS components include:

- **Web Interface:** Allows customers to access the authoritative database for accounts, contacts, users, authorization groups, product catalog, product subscriptions, and customer notification messages.
- **EPP Interface:** Provides an interface to the SRS that enables registrars to use EPP to register and manage domains, hosts, and contacts.
- **Authentication Provider:** A Verisign developed application, specific to the SRS, that authenticates a user based on a login name, password, and the SSL certificate common name and client IP address.

The SRS is designed to be scalable and fault tolerant by incorporating clustering in multiple tiers of the platform. New nodes can be added to a cluster within a single tier to scale a specific tier, and if one node fails within a single tier, the services will still be available. The SRS allows registrars to manage the .web gTLD domain names in a single architecture. To flexibly accommodate the scale of its transaction volumes, as well as new technologies, Verisign employs the following design practices:

- Scale for Growth: Scale to handle current volumes and projected growth.
- Scale for Peaks: Scale to twice base capacity to withstand "registration add attacks" from a compromised registrar system.
- Limit Database CPU Utilization: Limit utilization to no more than 50 percent during peak loads.
- Limit Database Memory Utilization: Each user's login process that connects to the database allocates a small segment of memory to perform connection overhead, sorting, and data caching. Verisign's standards mandate that no more than 40 percent of the total available physical memory on the database server will be allocated for these functions.

Verisign's SRS is built upon a three-tier architecture as illustrated in Figure 24-1 and detailed here:

- Gateway Layer: The first tier, the gateway servers, uses EPP to communicate with registrars. These gateway servers then interact with application servers, which comprise the second tier.
- Application Layer: The application servers contain business logic for managing and maintaining the registry business. The business logic is particular to each TLD's business rules and requirements. The flexible internal design of the application servers allows Verisign to easily leverage existing business rules to apply to the .web gTLD. The application servers store Web.com's data in the registry database, which comprises the third and final tier. This simple, industry-standard design has been highly effective with other customers for whom Verisign provides backend registry services.
- Database Layer: The database is the heart of this architecture. It stores all the essential information provisioned from registrars through the gateway servers. Separate servers query the database, extract updated zone and Whois information, validate that information, and distribute it around the clock to Verisign's worldwide domain name resolution sites.

Scalability and Performance. Verisign, Web.com's selected backend registry services provider, implements its scalable SRS on a supportable infrastructure that achieves the availability requirements in Specification 10. Verisign employs the design patterns of simplicity and parallelism in both its software and systems, based on its experience that these factors contribute most significantly to scalability and reliable performance. Going counter to feature-rich development patterns, Verisign intentionally minimizes the number of lines of code between the end user and the data delivered. The result is a network of restorable components that provide rapid, accurate updates. Figure 24-2 depicts EPP traffic flows and local redundancy in Verisign's SRS provisioning architecture. As detailed in the figure, local redundancy is maintained for each layer as well as each piece of equipment. This built-in redundancy enhances operational performance while enabling the future system scaling necessary to meet additional demand created by the .web gTLD.

Besides improving scalability and reliability, local SRS redundancy enables Verisign to take down individual system components for maintenance and upgrades, with little to no performance impact. With Verisign's redundant design, Verisign can perform routine maintenance while the remainder of the system remains online and unaffected. For the .web gTLD registry, this flexibility minimizes unplanned downtime and provides a more consistent end-user experience.

#### 1.2 Representative Network Diagrams

Figure 24-3 provides a summary network diagram of Web.com's selected backend registry services provider's (Verisign's) SRS. This configuration at both the

primary and alternate-primary Verisign data centers provides a highly reliable backup capability. Data is continuously replicated between both sites to ensure failover to the alternate-primary site can be implemented expeditiously to support both planned and unplanned outages.

### 1.3 Number of Servers

As Web.com's selected provider of backend registry services, Verisign continually reviews its server deployments for all aspects of its registry service. Verisign evaluates usage based on peak performance objectives as well as current transaction volumes, which drive the quantity of servers in its implementations. Verisign's scaling is based on the following factors:

- Server configuration is based on CPU, memory, disk IO, total disk, and network throughput projections.
- Server quantity is determined through statistical modeling to fulfill overall performance objectives as defined by both the service availability and the server configuration.
- To ensure continuity of operations for the .web gTLD, Verisign uses a minimum of 100 dedicated servers per SRS site. These servers are virtualized to meet demand.

### 1.4 Description of Interconnectivity with Other Registry Systems

Figure 24-4 provides a technical overview of the Web.com's selected backend registry services provider's (Verisign's) SRS, showing how the SRS component fits into this larger system and interconnects with other system components.

### 1.5 Frequency of Synchronization Between Servers

As Web.com's selected provider of backend registry services, Verisign uses synchronous replication to keep the Verisign SRS continuously in sync between the two data centers. This synchronization is performed in near-real time, thereby supporting rapid failover should a failure occur or a planned maintenance outage be required.

### 1.6 Synchronization Scheme

Verisign uses synchronous replication to keep the Verisign SRS continuously in sync between the two data centers. Because the alternate-primary site is continuously up, and built using an identical design to the primary data center, it is classified as a "hot standby."

## 2 SCALABILITY AND PERFORMANCE ARE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the .web gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

## 3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Verisign, Web.com's selected provider of backend registry services, is an



experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services provided to Web.com fully accounts for this personnel-related cost, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support SRS performance:

- Application Engineers: 19
- Database Administrators: 8
- Database Engineers: 3
- Network Administrators: 11
- Network Architects: 4
- Project Managers: 25
- Quality Assurance Engineers: 11
- SRS System Administrators: 13
- Storage Administrators: 4
- Systems Architects: 9

To implement and manage the .web gTLD as described in this application, Verisign, Web.com's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only the .web gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

#### 4 EVIDENCE OF COMPLIANCE WITH SPECIFICATION 6 AND 10 TO THE REGISTRY AGREEMENT

Section 1.2 (EPP) of Specification 6, Registry Interoperability and Continuity Specifications. Verisign, Web.com's selected backend registry services provider, provides these services using its SRS, which complies fully with Specification 6, Section 1.2 of the Registry Agreement. In using its SRS to

provide backend registry services, Verisign implements and complies with relevant existing RFCs (i.e., 5730, 5731, 5732, 5733, 5734, and 5910) and intends to comply with RFCs that may be published in the future by the Internet Engineering Task Force (IETF), including successor standards, modifications, or additions thereto relating to the provisioning and management of domain names that use EPP. In addition, Verisign's SRS includes a Registry Grace Period (RGP) and thus complies with RFC 3915 and its successors. Details of the Verisign SRS' compliance with RFC SRS/EPP are provided in the response to Question 25, Extensible Provisioning Protocol. Verisign does not use functionality outside the base EPP RFCs, although proprietary EPP extensions are documented in Internet-Draft format following the guidelines described in RFC 3735 within the response to Question 25. Moreover, prior to deployment, Web.com will provide to ICANN updated documentation of all the EPP objects and extensions supported in accordance with Specification 6, Section 1.2.

Specification 10, EPP Registry Performance Specifications. Verisign's SRS meets all EPP Registry Performance Specifications detailed in Specification 10, Section 2. Evidence of this performance can be verified by a review of the .com and .net Registry Operator's Monthly Reports, which Verisign files with ICANN. These reports detail Verisign's operational status of the .com and .net registries, which use an SRS design and approach comparable to the one proposed for the .web gTLD. These reports provide evidence of Verisign's ability to meet registry operation service level agreements (SLAs) comparable to those detailed in Specification 10. The reports are accessible at the following URL: <http://www.icann.org/en/tlds/monthly-reports/>.

In accordance with EPP Registry Performance Specifications detailed in Specification 10, Verisign's SRS meets the following performance attributes:

- EPP service availability:  $\leq$  864 minutes of downtime (~98%)
- EPP session-command round trip time (RTT):  $\leq$  4000 milliseconds (ms), for at least 90 percent of the commands
- EPP query-command RTT:  $\leq$  2000 ms, for at least 90 percent of the commands
- EPP transform-command RTT:  $\leq$  4000 ms, for at least 90 percent of the commands

## 25. Extensible Provisioning Protocol (EPP)

### 1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF THIS ASPECT OF REGISTRY TECHNICAL REQUIREMENTS

Please note; all figures, tables and diagrams referenced in the following response can be found in the attachment titled "Attachment dot web Q25." All EPP schemas can be found in the attachment titled "Attachment dot web Q25 EPP schemas."

Verisign, Web.com Group, Inc.'s ("Web.com") selected backend registry services provider, has used Extensible Provisioning Protocol (EPP) since its inception and possesses complete knowledge and understanding of EPP registry systems. Its first EPP implementation— for a thick registry for the .name generic top-level domain (gTLD)—was in 2002. Since then Verisign has continued its RFC-compliant use of EPP in multiple TLDs, as detailed in Figure 25-1.

Verisign's understanding of EPP and its ability to implement code that complies with the applicable RFCs is unparalleled. Mr. Scott Hollenbeck, Verisign's director of software development, authored the Extensible Provisioning Protocol and continues to be fully engaged in its refinement and enhancement (U.S. Patent Number 7299299 - Shared registration system for registering domain names). Verisign has also developed numerous new object mappings and object extensions following the guidelines in RFC 3735 (Guidelines for Extending the Extensible Provisioning Protocol). Mr. James Gould, a principal engineer at

Verisign, led and co-authored the most recent EPP Domain Name System Security Extensions (DNSSEC) RFC effort (RFC 5910).

All registry systems for which Verisign is the registry operator or provides backend registry services use EPP. Upon approval of this application, Verisign will use EPP to provide the backend registry services for this gTLD. The .com, .net, and .name registries for which Verisign is the registry operator use an SRS design and approach comparable to the one proposed for this gTLD. Approximately 915 registrars use the Verisign EPP service, and the registry system performs more than 140 million EPP transactions daily without performance issues or restrictive maintenance windows. The processing time service level agreement (SLA) requirements for the Verisign-operated .net gTLD are the strictest of the current Verisign managed gTLDs. All processing times for Verisign-operated gTLDs can be found in ICANN's Registry Operator's Monthly Reports at <http://www.icann.org/en/tlds/monthly-reports/>.

Verisign has also been active on the Internet Engineering Task Force (IETF) Provisioning Registry Protocol (provreg) working group and mailing list since work started on the EPP protocol in 2000. This working group provided a forum for members of the Internet community to comment on Mr. Scott Hollenbeck's initial EPP drafts, which Mr. Hollenbeck refined based on input and discussions with representatives from registries, registrars, and other interested parties. The working group has since concluded, but the mailing list is still active to enable discussion of different aspects of EPP.

#### 1.1 EPP Interface with Registrars

Verisign, Web.com's selected backend registry services provider, fully supports the features defined in the EPP specifications and provides a set of software development kits (SDK) and tools to help registrars build secure and stable interfaces. Verisign's SDKs give registrars the option of either fully writing their own EPP client software to integrate with the Shared Registration System (SRS), or using the Verisign-provided SDKs to aid them in the integration effort. Registrars can download the Verisign EPP SDKs and tools from the registrar website (<http://www.Verisign.com/domain-name-services/current-registrars/epp-sdk/index.html>).

The EPP SDKs provide a host of features including connection pooling, Secure Sockets Layer (SSL), and a test server (stub server) to run EPP tests against. One tool—the EPP tool—provides a web interface for creating EPP Extensible Markup Language (XML) commands and sending them to a configurable set of target servers. This helps registrars in creating the template XML and testing a variety of test cases against the EPP servers. An Operational Test and Evaluation (OT&E) environment, which runs the same software as the production system so approved registrars can integrate and test their software before moving into a live production environment, is also available.

## 2 TECHNICAL PLAN SCOPE/SCALE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the .web gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain the .web gTLD. Verisign's pricing for the backend

registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support the provisioning of EPP services:

- Application Engineers: 19
- Database Engineers: 3
- Quality Assurance Engineers: 11

To implement and manage the .web gTLD as described in this application, Verisign, Web.com's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only the .web gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and the .web gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 ABILITY TO COMPLY WITH RELEVANT RFCS

Verisign, Web.com's selected backend registry services provider, incorporates design reviews, code reviews, and peer reviews into its software development lifecycle (SDLC) to ensure compliance with the relevant RFCs. Verisign's dedicated QA team creates extensive test plans and issues internal

certifications when it has confirmed the accuracy of the code in relation to the RFC requirements. Verisign's QA organization is independent from the development team within engineering. This separation helps Verisign ensure adopted processes and procedures are followed, further ensuring that all software releases fully consider the security and stability of the .web gTLD.

For the .web gTLD, the Shared Registration System (SRS) complies with the following IETF EPP specifications, where the XML templates and XML schemas are defined in the following specifications:

- EPP RGP 3915 (<http://www.apps.ietf.org/rfc/rfc3915.html>): EPP Redemption Grace Period (RGP) Mapping specification for support of RGP statuses and support of Restore Request and Restore Report (authored by Verisign's Scott Hollenbeck)
- EPP 5730 (<http://tools.ietf.org/html/rfc5730>): Base EPP specification (authored by Verisign's Scott Hollenbeck)
- EPP Domain 5731 (<http://tools.ietf.org/html/rfc5731>): EPP Domain Name Mapping specification (authored by Verisign's Scott Hollenbeck)
- EPP Host 5732 (<http://tools.ietf.org/html/rfc5732>): EPP Host Mapping specification (authored by Verisign's Scott Hollenbeck)
- EPP Contact 5733 (<http://tools.ietf.org/html/rfc5733>): EPP Contact Mapping specification (authored by Verisign's Scott Hollenbeck)
- EPP TCP 5734 (<http://tools.ietf.org/html/rfc5734>): EPP Transport over Transmission Control Protocol (TCP) specification (authored by Verisign's Scott Hollenbeck)
- EPP DNSSEC 5910 (<http://tools.ietf.org/html/rfc5910>): EPP Domain Name System Security Extensions (DNSSEC) Mapping specification (authored by Verisign's James Gould and Scott Hollenbeck)

## 5 PROPRIETARY EPP EXTENSIONS

Verisign, Web.com's selected backend registry services provider, uses its SRS to provide registry services. The SRS supports the following EPP specifications, which Verisign developed following the guidelines in RFC 3735, where the XML templates and XML schemas are defined in the specifications:

- IDN Language Tag (<http://www.verisigninc.com/assets/idn-language-tag.pdf>): EPP internationalized domain names (IDN) language tag extension used for IDN domain name registrations
- RGP Poll Mapping (<http://www.verisigninc.com/assets/whois-info-extension.pdf>): EPP mapping for an EPP poll message in support of Restore Request and Restore Report
- Whois Info Extension (<http://www.verisigninc.com/assets/whois-info-extension.pdf>): EPP extension for returning additional information needed for transfers
- EPP ConsoliDate Mapping (<http://www.verisigninc.com/assets/consolidate-mapping.txt>): EPP mapping to support a Domain Sync operation for synchronizing domain name expiration dates
- NameStore Extension (<http://www.verisigninc.com/assets/namestore-extension.pdf>): EPP extension for routing with an EPP intelligent gateway to a pluggable set of backend products and services
- Low Balance Mapping (<http://www.verisigninc.com/assets/low-balance-mapping.pdf>): EPP mapping to support low balance poll messages that proactively notify registrars of a low balance (available credit) condition

As part of the 2006 implementation report to bring the EPP RFC documents from Proposed Standard status to Draft Standard status, an implementation test matrix was completed. Two independently developed EPP client implementations based on the RFCs were tested against the Verisign EPP server for the domain, host, and contact transactions. No compliance related issues were identified during this test, providing evidence that these extensions comply with RFC 3735 guidelines and further demonstrating Verisign's ability to design, test, and deploy an RFC-compliant EPP implementation.

### 5.1 EPP Templates and Schemas

The EPP XML schemas are formal descriptions of the EPP XML templates. They are used to express the set of rules to which the EPP templates must conform in order to be considered valid by the schema. The EPP schemas define the building

blocks of the EPP templates, describing the format of the data and the different EPP commands' request and response formats. The current EPP implementations managed by Verisign, Web.com's selected backend registry services provider, use these EPP templates and schemas, as will the .web gTLD. For each proprietary XML template/schema Verisign provides a reference to the applicable template and includes the schema. These schema can be found in the attachment titled "dot web Q25 EPP Schemas."

6 PROPRIETARY EPP EXTENSION CONSISTENCY WITH REGISTRATION LIFECYCLE  
Web.com's selected backend registry services provider's (Verisign's) proprietary EPP extensions, defined in Section 5 above, are consistent with the registration lifecycle documented in the response to Question 27, Registration Lifecycle. Details of the registration lifecycle are presented in that response. As new registry features are required, Verisign develops proprietary EPP extensions to address new operational requirements. Consistent with ICANN procedures Verisign adheres to all applicable Registry Services Evaluation Process (RSEP) procedures.

## 26. Whois

1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF THIS ASPECT OF REGISTRY  
TECHNICAL REQUIREMENTS

Please note; all figures, tables and diagrams referenced in the following response can be found in the attachment titled "Attachment dot web Q26."

Verisign, Web.com Group, Inc.'s ("Web.com") selected backend registry services provider, has operated the Whois lookup service for the gTLDs and ccTLDs it manages since 1991, and will provide these proven services for the .web gTLD registry. In addition, it continues to work with the Internet community to improve the utility of Whois data, while thwarting its application for abusive uses.

### 1.1 High-Level Whois System Description

Like all other components of Web.com's selected backend registry services provider's (Verisign's) registry service, Verisign's Whois system is designed and built for both reliability and performance in full compliance with applicable RFCs. Verisign's current Whois implementation has answered more than five billion Whois queries per month for the TLDs it manages, and has experienced more than 250,000 queries per minute in peak conditions. The .web gTLD will use a Whois system design and approach that is comparable to the current implementation. Independent quality control testing ensures Verisign's Whois service is RFC-compliant through all phases of its lifecycle.

Verisign's redundant Whois databases further contribute to overall system availability and reliability. The hardware and software for its Whois service is architected to scale both horizontally (by adding more servers) and vertically (by adding more CPUs and memory to existing servers) to meet future need.

Verisign can fine-tune access to its Whois database on an individual Internet Protocol (IP) address basis, and it works with registrars to help ensure their services are not limited by any restriction placed on Whois. Verisign provides near real-time updates for Whois services for the TLDs under its management. As information is updated in the registration database, it is propagated to the Whois servers for quick publication. These updates align with the near real-time publication of Domain Name System (DNS) information as it is updated in the registration database. This capability is important for the .web gTLD registry as it is Verisign's experience that when DNS data is updated in near real time, so should Whois data be updated to reflect the registration specifics of those domain names.

Verisign's Whois response time has been less than 500 milliseconds for 95 percent of all Whois queries in .com, .net, .tv, and .cc. The response time in these TLDs, combined with Verisign's capacity, enables the Whois system to respond to up to 30,000 searches (or queries) per second for a total capacity of 2.6 billion queries per day.

The Whois software written by Verisign complies with RFC 3912. Verisign uses an advanced in-memory database technology to provide exceptional overall system performance and security. In accordance with RFC 3912, Verisign provides a website at whois.nic.<TLD> that provides free public query-based access to the registration data.

Verisign currently operates both thin and thick Whois systems.

Verisign commits to implementing a RESTful Whois service upon finalization of agreements with the IETF (Internet Engineering Task Force).

#### Provided Functionalities for User Interface

To use the Whois service via port 43, the user enters the applicable parameter on the command line as illustrated here:

- For domain name: whois EXAMPLE.TLD
- For registrar: whois "registrar Example Registrar, Inc."
- For name server: whois "NS1.EXAMPLE.TLD" or whois "name server (IP address)"

To use the Whois service via the web-based directory service search interface:

- Go to <http://whois.nic.<TLD>>
- Click on the appropriate button (Domain, Registrar, or Name Server)
- Enter the applicable parameter:
  - Domain name, including the TLD (e.g., EXAMPLE.TLD)
  - Full name of the registrar, including punctuation (e.g., Example Registrar, Inc.)
  - Full host name or the IP address (e.g., NS1.EXAMPLE.TLD or 198.41.3.39)
- Click on the Submit button.

#### Provisions to Ensure That Access Is Limited to Legitimate Authorized Users and Is in Compliance with Applicable Privacy Laws or Policies

To further promote reliable and secure Whois operations, Verisign, Web.com's selected backend registry services provider, has implemented rate-limiting characteristics within the Whois service software. For example, to prevent data mining or other abusive behavior, the service can throttle a specific requestor if the query rate exceeds a configurable threshold. In addition, QoS technology enables rate limiting of queries before they reach the servers, which helps protect against denial of service (DoS) and distributed denial of service (DDoS) attacks.

Verisign's software also permits restrictions on search capabilities. For example, wild card searches can be disabled. If needed, it is possible to temporarily restrict and/or block requests coming from specific IP addresses for a configurable amount of time. Additional features that are configurable in the Whois software include help files, headers and footers for Whois query responses, statistics, and methods to memory map the database. Furthermore, Verisign is European Union (EU) Safe Harbor certified and has worked with European data protection authorities to address applicable privacy laws by developing a tiered Whois access structure that requires users who require access to more extensive data to (i) identify themselves, (ii) confirm that their use is for a specified purpose and (iii) enter into an agreement governing their use of the more extensive Whois data.

## 1.2 Relevant Network Diagrams

Figure 26-1 provides a summary network diagram of the Whois service provided by Verisign, Web.com's selected backend registry services provider. The figure details the configuration with one resolution/Whois site. For the .web gTLD Verisign provides Whois service from 6 of its 17 primary sites based on the proposed gTLD's traffic volume and patterns. A functionally equivalent resolution architecture configuration exists at each Whois site.

### 1.3 IT and Infrastructure Resources

Figure 26-2 summarizes the IT and infrastructure resources that Verisign, Web.com's selected backend registry services provider, uses to provision Whois services from Verisign primary resolution sites. As needed, virtual machines are created based on actual and projected demand.

### 1.4 Description of Interconnectivity with Other Registry Systems

Figure 26-3 provides a technical overview of the registry system provided by Verisign, Web.com's selected backend registry services provider, and shows how the Whois service component fits into this larger system and interconnects with other system components.

### 1.5 Frequency of Synchronization Between Servers

Synchronization between the SRS and the geographically distributed Whois resolution sites occurs approximately every three minutes. Verisign, Web.com's selected backend registry services provider, uses a two-part Whois update process to ensure Whois data is accurate and available. Every 12 hours an initial file is distributed to each resolution site. This file is a complete copy of all Whois data fields associated with each domain name under management. As interactions with the SRS cause the Whois data to be changed, these incremental changes are distributed to the resolution sites as an incremental file update. This incremental update occurs approximately every three minutes. When the new 12-hour full update is distributed, this file includes all past incremental updates. Verisign's approach to frequency of synchronization between servers meets the Performance Specifications defined in Specification 10 of the Registry Agreement for new gTLDs.

## 2 TECHNICAL PLAN SCOPE/SCALE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the .web gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

## 3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to



continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support Whois services:

- Application Engineers: 19
- Database Engineers: 3
- Quality Assurance Engineers: 11

To implement and manage the .web gTLD as described in this application, Verisign, Web.com's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only the .web gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and the .web gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

#### 4 COMPLIANCE WITH RELEVANT RFC

Web.com's selected backend registry services provider's (Verisign's) Whois service complies with the data formats defined in Specification 4 of the Registry Agreement. Verisign will provision Whois services for registered domain names and associated data in the top-level domain (TLD). Verisign's Whois services are accessible over Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6), via both Transmission Control Protocol (TCP) port 43 and a web-based directory service at whois.nic.<TLD>, which in accordance with RFC 3912, provides free public query-based access to domain name, registrar, and name server lookups. Verisign's proposed Whois system meets all requirements as defined by ICANN for each registry under Verisign management. Evidence of this successful implementation, and thus compliance with the applicable RFCs, can be verified by a review of the .com and .net Registry Operator's Monthly Reports that Verisign files with ICANN. These reports provide evidence of Verisign's ability to meet registry operation service level agreements (SLAs) comparable to those detailed in Specification 10. The reports are accessible at the following URL:

<http://www.icann.org/en/tlds/monthly-reports/>.

5 COMPLIANCE WITH SPECIFICATIONS 4 AND 10 OF REGISTRY AGREEMENT  
In accordance with Specification 4, Verisign, Web.com's selected backend registry services provider, provides a Whois service that is available via both port 43 in accordance with RFC 3912, and a web-based directory service at whois.nic.web also in accordance with RFC 3912, thereby providing free public query-based access. Verisign acknowledges that ICANN reserves the right to specify alternative formats and protocols, and upon such specification, Verisign will implement such alternative specification as soon as reasonably practicable.

The format of the following data fields conforms to the mappings specified in Extensible Provisioning Protocol (EPP) RFCs 5730 - 5734 so the display of this information (or values returned in Whois responses) can be uniformly processed and understood: domain name status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers, email addresses, date, and times.

Specifications for data objects, bulk access, and lookups comply with Specification 4 and are detailed in the following subsections, provided in both bulk access and lookup modes.

Bulk Access Mode. This data is provided on a daily schedule to a party designated from time to time in writing by ICANN. The specification of the content and format of this data, and the procedures for providing access, shall be as stated below, until revised in the ICANN Registry Agreement.

The data is provided in three files:

- Domain Name File: For each domain name, the file provides the domain name, server name for each name server, registrar ID, and updated date.
- Name Server File: For each registered name server, the file provides the server name, each IP address, registrar ID, and updated date.
- Registrar File: For each registrar, the following data elements are provided: registrar ID, registrar address, registrar telephone number, registrar email address, Whois server, referral URL, updated date, and the name, telephone number, and email address of all the registrar's administrative, billing, and technical contacts.

Lookup Mode. Figures 26-4 through Figure 26-6 provide the query and response format for domain name, registrar, and name server data objects.

5.1 Specification 10, RDDS Registry Performance Specifications  
The Whois service meets all registration data directory services (RDDS) registry performance specifications detailed in Specification 10, Section 2. Evidence of this performance can be verified by a review of the .com and .net Registry Operator's Monthly Reports that Verisign files monthly with ICANN. These reports are accessible from the ICANN website at the following URL:  
<http://www.icann.org/en/tlds/monthly-reports/>.

In accordance with RDDS registry performance specifications detailed in Specification 10, Verisign's Whois service meets the following proven performance attributes:

- RDDS availability:  $\leq 864$  min of downtime (~98%)
- RDDS query RTT:  $\leq 2000$  ms, for at least 95% of the queries
- RDDS update time:  $\leq 60$  min, for at least 95% of the probes

## 6 SEARCHABLE WHOIS

Verisign, Web.com's selected backend registry services provider, provides a searchable Whois service for the .web gTLD. Verisign has experience in providing tiered access to Whois for the .name registry, and uses these methods and control structures to help reduce potential malicious use of the function.

The searchable Whois system currently uses Apache's Lucene full text search engine to index relevant Whois content with near-real time incremental updates from the provisioning system.

Features of the Verisign searchable Whois function include:

- Provision of a web-based searchable directory service
- Ability to perform partial match, at least, for the following data fields: domain name, contacts and registrant's name, and contact and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state, or province)
- Ability to perform exact match, at least, on the following fields: registrar ID, name server name, and name server's IP address (only applies to IP addresses stored by the registry, i.e., glue records)
- Ability to perform Boolean search supporting, at least, the following logical operators to join a set of search criteria: AND, OR, NOT
- Search results that include domain names that match the selected search criteria

Verisign's implementation of searchable Whois is EU Safe Harbor certified and includes appropriate access control measures that help ensure that only legitimate authorized users can use the service. Furthermore, Verisign's compliance office monitors current ICANN policy and applicable privacy laws or policies to help ensure the solution is maintained within compliance of applicable regulations. Features of these access control measures include:

- All unauthenticated searches are returned as thin results.
- Registry system authentication is used to grant access to appropriate users for thick Whois data search results.
- Account access is granted by the Web.com defined .web gTLD admin user.

Potential Forms of Abuse and Related Risk Mitigation. Leveraging its experience providing tiered access to Whois for the .name registry and interacting with ICANN, data protection authorities, and applicable industry groups, Verisign, Web.com's selected backend registry services provider, is knowledgeable of the likely data mining forms of abuse associated with a searchable Whois service. Figure 26-7 summarizes these potential forms of abuse and Verisign's approach to mitigate the identified risk.

## 27. Registration Life Cycle

### 1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF REGISTRATION LIFECYCLES AND STATES

Please note; all figures, tables and diagrams referenced in the following response can be found in the attachment titled "Attachment dot web Q27." Starting with domain name registration and continuing through domain name delete operations, Web.com Group, Inc.'s ("Web.com") selected backend registry services provider's (Verisign's) registry implements the full registration lifecycle for domain names supporting the operations in the Extensible Provisioning Protocol (EPP) specification. The registration lifecycle of the domain name starts with registration and traverses various states as specified in the following sections. The registry system provides options to update domain names with different server and client status codes that block operations based on the EPP specification. The system also provides different grace periods for different billable operations, where the price of the billable operation is credited back to the registrar if the billable operation is removed within the grace period. Together Figure 27-1 and Figure 27-2 define the registration states comprising the registration lifecycle and explain the

trigger points that cause state-to-state transitions. States are represented as green rectangles within Figure 27-1.

### 1.1 Registration Lifecycle of Create/Update/Delete

The following section details the create/update/delete processes and the related renewal process that Verisign, Web.com's selected backend registry services provider, follows. For each process, this response defines the process function and its characterization, and as appropriate provides a process flow chart.

**Create Process.** The domain name lifecycle begins with a registration or what is referred to as a Domain Name Create operation in EPP. The system fully supports the EPP Domain Name Mapping as defined by RFC 5731, where the associated objects (e.g., hosts and contacts) are created independent of the domain name.

**Process Characterization.** The Domain Name Create command is received, validated, run through a set of business rules, persisted to the database, and committed in the database if all business rules pass. The domain name is included with the data flow to the DNS and Whois resolution services. If no name servers are supplied, the domain name is not included with the data flow to the DNS. A successfully created domain name has the created date and expiration date set in the database. Creates are subject to grace periods as described in Section 1.3 of this response, Add Grace Period, Redemption Grace Period, and Notice Periods for Renewals or Transfers.

The Domain Name Create operation is detailed in Figure 27-3 and requires the following attributes:

- A domain name that meets the string restrictions.
- A domain name that does not already exist.
- The registrar is authorized to create a domain name in .web.
- The registrar has available credit.
- A valid Authorization Information (Auth-Info) value.
- Required contacts (e.g., registrant, administrative contact, technical contact, and billing contact) are specified and exist.
- The specified name servers (hosts) exist, and there is a maximum of 13 name servers.
- A period in units of years with a maximum value of 10 (default period is one year).

**Renewal Process.** The domain name can be renewed unless it has any form of Pending Delete, Pending Transfer, or Renew Prohibited.

A request for renewal that sets the expiry date to more than ten years in the future is denied. The registrar must pass the current expiration date (without the timestamp) to support the idempotent features of EPP, where sending the same command a second time does not cause unexpected side effects.

Automatic renewal occurs when a domain name expires. On the expiration date, the registry extends the registration period one year and debits the registrar account balance. In the case of an auto-renewal of the domain name, a separate Auto-Renew grace period applies. Renewals are subject to grace periods as described in Section 1.3 of this response, Add Grace Period, Redemption Grace Period, and Notice Periods for Renewals or Transfers.

**Process Characterization.** The Domain Name Renew command is received, validated, authorized, and run through a set of business rules. The data is updated and committed in the database if it passes all business rules. The updated domain name's expiration date is included in the flow to the Whois resolution service.

The Domain Name Renew operation is detailed in Figure 27-4 and requires the following attributes:

- A domain name that exists and is sponsored by the requesting registrar.
- The registrar is authorized to renew a domain name in .web.
- The registrar has available credit.
- The passed current expiration date matches the domain name's expiration date.
- A period in units of years with a maximum value of 10 (default period is one year). A domain name expiry past ten years is not allowed.

Registrar Transfer Procedures. A registrant may transfer his/her domain name from his/her current registrar to another registrar. The database system allows a transfer as long as the transfer is not within the initial 60 days, per industry standard, of the original registration date.

The registrar transfer process goes through many process states, which are described in detail below, unless it has any form of Pending Delete, Pending Transfer, or Transfer Prohibited.

A transfer can only be initiated when the appropriate Auth-Info is supplied. The Auth-Info for transfer is only available to the current registrar. Any other registrar requesting to initiate a transfer on behalf of a registrant must obtain the Auth-Info from the registrant.

The Auth-Info is made available to the registrant upon request. The registrant is the only party other than the current registrar that has access to the Auth-Info. Registrar transfer entails a specified extension of the expiry date for the object. The registrar transfer is a billable operation and is charged identically to a renewal for the same extension of the period. This period can be from one to ten years, in one-year increments.

Because registrar transfer involves an extension of the registration period, the rules and policies applying to how the resulting expiry date is set after transfer are based on the renewal policies on extension.

Per industry standard, a domain name cannot be transferred to another registrar within the first 60 days after registration. This restriction continues to apply if the domain name is renewed during the first 60 days. Transfer of the domain name changes the sponsoring registrar of the domain name, and also changes the child hosts (ns1.sample.xyz) of the domain name (sample .xyz).

The domain name transfer consists of five separate operations:

- Transfer Request (Figure 27-5): Executed by a non-sponsoring registrar with the valid Auth-Info provided by the registrant. The Transfer Request holds funds of the requesting registrar but does not bill the registrar until the transfer is completed. The sponsoring registrar receives a Transfer Request poll message.
- Transfer Cancel (Figure 27-6): Executed by the requesting registrar to cancel the pending transfer. The held funds of the requesting registrar are reversed. The sponsoring registrar receives a Transfer Cancel poll message.
- Transfer Approve (Figure 27-7): Executed by the sponsoring registrar to approve the Transfer Request. The requesting registrar is billed for the Transfer Request and the sponsoring registrar is credited for an applicable Auto-Renew grace period. The requesting registrar receives a Transfer Approve poll message.
- Transfer Reject (Figure 27-8): Executed by the sponsoring registrar to reject the pending transfer. The held funds of the requesting registrar are reversed. The requesting registrar receives a Transfer Reject poll message.
- Transfer Query (Figure 27-9): Executed by either the requesting registrar or the sponsoring registrar of the last transfer.

The registry auto-approves a transfer if the sponsoring registrar takes no action. The requesting registrar is billed for the Transfer Request and the sponsoring registrar is credited for an applicable Auto-Renew grace period. The requesting registrar and the sponsoring registrar receive a Transfer Auto-

Approve poll message.

Delete Process. A registrar may choose to delete the domain name at any time.

Process Characterization. The domain name can be deleted, unless it has any form of Pending Delete, Pending Transfer, or Delete Prohibited.

A domain name is also prohibited from deletion if it has any in-zone child hosts that are name servers for domain names. For example, the domain name "sample.xyz" cannot be deleted if an in-zone host "ns.sample.xyz" exists and is a name server for "sample2.xyz."

If the Domain Name Delete occurs within the Add grace period, the domain name is immediately deleted and the sponsoring registrar is credited for the Domain Name Create. If the Domain Name Delete occurs outside the Add grace period, it follows the Redemption grace period (RGP) lifecycle.

Update Process. The sponsoring registrar can update the following attributes of a domain name:

- Auth-Info
- Name servers
- Contacts (i.e., registrant, administrative contact, technical contact, and billing contact)
- Statuses (e.g., Client Delete Prohibited, Client Hold, Client Renew Prohibited, Client Transfer Prohibited, Client Update Prohibited)

Process Characterization. Updates are allowed provided that the update includes the removal of any Update Prohibited status. The Domain Name Update operation is detailed in Figure 27-10. A domain name can be updated unless it has any form of Pending Delete, Pending Transfer, or Update Prohibited.

#### 1.2 Pending, Locked, Expired, and Transferred

Verisign, Web.com's selected backend registry services provider, handles pending, locked, expired, and transferred domain names as described here. When the domain name is deleted after the five-day Add grace period, it enters into the Pending Delete state. The registrant can return its domain name to active any time within the five-day Pending Delete grace period. After the five-day Pending Delete grace period expires, the domain name enters the Redemption Pending state and then is deleted by the system. The registrant can restore the domain name at any time during the Redemption Pending state.

When a non-sponsoring registrar initiates the domain name transfer request, the domain name enters Pending Transfer state and a notification is mailed to the sponsoring registrar for approvals. If the sponsoring registrar doesn't respond within five days, the Pending Transfer expires and the transfer request is automatically approved.

EPP specifies both client (registrar) and server (registry) status codes that can be used to prevent registry changes that are not intended by the registrant. Currently, many registrars use the client status codes to protect against inadvertent modifications that would affect their customers' high-profile or valuable domain names.

Verisign's registry service supports the following client (registrar) and server (registry) status codes:

- clientHold
- clientRenewProhibited
- clientTransferProhibited
- clientUpdateProhibited
- clientDeleteProhibited
- serverHold
- serverRenewProhibited

- serverTransferProhibited
- serverUpdateProhibited
- serverDeleteProhibited

### 1.3 Add Grace Period, Redemption Grace Period, and Notice Periods for Renewals or Transfers

Verisign, Web.com's selected backend registry services provider, handles Add grace periods, Redemption grace periods, and notice periods for renewals or transfers as described here.

- Add Grace Period: The Add grace period is a specified number of days following the initial registration of the domain name. The current value of the Add grace period for all registrars is five days.
- Redemption Grace Period: If the domain name is deleted after the five-day grace period expires, it enters the Redemption grace period and then is deleted by the system. The registrant has an option to use the Restore Request command to restore the domain name within the Redemption grace period. In this scenario, the domain name goes to Pending Restore state if there is a Restore Request command within 30 days of the Redemption grace period. From the Pending Restore state, it goes either to the OK state, if there is a Restore Report Submission command within seven days of the Restore Request grace period, or a Redemption Period state if there is no Restore Report Submission command within seven days of the Restore Request grace period.
- Renew Grace Period: The Renew/Extend grace period is a specified number of days following the renewal/extension of the domain name's registration period. The current value of the Renew/Extend grace period is five days.
- Auto-Renew Grace Period: All auto-renewed domain names have a grace period of 45 days.
- Transfer Grace Period: Domain names have a five-day Transfer grace period.

1.4 Aspects of the Registration Lifecycle Not Covered by Standard EPP RFCs  
Web.com's selected backend registry services provider's (Verisign's) registration lifecycle processes and code implementations adhere to the standard EPP RFCs related to the registration lifecycle. By adhering to the RFCs, Verisign's registration lifecycle is complete and addresses each registration-related task comprising the lifecycle. No aspect of Verisign's registration lifecycle is not covered by one of the standard EPP RFCs and thus no additional definitions are provided in this response.

2 CONSISTENCY WITH ANY SPECIFIC COMMITMENTS MADE TO REGISTRANTS AS ADAPTED TO THE OVERALL BUSINESS APPROACH FOR THE PROPOSED gTLD  
The registration lifecycle described above applies to the .web gTLD as well as other TLDs managed by Verisign, Web.com's selected backend registry services provider; thus Verisign remains consistent with commitments made to its registrants. No unique or specific registration lifecycle modifications or adaptations are required to support the overall business approach for the .web gTLD.

To accommodate a range of registries, Verisign's registry implementation is capable of offering both a thin and thick Whois implementation, which is also built upon Verisign's award-winning ATLAS infrastructure.

3 COMPLIANCE WITH RELEVANT RFCs  
Web.com's selected backend registry services provider's (Verisign's) registration lifecycle complies with applicable RFCs, specifically RFCs 5730 - 5734 and 3915. The system fully supports the EPP Domain Name Mapping as defined by RFC 5731, where the associated objects (e.g., hosts and contacts) are created independent of the domain name.

In addition, in accordance with RFCs 5732 and 5733, the Verisign registration system enforces the following domain name registration constraints:

- Uniqueness/Multiplicity: A second-level domain name is unique in the .web database. Two identical second-level domain names cannot simultaneously exist in .web. Further, a second-level domain name cannot be created if it conflicts with a reserved domain name.
- Point of Contact Associations: The domain name is associated with the following points of contact. Contacts are created and managed independently according to RFC 5733.
  - Registrant
  - Administrative contact
  - Technical contact
  - Billing contact
- Domain Name Associations: Each domain name is associated with:
  - A maximum of 13 hosts, which are created and managed independently according to RFC 5732
  - An Auth-Info, which is used to authorize certain operations on the object
  - Status(es), which are used to describe the domain name's status in the registry
  - A created date, updated date, and expiry date

4 DEMONSTRATES THAT TECHNICAL RESOURCES REQUIRED TO CARRY THROUGH THE PLANS FOR THIS ELEMENT ARE ALREADY ON HAND OR READILY AVAILABLE

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for the .web gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support the registration lifecycle:

- Application Engineers: 19
- Customer Support Personnel: 36
- Database Administrators: 8
- Database Engineers: 3
- Quality Assurance Engineers: 11
- SRS System Administrators: 13

To implement and manage the .web gTLD as described in this application, Verisign, Web.com's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.



When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only the .web gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and the .web gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

## 28. Abuse Prevention and Mitigation

### 1. COMPREHENSIVE ABUSE POLICIES, WHICH INCLUDE CLEAR DEFINITIONS OF WHAT CONSTITUTES ABUSE IN THE TLD, AND PROCEDURES THAT WILL EFFECTIVELY MINIMIZE POTENTIAL FOR ABUSE IN THE TLD

Please note; all figures, tables and diagrams referenced in the following response can be found in the attachment titled "Attachment dot web Q28."

Web.com Group, Inc ("Web.com") has been in the business of helping our near 3 million customers establish their online presences for over 15 years. As such, we have a rich history of understanding the importance of abuse prevention and mitigation as a core objective. We are active participants in a variety of industry and government efforts to prevent domain name abuse and are constantly updating our operating procedures to ensure our customers are as protected from this type of activity as they can be.

The .web gTLD will help customers launch and leverage their presence on the World Wide Web. As a leading global provider of online marketing services to small businesses, Web.com recognizes that finding a relevant and memorable domain name can be challenging. Since many keywords and descriptive phrases associated with existing gTLDs have already been registered, it is difficult to pinpoint a domain name which contains a limited number of characters. Consequently, prospective registrants are often unable to secure a unique name. Regularly, in the .com space amongst others, this is because of exploitative or abusive registrations. In the forthcoming .web namespace, we will endeavor to the utmost of our ability to prevent this pattern from repeating.

One of the most important reasons our customers choose Web.com is because of our reputation for great products and exceptional customer service. The .web gTLD is a natural extension of our business. It is a place where we can help customers be successful on the web. At Web.com, we believe that a website is only as good as the services and support behind it. With the .web gTLD, we have the chance to bring this same commitment to service and support to a gTLD. For companies and consumers who stake their reputation on a .web domain name, having a gTLD that is trusted and secure is critical.

Unfortunately, some of the current gTLDs are not operated in a manner that instills this level of confidence. Web.com hopes to make the .web gTLD different. In launching the .web gTLD we have put together a tapestry of efforts that seek to prevent and successfully mitigate domain name abuse, making the web a more accessible and friendly place for small and medium sized businesses as well as consumers. These efforts include:

- An acceptable use policy that clearly defines what is considered abuse and what registrants may and may not do with their domain names

- A seasoned abuse mitigation team that has years of experience in dealing with these issues
- Technological Measures for Removal of Orphan Glue Records
- Efforts and measures to promote accurate and complete Whois
- Requirements for .web accredited registrars to enact measures in support of these efforts

The fight against abusive behavior is not static and Web.com is committed to ensuring that our efforts are constantly evolving to meet the ever changing landscape of threats.

#### 1.1 .web Abuse Prevention and Mitigation Implementation Plan

Preventing domain name abuse in the .web gTLD is of critical importance to registrants, consumers and Web.com. To demonstrate our commitment to make the .web gTLD more resistant to abusive behavior than just about any other gTLD that currently exists, Web.com has explored various mechanisms to help prevent abusive registrations. We were particularly impressed with the set of 31 Proposed Security, Stability and Resiliency Requirements for Financial TLDs that were developed by the Security Standards Working Group (SSWG) under the guidance of the financial services industry. Following their recommendation that all potential applicants look at these standards for their own TLDs, Web.com has completed a thorough review to determine which might enhance the .web gTLD experience. While not all of the proposed standards are applicable to the .web gTLD, we will endeavor to implement several of them to aid in our efforts to prevent and mitigate abusive registrations.

Web.com has developed and will look to deploy a customized approach that seeks to minimize the potential for abusive registrations and mitigate them as soon as possible should they occur. Registrants, Registrars and the Registry will all play a role in this endeavor. Having all three levels of the .web gTLD ecosystem participate in these measures will help ensure a comprehensive approach to these critical objectives. Web.com has designed the following procedure to prevent and mitigate abusive registrations:

Acceptable Use Policy - Web.com has developed a draft Acceptable Use Policy (AUP) which can be found in "Attachment dot web Q28." This AUP clearly defines what is considered abuse and what type of behavior is expressly prohibited in conjunction with the use of a .web domain name. Web.com will require, through the Registry Registrar Agreement (RRA), that this AUP be included in the registration agreement used by all .web gTLD accredited registrars. This registration agreement must be accepted by a registrant prior to them being able to register a name in the .web gTLD.

Annual Certification of Registrar compliance with Registry-Registrar Agreement. The self-certification program consists, in part, of evaluations applied equally to all operational .web gTLD accredited registrars and conducted from time to time throughout the year. Process steps are as follows:

- Web.com sends an email notification to the ICANN primary registrar contact, requesting that the contact go to a designated URL, log in with his/her Web ID and password, and complete and submit the online form. The contact must submit the form within 15 business days of receipt of the notification.
- When the form is submitted, Web.com sends the registrar an automated email confirming that the form was successfully submitted.
- Web.com reviews the submitted form to ensure the certifications are compliant.
- Web.com sends the registrar an email notification if the registrar is found to be compliant in all areas.
- If a review of the response indicates that the registrar is out of compliance or if Web.com has follow-up questions, the registrar has 10 days to respond to the inquiry.
- If the registrar does not respond within 15 business days of receiving

the original notification, or if it does not respond to the request for additional information, Web.com sends the registrar a Breach Notice and gives the registrar 30 days to cure the breach.

- If the registrar does not cure the breach, Web.com terminates the Registry-Registrar Agreement (RRA).

The .web gTLD registry will provide and maintain a primary point of contact for abuse complaints. We will display the contact information for the Abuse Mitigation Team, which serves as the primary point of contact for reporting abuse within the .web gTLD, on the .web gTLD website.

Each .web gTLD accredited registrar will provide and maintain a primary point of contact for abuse complaints. The registrar must provide and maintain valid primary contact information for reporting abuse in the .web gTLD on their website. This will be required as part of the .web gTLD RRA.

Web.com will explicitly define for Registrars what constitutes abusive behavior including but not limited to, malicious, negligent, and reckless behavior. The definition of abusive behavior will be contained in the AUP that Registrars will be required to include as part of the Registration Agreement. This will be required as part of the .web gTLD RRA.

Registrar must notify Registry Operator immediately regarding any investigation or compliance action including the nature of the investigation or compliance action by ICANN or any outside party (e.g., law enforcement, etc.), along with the TLD impacted. This will be required as part of the .web gTLD RRA.

Development of an Abuse Prevention and Mitigation Working Group. To give the Web.com team alternate perspectives about handling incidents of abuse and ways to mitigate them, we will form an Abuse Prevention and Mitigation Working Group. This team will not only be comprised of a cross functional group of Web.com professionals but also look to involve representatives from law enforcement, our customer base and outside experts. The group would meet regularly to discuss the latest trends in domain name abuse and the most effective way to prevent and remedy them.

## 1.2 Policies for Handling Complaints Regarding Abuse

Web.com will staff a Single Point of Contact (SPoC) Abuse team to address abuse and malicious use requests. The role of the abuse team is to monitor registry services and review complaints entered online by end users, customers, and/or Law Enforcement. The complaints will be managed in accordance with the applicable Acceptable Use Policy (AUP) and Terms of Service (TOS) which shall allow the Abuse team discretion to suspend a domain instantly or send the complaint through the appropriate escalation channel for complaint resolution.

Complaints shall be received via email at [abuse@registry.web](mailto:abuse@registry.web) as will be prominently provided on the .web website (<http://registry.web>). Registrar access to .web's Abuse Team will be provided via a hotline number, email address and additional personnel for filing direct requests. Complaints may be submitted 24x7 and each request path requires the submitter to provide personal contact information. .web will acknowledge the complaint within one (1) business day and will provide the requestor acceptance and/or resolution within three (3) business days depending on severity and complexity of the complaint.

Web.com views domain name abuse as a serious matter that produces direct harm to Internet users and .web customers. As such, .web will handle each abuse complaint as a direct threat and intends to resolve each validated complaint with a sense of urgency. Our Abuse Policies recognize many forms of abuse related to the registrations and use of domain names. Abuses and their respective mitigation strategy listed here is not an exhaustive list, but is meant to highlight general process and procedure by which .web will manage the

most common forms of abuse. The .web Abuse Team collaborates and participates with industry experts and forums to understand the latest forms of abuse in an attempt to protect customers of our services and Internet users where possible.

#### DRAFT ABUSE REMEDY PROCESS

Listed here is the proposed process for dealing with the major forms of domain abuse:

1. Customer or end user submits abuse complaint to abuse@registry.web;
2. Abuse Coordinator receives request and acknowledges receipt of complaint;
3. Abuse Coordinator analyzes request to determine the abuse type to be addressed and references the .web knowledgebase for detailed procedures;
4. Abuse Coordinator assigns a severity rating based on complaint type;
5. Abuse Coordinator resolves the complaint based on the following decision tree:
  - a. Is the request a court ordered seizure and transfer?
    - i. Yes - See section 28.1.1
    - ii. No - next step
  - b. Does the request reflect a potential DDOS Attack?
    - i. Yes - See section 28.1.2
    - ii. No - next step
  - c. Is the request a phishing complaint?
    - i. Yes - See section 28.1.3
    - ii. No - next step
  - d. Is the complaint a notice of a trademark infringement?
    - i. Yes - See section 28.1.4
    - ii. No - next step
  - e. Is the request a possible hijacking case or a transfer dispute?
    - i. Yes - See section 28.1.5
    - ii. No - next step
  - f. Is the request an email service abuse?
    - i. Yes - See section 28.1.6
    - ii. No - next step
  - g. Does the complaint refer to abusive or offensive content hosted on a .web domain?
    - i. Yes - See section 28.1.7
    - ii. No - next step
  - h. For all other abuses not defined:
    - i. Escalate request to Abuse Manager for guidance and resolution

#### 28.1.1 Court Ordered Seizure and Transfer

Definition: Law enforcement via a court of legal jurisdiction orders that domain be seized due to illegal activity of applicable law.

Service Level: One (1) business day

#### Procedure:

- Abuse Coordinator contacts the legal jurisdiction to request signed copies of the court order;
- Upon receipt of court order, Abuse Coordinator confirms request with the Abuse Situation Manager;
- If the request is determined to be valid, Abuse Coordinator will submit a request to the Registry Support team to have the domain pushed to the requested registrar as directed by the applicable judicial entity;
- If the request is determined to be invalid or documents submitted are in question, the Abuse Coordinator will contact the legal jurisdiction requesting the appropriate documentation or to provide reasoning as to why the request cannot be fulfilled.

#### 28.1.2 DOS or DDOS Attack

Definition: A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer or network resource unavailable to its intended users.

Service Level: One (1) business day

Procedure:

- Abuse Coordinator will confirm the DDOS attack with the Abuse Manager;
- If the complaint is confirmed as a DDOS attack:
  - o Abuse Coordinator will escalate the request to the respective Registrar Support Team;
  - o If not , Abuse Coordinator will respond to the complainant as unable to confirm and request additional information or close the complaint;
- Registrar Support team will suspend the domain registration until further notice.

### 28.1.3 Phishing

Definition: Phishing is a website fraudulently presenting itself as a trusted site (often a bank) in order to deceive Internet users into divulging sensitive information (e.g. online banking credentials, email passwords).

Service Level: One (1) business day

Procedure:

- Abuse Coordinator will confirm the phishing scam with the Abuse Manager;
- If the complaint is confirmed as a legitimate phishing event;
  - o Abuse Coordinator will escalate the request to the Registry Support Team;
  - o If not , Abuse Coordinator will respond to the complainant as unable to confirm and request additional information or close the complaint;
- Registry Support Team will immediately suspend the domain;
- Abuse Manager will investigate the Phish event and determine the intent of the domain registrant, the Registry Support team seize and/or delete the domain from the zone.

### 28.1.4 Cybersquatting / Trademark Infringement

Definition: Cybersquatting is the deliberate and bad-faith registration and use of a name that is a registered brand or mark of an unrelated entity, often for the purpose of profiting (typically, though not exclusively, through pay-per-click advertisements).

Service Level: Three (3) business days

Procedure:

- If request appears to be an initial complaint on a possible infringement, Abuse Coordinator will direct complainant to the UDRP/WIPO process;
- If not , if the request of transfer is from a .web registrar, Abuse Coordinator will work with the Registrar to ensure the domain in question is transferred appropriately.

### 28.1.5 Transfer Disputes / Hijacking

Definition: Domain hijacking or domain theft is the act of changing the registration of a domain name without the permission of its original registrant.

Service Level: Three (3) business days

## Procedure:

- Abuse Coordinator will confirm the OFAC request with the Abuse Manager;
- Abuse Coordinator will escalate request to and Registrar shall internal policies and procedures to investigate the transfer.

## 28.1.6 Email Service Abuse

Definition: An illegitimate use of email systems to distribute abusive content or in a manner that violates the Acceptable Use Policy. Examples of this abuse are Un-Solicited Commercial Email (UCE/SPAM).

Service Level: Three (3) business days

## Procedure:

- Abuse Coordinator will validate the complaint for UCE/SPAM elements and collaborate with the Complainant to acquire the examples of the offensive material;
- If Abuse Coordinator deems the offensive material to violate Acceptable Use Policy and is deemed to be offensive material, Abuse Coordinator will escalate the request to the Registry Support team for suspension;
- Registry Support team will immediately suspend the domain;
- If a .web customer is found to be unknowingly sending UCE, Customer shall be allotted the opportunity to correct the situation and assurances must be received by offender to ensure against future occurrences.

## 28.1.7 Web Hosting Abuse

Definition: Content or material hosted on a website that that is deemed to be offensive or against the .web Acceptable Use Policy. Material that is deemed offensive by registrar/host shall result in a Warning, then Suspension if material is not removed and possible seizure or termination of services.

Service Level: Three (3) business days

## Procedure:

- Abuse Coordinator will validate the information in the complaint to confirm that the hosting package is being used in a way that is not compliant with the .web Acceptable Use Policy. Some examples may include the following:
  - o Documents, videos, pictures, music files, software etc. is not associated with the function or serving up of website;
  - o Content being stored is not accessible from the Website;
  - o An open FTP server;
  - o Storage being used as a hard drive/backup; or
  - o Space Manager usage exceeds 2GB of storage on the UNIX hosting platform only.
- If one or more of the above is confirmed and validated, the Abuse Coordinator or Technical Services will notify the Customer that they are in violation of the .web AUP and/or Terms of Service;
- An email will be sent immediately to the Registrant, Admin and Technical contact on file to advise of the violation. The email should instruct the Customer to take the appropriate action within 24 hours to remove the offending content or they may be subjected to a suspension of services;
- During Business Hours, the Abuse Coordinator will contact the Customer via phone in addition to sending the email to inform the Registrant, Admin or Technical contacts of the offending violation. The Technical Services agents will follow the same process for After Hours handling;
- If no response is received within 24 hours, a second phone and email attempt will be made to reach the Registrant, Admin and Technical contact;
- If the offending party does not respond by the end of the second business day, action will be taken to remove the offending content that is causing server degradation;
- Technical Support team will suspend the Hosting services;
- The Registry Support team will place the domain on Registrar hold to de-resolve the name;

- If the offending party responds and agrees to remove the offending content within the 24 hour time frame, the Abuse Coordinator or Technical Services agent must confirm the material has been removed, and note the appropriate remediation within the CRM system;
- If the offending party responds and agrees to remove the offending content after the service suspension, the Registry Support team may remove the suspension and allow customer to remove the content. Support will confirm the offending material has been removed, and note the appropriate CRM systems;
- If the offending party requests that .web remove the offending material, the Abuse Coordinator agent must call the Customer and obtain confirmation to remove the content on behalf of the Customer. The Abuse Coordinator will also obtain written confirmation from the Customer via the Registrant, Administrative or Technical Contacts that are listed. The confirmation should be noted in the appropriate CRM system;
- If there is no response from the offending party after 7 Days, the Abuse Coordinator will submit a request to delete the offending content from the servers to the Abuse Manager for approval to delete the content;
- Prior to deleting the content, an email will be sent to the appropriate internal Legal point of contact to advise of the issue and obtain approval to delete the content.

### 1.3 Proposed Measures for Removal of Orphan Glue Records

Although orphan glue records often support correct and ordinary operation of the Domain Name System (DNS), registry operators will be required to remove orphan glue records (as defined at <http://www.icann.org/en/committees/security/sac048.pdf>) when provided with evidence in written form that such records are present in connection with malicious conduct. Web.com's selected backend registry services provider's registration system is specifically designed to not allow orphan glue records. Registrars are required to delete/move all dependent DNS records before they are allowed to delete the parent domain.

To prevent orphan glue records, Verisign, Web.com's chosen backend registry services provider, performs the following checks before removing a domain or name server:

Checks during domain delete:

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

Check during explicit name server delete:

- Verisign confirms that the current name server is not referenced by any domain name (in-zone) before deleting the name server.

Zone-file impact:

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

### 1.4 Resourcing Plans

Details related to resourcing plans for the initial implementation and ongoing maintenance of Web.com's abuse plan are provided in Section 2 of this response.

### 1.5 Measures to Promote Whois Accuracy

Web.com supports efforts to improve the accuracy and completeness of Whois

records. To that end, we will seek to implement a series of measures that require registrars and registrants to help us in this pursuit. This includes a Whois reminder process at the registry level, regular scans of the Whois data to search for blank or incomplete data and economic incentives for registrars who achieve 100% complete and accurate Whois data for those names they have registered.

#### Regular Monitoring of Registration Data for Accuracy and Completeness

Whois data reminder process. Verisign regularly reminds registrars of their obligation to comply with ICANN's Whois Data Reminder Policy, which was adopted by ICANN as a consensus policy on 27 March 2003

(<http://www.icann.org/en/registrars/wdrp.htm>). Verisign sends a notice to all registrars once a year reminding them of their obligation to be diligent in validating the Whois information provided during the registration process, to investigate claims of fraudulent Whois information, and to cancel domain name registrations for which Whois information is determined to be invalid.

Bi-Annual Whois Verification by Registrars. As will be required in the Registry-Registrar Agreement, all .web accredited registrars will be required to verify Whois data for each record they have registered in the TLD twice a year.

Verification can take place via email, phone or any other methods as long as there is a proactive action by the registrant to confirm the accuracy of the Whois data associated with the domain name. Web.com will randomly audit Whois records to ensure compliance and accuracy. As part of the .web gTLD Abuse reporting system, users can report missing or incomplete Whois data via the registry website.

Quarterly Scan of the Zone file for incomplete Registrant Data. On a quarterly basis, Web.com will do a scan of all Whois records in the .web gTLD to find any blank fields or missing registration data. Upon completion of the scan, registrars will be sent a report detailing which domain names are missing data. As part of their responsibilities in the RAA to work towards 100% accuracy of Whois data, registrars must then alert registrants that there is data missing in their Whois record and remind them of their responsibility contained in the registration agreement that they must comply with ICANN requirements for complete and accurate Whois data.

#### Economic incentives for Registrars to achieve 100% Whois Accuracy

Web.com will offer Market Development Funds (MDF) to those registrars who can demonstrate via a third party audit that the .web gTLD names registered with them have 100% complete and accurate Whois data.

#### 1.6 Malicious or Abusive Behavior Definitions, Metrics, and Service Level Requirements for Resolution

Web.com defines Malicious and Abusive behavior based on the following but not limited definitions:

Phishing is a criminal activity employing tactics to defraud and defame Internet users via sensitive information with the intent to steal or expose credentials, money or identities. A phishing attack begins with a spoofed email posing as a trustworthy electronic correspondence that contains hijacked brand names i.e. (financial institutions, credit card companies, e-commerce sites). The language of a phishing email is misleading and persuasive by generating either fear and/or excitement to ultimately lure the recipient to a fraudulent website. It is paramount for both the phishing email and website to appear credible in order for the attack to influence the recipient. As with the spoofed email, phishers aim to make the associated phishing website appear credible. The legitimate target website is mirrored to make the fraudulent site look professionally designed. Fake third-party security endorsements, spoofed address bars, and spoofed padlock icons falsely lend credibility to fraudulent sites as well. The persuasive inflammatory language of the email



combined with a legitimate looking website is used to convince recipients to disclose sensitive information such as passwords, usernames, credit card numbers, social security numbers, account numbers, and mother's maiden name.

Malware is malicious software that was intentionally developed to infiltrate or damage a computer, mobile device, software and/or operating infrastructure or website without the consent of the owner or authorized party. This includes, amongst others, Viruses, Trojan horses, and worms.

Domain Name or Domain Theft is the act of changing the registration of a domain name without the permission of its original registrant.

Section 1.2 outlines the Web.com Policies and Procedures for Handling Complaints Regarding Abuse as defined above.

As pertains to Web.com performance metrics and service level requirements for resolution, we adhere to a 12 hour timeframe to address and potentially rectify the issue as it pertains to all forms of abuse and fraud. Once a notification is received via email, call center or fax, the Web.com Customer Service centers immediately create a support ticket in order to monitor and track the issue through resolution. If notifications are received during normal business hours (8am - 11pm EST. (Monday - Friday) and 8am - 6pm EST (Saturday & Sunday) the majority of issues are resolved in less than a 4 hour period.

#### 1.7 Controls to Ensure Proper Access to Domain Functions

To ensure proper access to domain functions, Web.com incorporates Verisign's Registry-Registrar Two-Factor Authentication Service into its full-service registry operations. The service is designed to improve domain name security and assist registrars in protecting the accounts they manage by providing another level of assurance that only authorized personnel can communicate with the registry. As part of the service, dynamic one-time passwords (OTPs) augment the user names and passwords currently used to process update, transfer, and/or deletion requests. These one-time passwords enable transaction processing to be based on requests that are validated both by "what users know" (i.e., their user name and password) and "what users have" (i.e., a two-factor authentication credential with a one-time-password).

Registrars can use the one-time-password when communicating directly with Verisign's Customer Service department as well as when using the registrar portal to make manual updates, transfers, and/or deletion transactions. The Two-Factor Authentication Service is an optional service offered to registrars that execute the Registry-Registrar Two-Factor Authentication Service Agreement. As shown in Figure 28-1, the registrars' authorized contacts use the OTP to enable strong authentication when they contact the registry. There is no charge for the Registry-Registrar Two-Factor Authentication Service. It is only enabled for registrars that wish to take advantage of the added security provided by the service.

## 2. TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

### Resource Planning

Web.com is a leading provider of Internet services for small to medium-sized businesses (SMBs). Web.com is the parent company of two global domain name registrars and further meets the Internet needs of SMBs throughout their lifecycle with affordable value added services that including domain name registration, website design, search engine optimization, search engine marketing, social media and mobile products, local sales leads, eCommerce solutions and call center services. Headquartered in Jacksonville, FL, USA, Web.com is NASDAQ traded company serving nearly three million customers with more than 1,700 global employees in fourteen locations in North America, South America and the United Kingdom.

Our business is helping people establish, maintain, promote, and optimize their web presence. Web.com intentionally chose Verisign as our registry services provider because of their unsurpassed track record in operating some of the world's most complex and critical top level domains. Verisign's support for the .web gTLD will help ensure its success

The .web gTLD will be fully supported by a cross function team of Web.com professionals. Numbers and types of employees will vary for each function but Web.com projects it will use the following personnel to support the resource planning requirements:

- Quality Assurance Engineer: 0.5 FTE
- System Administrator: 1 FTE
- Database Administrator: 0.5 FTE
- Technical Project Manager: 0.5 FTE
- Marketing Director: 1 FTE
- Sales Manager: 1 FTE
- Legal Counsel: 1 FTE
- Finance/Accounting: 1 FTE
- Customer Service: 2 FTEs

#### Resource Planning Specific to Backend Registry Activities

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support abuse prevention and mitigation:

- Application Engineers: 19
- Business Continuity Personnel: 3
- Customer Affairs Organization: 9
- Customer Support Personnel: 36
- Information Security Engineers: 11
- Network Administrators: 11
- Network Architects: 4
- Network Operations Center (NOC) Engineers: 33
- Project Managers: 25
- Quality Assurance Engineers: 11
- Systems Architects: 9

To implement and manage the Web.com .web gTLD as described in this application,

Verisign, Web.com's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

### 3. POLICIES AND PROCEDURES IDENTIFY AND ADDRESS THE ABUSIVE USE OF REGISTERED NAMES AT STARTUP AND ON AN ONGOING BASIS

#### 3.1 Start-Up Anti-Abuse Policies and Procedures

Verisign, Web.com's selected backend registry services provider, provides the following domain name abuse prevention services, which Web.com incorporates into its full-service registry operations. These services are available at the time of domain name registration.

**Registry Lock.** The Registry Lock Service allows registrars to offer server-level protection for their registrants' domain names. A registry lock can be applied during the initial standup of the domain name or at any time that the registry is operational.

Specific Extensible Provisioning Protocol (EPP) status codes are set on the domain name to prevent malicious or inadvertent modifications, deletions, and transfers. Typically, these 'server' level status codes can only be updated by the registry. The registrar only has 'client' level codes and cannot alter 'server' level status codes. The registrant must provide a pass phrase to the registry before any updates are made to the domain name. However, with Registry Lock, provided via Verisign, Web.com's subcontractor, registrars can also take advantage of server status codes.

The following EPP server status codes are applicable for domain names: (i) serverUpdateProhibited, (ii) serverDeleteProhibited, and (iii) serverTransferProhibited. These statuses may be applied individually or in combination.

The EPP also enables setting host (i.e., name server) status codes to prevent deleting or renaming a host or modifying its IP addresses. Setting host status codes at the registry reduces the risk of inadvertent disruption of DNS resolution for domain names.

The Registry Lock Service is used in conjunction with a registrar's proprietary security measures to bring a greater level of security to registrants' domain names and help mitigate potential for unintended deletions, transfers, and/or updates.

Two components comprise the Registry Lock Service:

- Web.com and/or its registrars provides Verisign, the provider of backend registry services, with a list of the domain names to be placed on the server status codes. During the term of the service agreement, the registrar

can add domain names to be placed on the server status codes and/or remove domain names currently placed on the server status codes. Verisign then manually authenticates that the registrar submitting the list of domain names is the registrar of record for such domain names.

- If Web.com and/or its registrars requires changes (including updates, deletes, and transfers) to a domain name placed on a server status code, Verisign follows a secure, authenticated process to perform the change. This process includes a request from a Web.com-authorized representative for Verisign to remove the specific registry status code, validation of the authorized individual by Verisign, removal of the specified server status code, registrar completion of the desired change, and a request from the Web.com-authorized individual to reinstate the server status code on the domain name. This process is designed to complement automated transaction processing through the Shared Registration System (SRS) by using independent authentication by trusted registry experts.

Web.com intends to charge registrars based on the market value of the Registry Lock Service. A tiered pricing model is expected, with each tier having an annual fee based on per domain name/host and the number of domain names and hosts to be placed on Registry Lock server status code(s).

### 3.2 Ongoing Anti-Abuse Policies and Procedures

#### 3.2.1 Policies and Procedures That Identify Malicious or Abusive Behavior

Verisign, Web.com's selected backend registry services provider, provides the following service to Web.com for incorporation into its full-service registry operations.

Malware scanning service. Registrants are often unknowing victims of malware exploits. Verisign has developed proprietary code to help identify malware in the zones it manages, which in turn helps registrars by identifying malicious code hidden in their domain names.

Verisign's malware scanning service helps prevent websites from infecting other websites by scanning web pages for embedded malicious content that will infect visitors' websites. Verisign's malware scanning technology uses a combination of in-depth malware behavioral analysis, anti-virus results, detailed malware patterns, and network analysis to discover known exploits for the particular scanned zone. If malware is detected, the service sends the registrar a report that contains the number of malicious domains found and details about malicious content within its TLD zones. Reports with remediation instructions are provided to help registrars and registrants eliminate the identified malware from the registrant's website.

#### 3.2.2 Policies and Procedures That Address the Abusive Use of Registered Names

Suspension processes.

In the case of domain name abuse, Web.com will determine whether to take down the subject domain name. Verisign, Web.com's selected backend registry services provider, will follow the following auditable processes to comply with the suspension request.

Verisign Suspension Notification. Web.com submits the suspension request to Verisign for processing, documented by:

- Threat domain name
- Registry incident number
- Incident narrative, threat analytics, screen shots to depict abuse, and/or other evidence
- Threat classification
- Threat urgency description
- Recommended timeframe for suspension/takedown
- Technical details (e.g., Whois records, IP addresses, hash values, anti

-virus detection results/nomenclature, name servers, domain name statuses that are relevant to the suspension)

- Incident response, including surge capacity

Verisign Notification Verification. When Verisign receives a suspension request from Web.com, it performs the following verification procedures:

- Validate that all the required data appears in the notification.
- Validate that the request for suspension is for a registered domain name.
- Return a case number for tracking purposes.

Suspension Rejection. If required data is missing from the suspension request, or the domain name is not registered, the request will be rejected and returned to Web.com with the following information:

- Threat domain name
- Registry incident number
- Verisign case number
- Error reason

Registrar Notification. Once Verisign has performed the domain name suspension, and upon Web.com request, Verisign notifies the registrar of the suspension. Registrar notification includes the following information:

- Threat domain name
- Registry incident number
- Verisign case number
- Classification of type of domain name abuse
- Evidence of abuse
- Anti-abuse contact name and number
- Suspension status
- Date/time of domain name suspension

Registrant Notification. Once Verisign has performed the domain name suspension, and upon Web.com request, Verisign notifies the registrant of the suspension. Registrant notification includes the following information:

- Threat domain name
- Registry incident number
- Verisign case number
- Classification of type of domain name abuse
- Evidence of abuse
- Registrar anti-abuse contact name and number

Upon Web.com request, Verisign can provide a process for registrants to protest the suspension.

Domain Suspension. Verisign places the domain to be suspended on the following statuses:

- serverUpdateProhibited
- serverDeleteProhibited
- serverTransferProhibited
- serverHold

Suspension Acknowledgement. Verisign notifies Web.com that the suspension has been completed. Acknowledgement of the suspension includes the following information:

- Threat domain name
- Registry incident number
- Verisign case number
- Case number
- Domain name

- Web.com abuse contact name and number, or registrar abuse contact name and number
- Suspension status

#### 4. WHEN EXECUTED IN ACCORDANCE WITH THE REGISTRY AGREEMENT, PLANS WILL RESULT IN COMPLIANCE WITH CONTRACTUAL REQUIREMENTS

Web.com is fully committed to improving the completeness and accuracy of Whois data and to preventing and mitigating domain name abuse in the .web gTLD. We strongly believe the efforts that we have outlined will go a long way in this critical area and most certainly meet the requirements as outlined by ICANN.

The fight against domain names abuse is not a static fight. The tactics used by malicious parties are constantly evolving and web.com is committed to evolving our systems to address these ongoing threats not because ICANN says we have to but simply because it is what our customers have come to expect from Web.com.

The .web gTLD is an extension of our current business. At Web.com, we believe that a website is only as good as the services and support behind it. With the .web gTLD, we have the chance to bring this same commitment to service and support to a gTLD. For companies and consumers who stake their reputation on a .web domain name, having a gTLD that is trusted and secure is critical.

#### 5. TECHNICAL PLAN SCOPE/SCALE THAT IS CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

##### Scope/Scale Consistency

As one of the first domain registrars, Web.com and its subsidiaries have seen the Internet grow exponentially across three decades. Web.com has grown to a point where it now serves approximately 3 million customers, comprising over 8 million domain names under management. As our customer base grew and the number of domains we managed with it, we expanded our operations to meet customer needs. We anticipate doing exactly the same as .web proliferates. Our systems are highly developed and continually tested and audited, and will scale as we scale. The commitments we will seek to make to prevent domain name abuse will expand to meet the anticipated growth of the .web gTLD. We invest tens of millions each year in upgrading infrastructure and developing new business processes to meet the growth and needs of our customer base, and consider doing so of paramount importance.

After 15 years of developing in this way, Web.com is a leading provider of Internet services for small- to medium-sized businesses (SMBs). Web.com is the parent company of two global domain name registrars, and further meets the Internet needs of consumers and businesses throughout their lifecycle with affordable value-added services. Those services include domain name registration; website design; search engine optimization; search engine marketing; social media and mobile products; local sales leads; eCommerce solutions; and call center services.

Headquartered in Jacksonville, FL, USA, Web.com is a publicly traded company (Nasdaq: WWWW), with more than 1,700 global employees in fourteen locations in North America, South America and the United Kingdom. Web.com brings a wealth of experience in providing a seamless process for customers from the first point of registration through the growth of their Internet properties.

Indeed, following our acquisition of Register.com in July 2010 and the subsequent acquisition of Network Solutions, LLC, in October 2011, we have become one of the largest domain name registrars in the world. Web.com offers a variety of gTLDs and a full suite of domain name services, including registration, management, renewal, expiration protection and privacy services.

It is clear, therefore, that managing the potentially enormous growth of

the .web namespace will be a challenge, but a challenge to which we are more than equal.

#### Scope/Scale Consistency Specific to Backend Registry Activities

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the .web gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Other Operating Cost" (Template 1, Line I.L) within the Question 46 financial projections response.

## 29. Rights Protection Mechanisms

### 1 MECHANISMS DESIGNED TO PREVENT ABUSIVE REGISTRATIONS

Web.com Group, Inc ("Web.com") has been in the business of helping our nearly 3 million customers establish their online presence for over 15 years. Through our recent acquisition of Network Solutions, the oldest ICANN accredited registrar, with over 25 years of experience, we have a long history of understanding the importance of rights protection. This is a core objective not only from our own personal perspective as the holder of various trademarks including web.com®, but also on behalf of our customers who have their own trademarks.

Web.com will implement and adhere to any rights protection mechanisms (RPMs) that may be mandated by ICANN, including each mandatory RPM set forth in the Registry Agreement, specifically Specification 7. Web.com acknowledges that, at a minimum, ICANN requires a Sunrise period, a Trademark Claims period, and interaction with the Trademark Clearinghouse with respect to the registration of domain names for the .web gTLD. It should be noted that because ICANN, as of the time of this application submission, has not issued final guidance with respect to the Trademark Clearinghouse, Web.com cannot fully detail the specific implementation of the Trademark Clearinghouse within this application. Web.com will adhere to all processes and procedures to comply with ICANN guidance once this guidance is finalized.

We understand the importance of Trademark holders to manage and protect their brands. In order to demonstrate our commitment to ensure the .web gTLD will accommodate the Intellectual Property community, Web.com has analyzed various additional mechanisms to help prevent abusive registrations. We were particularly impressed with the set of 31 Proposed Security, Stability and Resiliency Requirements for Financial gTLDs that were developed by the Security Standards Working Group (SSWG) under the guidance of the financial services industry. Following their recommendation that all potential applicants look at these standards for their own gTLDs, Web.com completed a thorough review to determine which standards may enhance the .web gTLD experience. While not all of the proposed standards are applicable to the .web gTLD, we will strive to

implement several of these standards to ensure trademark owners will be able to take advantage of the additional protection beyond the minimums set forth by ICANN.

Web.com has developed and will deploy a customized approach that seeks to minimize the potential for abusive registrations and incorporate a proactive mitigation process if a situation were to arise. Registrants, Registrars and the Registry will be contributing participants in this endeavor. Having all three participating entities of the .web gTLD ecosystem take part in these measures will ensure a comprehensive approach to these critical objectives. Web.com has designed the following procedures to help protect the rights of trademark owners:

- Extended Sunrise Services
- Extended Trademark Claims Service
- Name Selection Policy
- Acceptable Use Policy
- Name Allocation Policy
- URS and UDRP
- PDDRP and RRDRP
- Rapid Takedown or Suspension
- Anti-Abuse Process
- Malware Code Identification
- DNSSEC Signing Service
- Biannual WHOIS Verification
- Participation in Anti-abuse Community Activities

As described in this response, Web.com will implement a Sunrise period and Trademark Claims service with respect to the registration of domain names within the .web gTLD. Certain aspects of the Sunrise period and/or Trademark Claims service may be administered on behalf of Web.com by Web.com approved registrars or by authorized subcontractors of Web.com, such as its selected backend registry services provider, Verisign.

Sunrise Periods. As it pertains to the launch of the .web gTLD, Web.com is currently planning on holding two different sunrise periods. Sunrise A will enable those participants that wish to register trademarks in the .web gTLD. A second sunrise period, Sunrise B, will be held for those who wish to reserve a domain name already registered in another gTLD. A more detailed explanation of each Sunrise Period follows.

#### Sunrise A

As set forth in the ICANN Applicant Guidebook, the Sunrise service pre-registration procedure for domain names must last for at least 30 days prior to the launch of the general registration of domain names in the gTLD.

To ensure that trademark owners have ample time to participate in the midst of the possible launch of several other gTLDs, Web.com is planning on extending the sunrise to 60 days, 30 days longer than the ICANN mandated minimum.

During the Sunrise period, holders of marks that have been previously validated by the Trademark Clearinghouse receive notice of domain names that are an identical match (as defined in the ICANN Applicant Guidebook) to their mark(s). Such notice is in accordance with ICANN's requirements and is provided by Web.com either directly or through Web.com-approved registrars.

Web.com requires all registrants, either directly or through Web.com-approved registrars, who are in good-standing with ICANN, to i) affirm that said registrants meet the Sunrise Eligibility Requirements (SER) and ii) submit to the Sunrise Dispute Resolution Policy (SDRP) consistent with Section 6 of the Trademark Clearinghouse model. At a minimum Web.com recognizes and honors all word marks for which a proof of use was submitted and validated by the Trademark Clearinghouse.



During the Sunrise period, Web.com and/or Web.com-approved registrars, as applicable, are responsible for determining whether each domain name is eligible to be registered (including in accordance with the SERs).

#### Sunrise B

During a potential Sunrise B, registrants of domain names in other gTLDs may be able to file an application through a .web gTLD accredited registrar to register their existing domain name in the .web gTLD. Proof of registration of the domain name will be verified at the time of application. This sunrise period will last 30 days and at the end of the registration period, if there are no identical matches to any other applied for strings, the domain name will be registered to the appropriate applicant. If there are competing applications for the same domain name, qualified applicants will proceed to a closed auction to resolve the conflict.

Trademark Claims Service. As provided by the Trademark Clearinghouse model set forth in the January 11, 2012 version of the ICANN Applicant Guidebook, all new gTLDs will be required to provide a Trademark Claims service for a minimum of 60 days after the launch of the general registration of domain names in the gTLD (Trademark Claims period).

Similar to our voluntarily extending the sunrise period to accommodate the needs of trademark owners, Web.com is planning on extending the trademark claims services to 120 days, double the ICANN mandated minimum. As the processes for how the trademark clearinghouse, including technical and financial specifics of how the program will work, are not finalized as of the filing of this application, Web.com reserves the right to revisit the length of the Trademark Claims Service.

During the Trademark Claims period, in accordance with ICANN's requirements, Web.com or the Web.com-approved registrar will send a Trademark Claims Notice to any prospective registrant of a domain name that is an identical match (as defined in the ICANN Applicant Guidebook) to any mark that is validated in the Trademark Clearinghouse. The Trademark Claims Notice will include links to the Trademark Claims as listed in the Trademark Clearinghouse and will be provided at no cost.

Prior to registration of said domain name, Web.com or the Web.com-approved registrar will require each prospective registrant to provide the warranties dictated in the Trademark Clearinghouse model set forth in the ICANN Applicant Guidebook. Those warranties will include receipt and understanding of the Trademark Claims Notice and confirmation that registration and use of said domain name will not infringe on the trademark rights of the mark holders listed. Without receipt of said warranties, Web.com or the Web.com-approved registrar will not have the ability to process the domain name registration.

Following the registration of a domain name, the Web.com-approved registrar will provide a notice of domain name registration to the holders of marks that have been previously validated by the Trademark Clearinghouse and are an identical match. This notice will be as dictated by ICANN. At a minimum Web.com will recognize, honor and adhere to all word marks validated by the Trademark Clearinghouse.

#### Adoption of Certain SSWG Elevated Security Standards

As referenced earlier in this question, Web.com will work to implement the following elevated security standards in the .web gTLD:

##### Name Selection Policy

The .web gTLD will enforce a name selection policy that ensures that all names registered in the gTLD will be in compliance with ICANN mandated technical

standards. These include restrictions on 2 character names, tagged names, and reserved names for Registry Operations. All names must also be in compliance with all applicable RFCs governing the composition of domain names. In addition, registrations of Country, Geographical and Territory Names will only be allowed in compliance with the restrictions as outlined in the answer to Question 22.

#### Name Allocation Policy

As described above, Web.com plans on implementing an extended Sunrise A period for Trademark Holders and a Sunrise B Period for domain name holders. In addition, our current plans call for incorporating a Landrush Period during which applicants can secure preferred .web domains, followed by a General Availability. With the exception of the Sunrise B Period, all registrations will occur on a first come first served basis. Web.com reserves the right to adjust this allocation Policy as it works through implementation details.

#### Acceptable Use Policy

Web.com has developed a draft the Registry Operator Acceptable Use Policy (AUP) which is further described in our response to Question 28. This AUP clearly defines what type of behavior is expressly prohibited in conjunction with the use of a .web domain name. Web.com will require, through the Registry Registrar Agreement (RRA), that this AUP be included in the registration agreement used by all .web gTLD accredited registrars. This registration agreement must be agreed upon by a registrant prior to them being able to register a name in the .web gTLD.

## 2 MECHANISMS DESIGNED TO IDENTIFY AND ADDRESS THE ABUSIVE USE OF REGISTERED NAMES ON AN ONGOING BASIS

In addition to the Sunrise and Trademark Claims services described in Section 1 of this response, Web.com will implement and adhere to RPMs post-launch as mandated by ICANN, and confirm that registrars accredited for the .web gTLD are in compliance with these mechanisms. Certain aspects of these post-launch RPMs may be administered on behalf of Web.com by Web.com-approved registrars or by approved subcontractors of Web.com, such as its selected backend registry services provider, Verisign.

These post-launch RPMs include the established Uniform Domain Name Dispute Resolution Policy (UDRP), as well as the newer Uniform Rapid Suspension System (URS) and Trademark Post-Delegation Dispute Resolution Procedure (PDDRP). Where applicable, Web.com will implement all determinations and decisions issued under the corresponding RPM.

After a domain name is registered, trademark holders may object to the registration through the UDRP or URS. Objections to the operation of the gTLD can be made through the PDDRP.

The following descriptions provide implementation details of each post-launch RPM for the .web gTLD:

- **UDRP:** The UDRP provides a mechanism for complainants to object to domain name registrations. The complainant files its objection with a UDRP provider and the domain name registrant has an opportunity to respond. The UDRP provider makes a decision based on the papers filed. If the complainant is successful, ownership of the domain name registration is transferred to the complainant. If the complainant is not successful, ownership of the domain name remains with the domain name registrant. Web.com and entities operating on its behalf adhere to all decisions rendered by UDRP providers.
- **URS:** As provided in the Applicant Guidebook, all registries are required to implement the URS. Similar to the UDRP, a complainant files its objection with a URS provider. The URS provider conducts an administrative

review for compliance with filing requirements. If the complaint passes review, the URS provider notifies the registry operator and locks the domain. A domain lock means that the registry restricts all changes to the registration data, but the name will continue to resolve. After the domain is locked, the complaint is served to the domain name registrant, who has an opportunity to respond accordingly. If the complainant is successful, the registry operator is informed and the domain name is suspended for the balance of the registration period; the domain name will not resolve to the original source, but to an informational approved web page provided by the URS provider. If the complainant is not successful, the URS is terminated and full control of the domain name registration is returned to the domain name registrant. Similar to the existing UDRP, Web.com and entities operating on its behalf adhere to decisions rendered by the URS providers.

- **PDDRP:** As provided in the Applicant Guidebook, all registries are required to implement the PDDRP. The PDDRP provides a mechanism for a complainant to object to the registry operator's manner of operation or use of the gTLD. The complainant files its objection with a PDDRP provider, who performs a threshold review. The registry operator has the opportunity to respond and the provider issues its determination based on the papers filed, although there may be opportunity for further discovery and a hearing. Web.com participates in the PDDRP process as specified in the Applicant Guidebook.

Additional Measures Specific to Rights Protection. Web.com provides additional measures against abusive registrations. These measures will assist with mitigation of, but are not limited to, the following activities: phishing, pharming, and other Internet security threats. The measures exceed the minimum requirements for RPMs defined by Specification 7 of the Registry Agreement and are available at the time of registration.

These measures include:

- **Rapid Takedown or Suspension Based on Court Orders:** Web.com complies promptly with any order from a court of competent jurisdiction that directs it to take any action on a domain name that is within its technical capabilities as a gTLD registry. These orders may be issued when abusive content, such as but not limited to child pornography, counterfeit goods or illegal pharmaceuticals, is associated with the domain name.
- **Anti-Abuse Process:** Web.com implements an anti-abuse process that is executed based on the type of domain name takedown requested. The anti-abuse process is for malicious exploitation of the DNS infrastructure, such as phishing, botnets, and malware.
- **Authentication Procedures:** Verisign, Web.com's selected backend registry services provider, uses two-factor authentication to enhance security protocols for telephone, email, and chat communications.
- **Registry Lock:** Verisign's Registry Lock service allows registrants to lock a domain name at the authoritative registry level to protect against both unintended and malicious changes, deletions, and transfers. Only Verisign, as Web.com's backend registry services provider, can release the lock; thus all other entities that normally are permitted to update Shared Registration System (SRS) records are prevented from doing so. This lock is released only after the authorized registrar makes the request to unlock.
- **Malware Code Identification:** This safeguard reduces opportunities for abusive behaviors that use registered domain names in the gTLD. Registrants are often unknowing victims of malware exploits. As Web.com's backend registry services provider, Verisign has developed proprietary code to help identify malware in the zones it manages, which in turn helps registrars by identifying malicious code hidden in their domain names.
- **DNSSEC Signing Service:** Domain Name System Security Extensions (DNSSEC) helps mitigate pharming and phishing attacks that use cache poisoning to redirect unsuspecting users to fraudulent websites or addresses. It uses public key cryptography to digitally sign DNS data when it comes into the system and then validate it at its destination. The .web gTLD is DNSSEC-enabled as part of Verisign's core backend registry services.

- Biannual Whois Verification As detailed in our response to Question 28, all .web gTLD accredited registrars will be required as part of their RRA with Web.com to perform a Whois confirmation process twice a year. By asking registrants to confirm this information every 6 months, the .web gTLD should have a higher level of accurate Whois information for registered names in the event there is a case of trademark infringement by a non authorized registrant. Having accurate Whois information is critical to solving these issues in a timely manner.
- Participation in Anti-abuse Community Activities. Since our founding in 1997, Web.com has been an active participant and leader in multiple organizations, symposia, forums and other efforts that focus on the prevention of domain name abuse, including trademark infringement. Specifically, we are an active member of the Certificate Authentication Board, ICANN, the Internet standards development community, and we participate in SSAC. We find this participation extremely helpful in staying abreast of the latest changes and challenges in this field. Participation in these efforts also allows us to not only share our best practices with the rest of the anti-abuse community, but to learn from what others have been doing and incorporate it into how we operate our business. As mentioned earlier in this question, Web.com will be incorporating some of the SSWG enhanced security standards which is proof that community led efforts can produce significant results.

### 3. RESOURCING PLANS

#### Resource Planning

Web.com is a leading provider of Internet services for small to medium-sized businesses (SMBs). Web.com is the parent company of two global domain name registrars and further meets the Internet needs of consumers and businesses throughout their lifecycle with affordable value added services that including domain name registration, website design, search engine optimization, search engine marketing, social media and mobile products, local sales leads, eCommerce solutions and call center services. Headquartered in Jacksonville, FL, USA, Web.com is NASDAQ traded company serving nearly three million customers with more than 1,700 global employees in fourteen locations in North America, South America and the United Kingdom.

Our business is helping people establish, maintain, promote, and optimize their web presence. Web.com intentionally chose Verisign as our registry services provider because of their unsurpassed track record in operating some of the world's most complex and critical top level domains. Verisign's support for the .web gTLD will help ensure its success

The .web gTLD will be fully supported by a cross function team of Web.com professionals. Numbers and types of employees will vary for each function but Web.com projects it will use the following personnel to support the resource planning requirements;

- Quality Assurance Engineer: 0.5 FTE
- System Administrator: 1 FTE
- Database Administrator: 0.5 FTE
- Technical Project Manager: 0.5 FTE
- Marketing Director: 1 FTE
- Sales Manager: 1 FTE
- Legal Counsel: 1 FTE
- Finance/Accounting: 1 FTE
- Customer Service: 2 FTEs

#### Resource Planning Specific to Backend Registry Activities

Verisign, Web.com's selected backend registry services provider, is the most experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely modifies these staffing models

to account for new tools, standards and policy implementations and process innovations. These models enable Verisign to continually allocate the appropriate staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it will extend to Web.com fully accounts for cost related to this infrastructure, which is provided as Line IIb.G, Total Critical Registry Function Cash Outflows, within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability at 100 percent of the time for more than 13 years for .com, which exceeds the current several level agreements, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's gTLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support the implementation of RPMs:

- Customer Affairs Organization: 9
- Customer Support Personnel: 36
- Information Security Engineers: 11

To implement and manage the .web gTLD as described in this application, Verisign, Web.com's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of gTLDs. Consistent with its resource modeling, Verisign frequently reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified and skilled candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its gTLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its gTLD best practices are followed consistently. This consistent demonstration of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest gTLDs (i.e., .com). Moreover, by augmenting existing teams, Verisign ensures new employees are provided the opportunity to be trained and mentored by existing senior staff. This coaching and mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

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

1 DETAILED DESCRIPTION OF PROCESSES AND SOLUTIONS DEPLOYED TO MANAGE LOGICAL SECURITY ACROSS INFRASTRUCTURE AND SYSTEMS, MONITORING AND DETECTING THREATS AND SECURITY VULNERABILITIES AND TAKING APPROPRIATE STEPS TO RESOLVE THEM

Please note; all figures, tables and diagrams referenced in the following response can be found in attachment titled "Attachment dot web Q30A."

Web.com Group, Inc. ("Web.com") selected backend registry services provider's (Verisign's) comprehensive security policy has evolved over the years as part of managing some of the world's most critical TLDs. Verisign's Information Security Policy is the primary guideline that sets the baseline for all other policies, procedures, and standards that Verisign follows. This security policy addresses all of the critical components for the management of backend registry services, including architecture, engineering, and operations.

Verisign's general security policies and standards with respect to these areas are provided as follows:

- Architecture
  - Information Security Architecture Standard: This standard establishes the Verisign standard for application and network architecture. The document explains the methods for segmenting application tiers, using authentication mechanisms, and implementing application functions.
  - Information Security Secure Linux Standard: This standard establishes the information security requirements for all systems that run Linux throughout the Verisign organization.
  - Information Security Secure Oracle Standard: This standard establishes the information security requirements for all systems that run Oracle throughout the Verisign organization.
  - Information Security Remote Access Standard: This standard establishes the information security requirements for remote access to terminal services throughout the Verisign organization.
  - Information Security SSH Standard: This standard establishes the information security requirements for the application of Secure Shell (SSH) on all systems throughout the Verisign organization.
- Engineering
  - Secure SSL/TLS Configuration Standard: This standard establishes the information security requirements for the configuration of Secure Sockets Layer/Transport Layer Security (SSL/TLS) for all systems throughout the Verisign organization.
  - Information Security C++ Standards: These standards explain how to use and implement the functions and application programming interfaces (APIs) within C++. The document also describes how to perform logging, authentication, and database connectivity.
  - Information Security Java Standards: These standards explain how to use and implement the functions and APIs within Java. The document also describes how to perform logging, authentication, and database connectivity.
- Operations
  - Information Security DNS Standard: This standard establishes the information security requirements for all systems that run DNS systems throughout the Verisign organization.
  - Information Security Cryptographic Key Management Standard: This standard provides detailed information on both technology and processes for the use of encryption on Verisign information security systems.
  - Secure Apache Standard: Verisign has a multitude of Apache web servers, which are used in both production and development environments on the Verisign intranet and on the Internet. They provide a centralized, dynamic, and extensible interface to various other systems that deliver information to the end user. Because of their exposure and the confidential nature of the data that these systems host, adequate security measures must be in place. The Secure Apache Standard establishes the information security requirements for all systems that run Apache web servers throughout the Verisign organization.
  - Secure Sendmail Standard: Verisign uses sendmail servers in both the production and development environments on the Verisign intranet and on the Internet. Sendmail allows users to communicate with one another via email. The Secure Sendmail Standard establishes the information security requirements for all systems that run sendmail servers throughout the Verisign organization.
  - Secure Logging Standard: This standard establishes the information

security logging requirements for all systems and applications throughout the Verisign organization. Where specific standards documents have been created for operating systems or applications, the logging standards have been detailed. This document covers all technologies.

- Patch Management Standard: This standard establishes the information security patch and upgrade management requirements for all systems and applications throughout Verisign.

- General

- Secure Password Standard: Because passwords are the most popular and, in many cases, the sole mechanism for authenticating a user to a system, great care must be taken to help ensure that passwords are "strong" and secure. The Secure Password Standard details requirements for the use and implementation of passwords.

- Secure Anti-Virus Standard: Verisign must be protected continuously from computer viruses and other forms of malicious code. These threats can cause significant damage to the overall operation and security of the Verisign network. The Secure Anti-Virus Standard describes the requirements for minimizing the occurrence and impact of these incidents.

Security processes and solutions for the .web gTLD are based on the standards defined above, each of which is derived from Verisign's experience and industry best practice. These standards comprise the framework for the overall security solution and applicable processes implemented across all products under Verisign's management. The security solution and applicable processes include, but are not limited to:

- System and network access control (e.g., monitoring, logging, and backup)

- Independent assessment and periodic independent assessment reports

- Denial of service (DoS) and distributed denial of service (DDoS) attack mitigation

- Computer and network incident response policies, plans, and processes

- Minimization of risk of unauthorized access to systems or tampering with registry data

- Intrusion detection mechanisms, threat analysis, defenses, and updates

- Auditing of network access

- Physical security

Further details of these processes and solutions are provided in Part B of this response.

#### 1.1 Security Policy and Procedures for the Proposed Registry

Specific security policy related details, requested as the bulleted items of Question 30 - Part A, are provided here.

Independent Assessment and Periodic Independent Assessment Reports. To help ensure effective security controls are in place, Web.com, through its selected backend registry services provider, Verisign, conducts a yearly American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) SAS 70 audit on all of its data centers, hosted systems, and applications. During these SAS 70 audits, security controls at the operational, technical, and human level are rigorously tested. These audits are conducted by a certified and accredited third party and help ensure that Verisign in-place environments meet the security criteria specified in Verisign's customer contractual agreements and are in accordance with commercially accepted security controls and practices. Verisign also performs numerous audits throughout the year to verify its security processes and activities. These audits cover many different environments and technologies and validate Verisign's capability to protect its registry and DNS resolution environments. Figure 30A-1 lists a subset of the audits that Verisign conducts. For each audit program or certification listed in Figure 30A-1, Verisign has included, as attachments to the Part B component of this response, copies of the assessment reports conducted by the listed third-party auditor. From Verisign's experience operating registries, it has determined that together

these audit programs and certifications provide a reliable means to ensure effective security controls are in place and that these controls are sufficient to meet ICANN security requirements and therefore are commensurate with the guidelines defined by ISO 27001.

Augmented Security Levels or Capabilities. See Section 5 of this response.

Commitments Made to Registrants Concerning Security Levels. See Section 4 of this response.

## 2 SECURITY CAPABILITIES ARE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the .web gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

## 3 TECHNICAL PLAN ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

### Resource Planning

Web.com is a leading provider of Internet services for small to medium-sized businesses (SMBs). Web.com is the parent company of two global domain name registrars and further meets the Internet needs of consumers and businesses throughout their lifecycle with affordable value added services that including domain name registration, website design, search engine optimization, search engine marketing, social media and mobile products, local sales leads, eCommerce solutions and call center services. Headquartered in Jacksonville, FL, USA, Web.com is NASDAQ traded company serving nearly three million customers with more than 1,700 global employees in fourteen locations in North America, South America and the United Kingdom.

Our business is helping people establish, maintain, promote, and optimize their web presence. Web.com intentionally chose Verisign as our registry services provider because of their unsurpassed track record in operating some of the world's most complex and critical top level domains. Verisign's support for the .web gTLD will help ensure its success.

The .web gTLD will be fully supported by a cross function team of Web.com professionals. Numbers and types of employees will vary for each function but Web.com projects it will use the following personnel to support the resource planning requirements:

- Quality Assurance Engineer: 0.5 FTE
- System Administrator: 1 FTE
- Database Administrator: 0.5 FTE
- Technical Project Manager: 0.5 FTE



- Marketing Director: 1 FTE
- Sales Manager: 1 FTE
- Legal Counsel: 1 FTE
- Finance/Accounting: 1 FTE
- Customer Service: 2 FTEs

#### Resource Planning Specific to Backend Registry Activities

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel role, which is described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support its security policy:

- Information Security Engineers: 11

To implement and manage the .web gTLD as described in this application, Verisign, Web.com's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only the .web gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this the .web gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

#### 4 SECURITY MEASURES ARE CONSISTENT WITH ANY COMMITMENTS MADE TO REGISTRANTS REGARDING SECURITY LEVELS

Verisign is Web.com's selected backend registry services provider. For the .web gTLD, no unique security measures or commitments must be made by Verisign or Web.com to any registrant.

5 SECURITY MEASURES ARE APPROPRIATE FOR THE APPLIED-FOR gTLD STRING (FOR EXAMPLE, APPLICATIONS FOR STRINGS WITH UNIQUE TRUST IMPLICATIONS, SUCH AS FINANCIAL SERVICES-ORIENTED STRINGS, WOULD BE EXPECTED TO PROVIDE A COMMENSURATE LEVEL OF SECURITY)

No unique security measures are necessary to implement the .web gTLD. As defined in Section 1 of this response, Verisign, Web.com's selected backend registry services provider, commits to providing backend registry services in accordance with the following international and relevant security standards:

- American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) SAS 70
- WebTrust/SysTrust for Certification Authorities (CA)

© *Internet Corporation For Assigned Names and Numbers.*



# **Annex 4.**



## New gTLD Application Submitted to ICANN by: DotWeb Inc.

String: web

Originally Posted: 13 June 2012

Application ID: 1-956-26846

### Applicant Information

#### 1. Full legal name

DotWeb Inc.

#### 2. Address of the principal place of business

Contact Information Redacted

#### 3. Phone number

Contact Information Redacted

#### 4. Fax number

Contact Information Redacted

## 5. If applicable, website or URL

<http://www.radixregistry.com>

## Primary Contact

### 6(a). Name

Mr. Brijesh Harish Joshi

### 6(b). Title

Director & GM

### 6(c). Address

### 6(d). Phone Number

Contact Information Redacted

### 6(e). Fax Number

### 6(f). Email Address

Contact Information Redacted

## Secondary Contact

### 7(a). Name

Mr. Namit Sunil Merchant

**7(b). Title**

General Manager

**7(c). Address**

**7(d). Phone Number**

Contact Information Redacted

**7(e). Fax Number**

**7(f). Email Address**

Contact Information Redacted

**Proof of Legal Establishment**

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

International Business Company (Limited Liability Company)

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

Republic of Seychelles, International Business Companies Act, 1994 (Act 24 of 1994)

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

Attachments are not displayed on this form.

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

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

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

## Applicant Background

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

Brijesh Joshi	Director & General Manager
---------------	----------------------------

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

Brijesh Joshi	Director & General Manager
Namit Merchant	General Manager
Vishal Manjalani	Vice President

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

Directi FZC dba Radix	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.**

web



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

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

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

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

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

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

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

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

Attachments are not displayed on this form.

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

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

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

We have engaged ARI Registry Services (ARI) to deliver backend technology services for this TLD.

ARI is experienced with:

- The operational issues of operating TLDs, including ccTLDs.
- TLDs that offer registrations at the third level (e.g. .com.au, .net.au) and which have their own set of unique issues.
- The rendering and operational issues surrounding the introduction of IDNs.

The following is the result of ARI's analysis.

1. INTRODUCTION

ARI has not found any issues unique to this TLD with respect to operational and rendering issues.

This has been established by:

- Testing of the TLD string itself.
- Researching issues experienced by others.
- Our understanding of published material.
- Our own experience.

2. LOCAL TESTING OF THE TLD STRING

ARI has executed a suite of tests to evaluate any issues arising from the use of the TLD string. ARI configured a test environment that consisted of DNS software that served authoritative responses for this TLD, web server software that hosted a simple website, and an email server that provided mailboxes for sample domains in this TLD. Testing included:

- Navigation of websites using the address bar and hyperlinks.
- Composition and delivery of mail.
- Mail filters such as spam detection.
- Display of domain names in address bars, hyperlinks, and free text.

Where possible, ARI attempted to test many equivalent applications, however the number of and different versions of applications means that testing was limited to the more common environments. Tested platforms and applications included:

- Microsoft Windows, Apple OS X and Red Hat Linux.
- Internet Explorer, Safari, Opera, Firefox and Chrome.
- Exchange, Sendmail and Postfix.

ARI did not find any operational or rendering issues with this TLD that are unique to this TLD.

This completes our response to Q16.

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

## Mission/Purpose

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

The mission/purpose of .web is first choice. Domain name first choice, once again - globally. Some registrants got their first choice of a .com name. Many did not. When the .com registry gained its momentum selling names early on, the North American market and particularly the United States were the first and primary purchasers of .com names. They got their first choice. And many global registrants who came after did not. Other generic top level domains have been introduced: .info, .biz, .net, .org - but none of those names have the true global generic appeal of the .com brand. Each of those four strings brings some characteristic that taints the string with some preconception.

- \* .info is short for information - but my site does much more than information
- \* .biz is short for business - but my site is not business related
- \* .net is short for network - but the term "the net" died several years ago
- \* .org is short for organization - but my site is not a non-profit
- \* .com is short for commercial or company, and is not truly a generic extension

Country code top-level domains (ccTLD) are an option, however a ccTLD such as Germany (.DE) or Japan (.JP) brings the impression that the website is tied to the country or region, but not truly global. Hence the need for .web - a truly generic top level domain that means the same in Shanghai, Munich, Sao Paulo, Mumbai, Johannesburg, Tokyo and your city. The mission of .web is to give international registrants the same opportunity the North American market had - to get their unique name in a truly global name space - with nothing added - just trusted and secure access to the web. The mission of .web is first choice.

The goal of .web is to provide first choice name registration to individuals, entrepreneurs, communities, small and medium sized businesses, multi-national corporations, non-profits and anyone else seeking a truly global domain name. Based on our experience, when a potential registrant goes to a registrar's site to register a new gTLD domain name, the domain name is unavailable over 70% of the time (Source: Internal Research on com availability checks) and the registrant is presented with a long list of permutation options that are not their first choice - either for the name or the TLD.

The goal of .web is to register your first choice name. The Mission and purpose of our TLD is also to contribute to the Internet Namespace in the following ways:

#### 1.1 ENHANCE REGISTRANT CHOICE

To create a namespace that provides registrants greater choice to represent themselves online in the manner they please. Due to the saturated nature of the existing gTLD space, many Internet users have to opt for a name that does not suit their needs best. Our Registry will provide Registrants a higher probability of obtaining their desired name.

#### 1.2 CREATE A CLEANER INTERNET SPACE

To create a cleaner internet experience for end users by implementing pioneering registration policies, content and usage policies, and abuse

mitigation processes.

### 1.3 CREATE A STABLE AND RESILIENT INTERNET SPACE

To deliver a stable and resilient internet experience to registrants and end-users by going above and beyond the ICANN mandated SLAs and delivering 100% resolution uptime

This completes our response to Q18(a).

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

### 1. GOAL OF .WEB

#### 1.1 SPECIALTY

\* Our goal for .web in terms of area of specialty is to be the first choice generic TLD among new registrants. We will support the rapidly developing domain name markets, not just in traditional markets such as Western Europe and North America, but equally in the growing regions of South America, Asia, Eastern Europe, the entire Pacific Rim. The .web registry will provide registrants the opportunity for first choice of their preferred domain name on a generic global TLD.

#### 1.2 SERVICE LEVELS

Our goal for .Web in terms of service levels is to go above and beyond the ICANN SLAs. ICANN provides for its expected SLA in Specification 10 in the Registry Agreement in the Applicant guidebook.

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provides registry services for a number of TLDs including the .au ccTLD.

Our contract with ARI is attached to our response to Q46. This contract details the SLA we intend on achieving with this TLD. As can be seen in the contract we have exceeded the ICANN required SLA on every parameter.

Our response to Q34 and Q35 provides details on ARI's distributed anycast DNS network. ARI's DNS network provides for 16 geo distributed sites resulting in a very low resolution latency for end-users, amongst the lowest in the industry.

It is our objective to provide 100% uptime, a resilient global DNS infrastructure, and very low latency in terms of DNS resolution for this TLD

#### 1.3 REPUTATION

Reputation of our TLD is of paramount importance to us. The reputation of our TLD directly relates to how end-users on the internet perceive our Registrants.

We will ensure the highest reputation of .Web by ensuring the following -

- \* Maintaining a high quality bar with respect to Registrants in the TLD
- \* Well defined Acceptable usage and content policies
- \* Well defined dispute resolution mechanisms
- \* Ensuring Whois accuracy to support abuse mitigation
- \* Well defined and implemented abuse mitigation processes
- \* Well defined and implemented rights protection mechanisms
- \* Exceptional service levels

To this effect we have created unprecedented Abuse mitigation policies and Rights protection mechanisms that go significantly above and beyond mandatory requirements and common practice described in considerable detail in our

response to Q28 and Q29. We also commit to extremely high service levels that go beyond the stipulated service levels in the applicant guidebook.

## 2. CONTRIBUTION OF .WEB TO THE NAMESPACE

### 2.1 CONTRIBUTION IN TERMS OF COMPETITION, DIFFERENTIATION, OR INNOVATION

Per ICANN's Bylaws as amended June 24, 2011, ICANN's core value number six is "Introducing and promoting competition in the registration of domain names where practicable and beneficial in the public interest."

The .web registry will be a new direct and formidable competitor to the current group of global generic TLDs. This will be especially true in the key growing international markets. Since Directi has been a registrar for over 10 years, managing over 4 million domain names across the globe, we understand the nuances of domain name buying behaviour. The .Web registry will leverage this unique market knowledge to design competitive offerings against other global gTLDs.

Directi will be offering the language and culture agnostic .web to international markets, with the goal of a truly global distribution of registrants. Most gTLDs have largely focused on developed markets with 70+% internet penetration, namely North America and European marketplaces. Domain Name and website growth is yet to occur in other developing markets like India, Brazil, Russia, China, Indonesia etc. However as the market for websites and domain names grows in these economies the existing gTLD space in TLDs like .com, .net, .org etc will already be saturated with all tier 1 names no longer available to markets like asia, africa. 70% of .com check availability checks return unavailable (data obtained from Internal Reserach). New companies have to resort to 2nd tier long multi-word names for their businesses in these markets. .Web will broaden the namespace by providing an alternative for Registrants in developing markets to register the domain name of their choice, creating competition.

Lastly .Web will provide registrants the option to register more desirable and shorter names as opposed to names they would have otherwise registered in existing gTLDs due to the high saturation of the existing namespaces.

Our intent is to operate .Web with a focus on integrity and quality for the .Web brand. This entails running robust abuse mitigation programs and pioneering Rights Protection Mechanisms from initiation, which in our case not only meets ICANN's requirements, but extends significantly beyond it as described in our response to Q28 and Q29.

## 3. USER EXPERIENCE GOALS

.Web considers both its Registrants and the end-users that access .Web websites as its users. Our goal is to create a highly reliable namespace and provide an outstanding user experience to both Registrants and end-users of .Web.

Registrants of .Web have an assurance of a scalable, resilient registry with 100% uptime, low latency, and exemplary security standards. Registrants will have the option to register the domain name of their choice, without much saturation of the namespace. Our registration policies and abuse mitigation policies ensure that Registrants will get advantages like higher recognition, better branding and more desirable, shorter names.

Our content and acceptable use policies and abuse mitigation processes ensure that end-users are benefited from a clean namespace. These are described in further detail in our response to Q28 and Q29.

## 4. REGISTRATION POLICIES IN SUPPORT OF GOALS

### 4.1 GENERAL NAMES

The purpose of .web is to allow registrants to register their first choice name. As such, the TLD will offer registrations at the second level, and will have an open registration policy so that registrants have the choice and the freedom to find the name that they like best. The TLD will be open to registrants in all areas of the world, without nexus or pre-qualification requirements. Registrations in .web can be used for any purpose, including for use by businesses, individuals, and not-for-profit entities. We anticipate that registrants will introduce many unique, new, dedicated Web sites to the Internet using their .web domain names.

The goals of .Web are outlined in the sections above. These goals are supported by the following artifacts -

- \* Registration policies and processes
- \* Acceptable usage policies and content guidelines
- \* Abuse mitigation processes
- \* Rights protection mechanisms
- \* Dispute resolution polices

To this effect we have created unprecedented Abuse mitigation policies and Rights protection mechanisms that go significantly above and beyond mandatory requirements and common practice. The salient aspects of all of the above are described below -

- \* DotWeb Inc. is a wholly owned subsidiary within the Directi Group. The Directi Group runs various businesses including several ICANN Accredited Domain Registrars (ResellerClub.com and BigRock.com) and Web Hosting companies. With over four million active domain names registered through its registrars, Directi has significant experience (over 10 years) of managing domain name abuse mitigation and rights protection. Directi has been heralded as a white hat registrar and the undisputed leader with respect to abuse mitigation.
- \* Our Abuse and compliance processes will be run by the Directi Group
- \* We have an elaborate and detailed Accepted usage and content policy that covers over 11 macro forms of violations
- \* .Web will create a zero-tolerance reputation when it comes to abuse
- \* We have a defined SLA for responding to abuse complaints ensuring guaranteed turn-around time on any abuse complaint depending on its severity
- \* We will work closely with LEA and other security groups to mitigate abuse within the TLD by providing them with special interfaces (eg searchable whois) and interacting with them regularly in terms of knowledge sharing.
- \* Other abuse mitigation steps we undertake include profiling, blacklisting, proactive quality reviews, industry collaboration and information sharing, regular sampling, contractual enforcements and sanctions
- \* The protection of trademark rights is a core goal of .Web. .Web will have a professional plan for rights protection. It will incorporate best practices of existing TLDs, going above and beyond the ICANN mandated RPMs to prevent abusive registrations and rapidly take-down abuse when it does occur.
- \* Standard RPMs such as Sunrise, Trademarks claims service, URS, UDRP, SDRP, PDDRP, SPOC etc are all provided for. Additional RPMs such as Optional Trademark declaration, profiling and blacklisting, proactive quality reviews, APWG Review and others will also be provided.

The above salient points barely scratch the surface in detailing the steps that .Web will take in order to build a reputation of operating a clean, secure and trusted namespace. Significant details of all of the above and more are provided in our responses to Q26, Q27, Q28 and Q29

#### 4.2. OTHER NAMES

- \* We will reserve the following classes of domain names, which will not be available to registrants via the Sunrise or subsequent periods:
  - \*\* The reserved names required in Specification 5 of the new gTLD Registry Agreement.
  - \*\* The geographic names required in Specification 5 of the new gTLD Registry

Agreement. See our response to Question 22 ("Protection of Geographic Names") for details.

\*\* The registry operator will reserve its own name and variations thereof, and registry operations names (such as nic.Web, registry.Web, and www.Web), so that we can point them to our Web site. Reservation of the registry operator's names was standard in ICANN's past gTLD contracts.

\*\* We will also reserve names related to ICANN and Internet standards bodies (iana.Web, ietf.Web, w3c.Web, etc.), for delegation of those names to the relevant organizations upon their request. Reservation of this type of names was standard in ICANN's past gTLD contracts. The list of reserved names will be published publicly before the Sunrise period begins, so that registrars and potential registrants will know which names have been set aside.

\* We will reserve generic names which will be set aside for distribution via special mechanisms.

## 5. PROTECTING PRIVACY OF REGISTRANTS' OR USERS' INFORMATION

.Web is committed to providing a secure and trusted namespace to its Registrants and end-users. To that extent we will have several measures for protecting the privacy or confidential information of registrants or users -

\* Our Whois service (web-based whois, port 43 whois and searchable whois) all have built in abuse prevention mechanisms to prevent unauthorized access, data mining, data scraping and any other abusive behavior. Details of this are provided in our response to Q26

\* .Web will allow Registrants to use privacy protection services provided by their Registrars in the form of a Proxy whois service as long as they follow the guidelines stipulated within our response to Q28 to prevent any abuse of the same

\* As per the requirements of the new gTLD Registry Agreement (Article 2.17), we shall notify each of our registrars regarding the purposes for which data about any identified or identifiable natural person ("Personal Data") submitted to the Registry Operator by such registrar is collected and used, and the intended recipients (or categories of recipients) of such Personal Data. (This data is basically the registrant and contact data required to be published in the WHOIS.)

\* We will also require each registrar to obtain the consent of each registrant in the TLD for such collection and use of Personal Data. As the registry operator, we shall not use or authorize the use of Personal Data in a way that is incompatible with the notice provided to registrars.

\* As the registry operator we shall take significant steps to protect Personal Data collected from registrars from loss, misuse, unauthorized disclosure, alteration, or destruction. In our responses to Q24, Q30 and Q38 we detail the security policies and procedures we will use to protect the registry system and the data contained there from unauthorized access and loss.

\* As registry operator we impose certain operational standards for our registrars. In order to gain and maintain accreditation for our TLD, we require them to adhere to certain information technology policies designed to help protect registrant data. These include standards for access to the registry system. Please see our response to Q24, Q25 and Q30 for details.

\* We offer a "registry lock" service, designed to help protect participating registrants' contact data from unauthorized modification, and against unauthorized domain transfers and deletions. Please see our response to Q27 for details.

\* .Web implements DNSSEC at the zone which guarantees origin authentication of DNS data, authenticated denial of existence, and data integrity. This protects

end-users from a man-in-the-middle attack protecting the privacy of data of end-users.

## 6. OUTREACH AND COMMUNICATIONS

\* Our goal for .web is for it to be the first-choice generic TLD among new registrants. To achieve this, we will emphasize distribution channels internationally.

\* We will also engage in relevant PR and outreach programs as well as ensure appropriate publication of information on our website.

\* For many Internet users, the World Wide Web is the first thing they think of when they think of the Internet. For first-time registrants, a .web TLD will be easy to understand and easy to communicate about.

\* Our outreach efforts will be directed towards our target market in coordination with Registrar partners, to ensure greater adoption of the .Web TLD. One important method of outreach will involve co-marketing programs with registrars. We will also leverage Directi's existing channel of 65,000 Resellers, and its strategic relationships with other ICANN Accredited Registrars.

The communication and outreach will focus on -

\* Educating audiences regarding this new namespace which has a high availability of names, and the immense possibilities and internet innovations that it could result in.

\* Generating awareness of our Registration policies, Acceptable usage and content policies, Abuse mitigation processes and Rights protection mechanisms

This completes our response to Q18(b).

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

.Web considers both its Registrants and the end-users that access .Web websites as its users. Our goal is to create a highly reliable namespace and provide an outstanding user experience to both Registrants and end-users of .Web. To that extent it is our goal to -

\* Reduce / minimize any incremental costs / negative consequences imposed upon our users

\* Increase / maximize the value added to our Registrants and end-users

\* Ensure that the net effect of .Web on its users is that of positive value creation

In this response we explore how .Web achieves a net benefit for Registrants and End-users.

### 1. MINIMIZING COSTS

#### 1.1 REGISTRANTS

It is our goal to provide Registrants of .Web incremental value and minimize any negative consequences and costs associated with .Web. We address this in the following manner

##### 1.1.1 SUNRISE, TMCH, RPMs



Rights protection is a core goal of .Web. Our Rights Protection mechanisms go significantly above and beyond the mandatory RPMs ensuring protection of trademark and IP rights of domain registrants and reducing the costs associated with rights protection for Registrants. Our elaborate RPMs are described in significant detail in our response to Q29. Some salient aspects of these are as follows -

- \* We offer a sunrise period to provide an opportunity for legitimate Registrants to block domain names in .Web before general availability begins, preventing unnecessary post-facto litigation

- \* We will integrate with the Trademark Clearing House in the manner prescribed to provide the Trademarks claims service, so as to alert potential Registrants of any trademark violations prior to registration, as well as notify mark holders of potential mark violations

- \* We will provide SDRP, URS, UDRP and PDDRP reducing litigation costs by providing legitimate Registrants the opportunity to resolve disputes through standardized arbitration proceedings.

- \* Additionally we have pioneering RPMs like Optional Trademark Declaration, Profiling and Blacklisting, Proactive Quality assurance, APWG review etc - all intended to reduce rights violations and hence reduce costs for Registrants

The above salient points barely scratch the surface in detailing the steps that .Web will take in order to reduce costs of Registrants with respect to rights violations. Significant details of all of the above and more are provided in our responses to Q26, Q27, Q28 and Q29.

#### 1.1.2 MULTIPLE APPLICATIONS FOR A DOMAIN

All of the RPMs described in section 1.1.1 above ensure that applicants for domain names in .Web are legitimate right holders for the applied string.

During general availability domain names will be allocated on a first come first serve basis amongst applicants. During the initial registry launch periods of Sunrise and Landrush if multiple applications for the same domain name are received from applicants then the same will be distributed in the following manner -

- \* In case of multiple sunrise applications for the same domain name, all applications will be validated against the TMCH for a valid trademark. Applications that do not qualify will be dropped.

- \* All remaining applications will be distributed through a fair auction.

#### 1.1.3 COST BENEFITS FOR REGISTRANTS

The ICANN new gTLD program marks a historical event in the timeline of the Internet. It is an unprecedented event and one that will yield tremendous benefits for consumers. At this preliminary stage it is impossible to determine the true value consumers will derive from increase in competition and choice. However there is historical data to go by. Upon the launch of Domain Registrars and creation of competition amongst registrars, the Registrants benefited from reduced pricing.

With .Web our goal is to provide fair pricing for domains within .Web that reflect the value proposition derived by the Registrants of .Web. While we do not have any committed pricing plans as yet and the same will be determined during the launch process, we do anticipate providing promotional offers through the life of .Web for the purpose of customer acquisition. This is not too dissimilar from other gTLD registries currently in existence who offer ongoing promotional offers to their customer base.

#### 1.1.4 PRICE ESCALATIONS

The ICANN new gTLD program is an unprecedented event and the actual nature of pricing pressures will only be determinable once several TLDs have successfully launched. At this preliminary stage it is impossible to commit to any pricing strategy on our part. We strongly believe that ultimately, the open market will determine the viability of pricing models and dictate pricing strategy for everyone. We intend to maintain the freedom to set pricing to accommodate for the existence of 100s of TLDs and business models and create a sustainable long term business model. Our goal is to provide fair pricing for domains within .Web that reflect the value proposition derived by the Registrants of .Web.

#### 1.2 END USERS

It is our goal to provide end users of .Web incremental value and minimize any negative consequences and costs associated with .Web. We address this in the following manner

End-users bear a considerable amount of cost as a result of various forms of Internet abuse such as spam, malware, phishing, pharming, hacking, identity theft etc. Any TLD that implements policies and processes to create a clean namespace will result in a considerable reduction of these forms of abuse and hence a significant saving in terms of cost to consumers

.Web intends to set an example when it comes to abuse mitigation and preventing abuse within .Web. To this effect we have created unprecedented Abuse mitigation policies and Rights protection mechanisms that go significantly above and beyond mandatory requirements and common practice. These are detailed in our response to Q28. We strongly believe these practices will result in a significant reduction in online abuse and considerable savings for end users of .Web. We similarly hope to set an example for other TLDs and cooperate with the industry in creating a clean internet experience for internet users.

#### 2. COST BENEFIT ANALYSIS

There has been considerable debate within the community concerning the cost benefit analysis of launching new gTLDs. We strongly believe that the launch of new gTLDs and our implementation of .Web will add considerable value and result in a net positive effect on Registrants and end-users worldwide.

We recognize that there will be a post launch review of the New gTLD Program, from the perspective of assessing the relative costs and benefits achieved in the expanded gTLD space.

To this extent we would like to offer the following pointers concerning .Web as well as the general expansion of the new gTLD space in determining the net positive value generated for Registrants and end users -

\* .Web will reduce overall cost for end-users in combating fraud and other forms of online abuse by implementing pioneering processes and anti-abuse policies as described in our response to Q28. Billions of dollars are spent worldwide combating various forms of fraud such as malware, phishing, spamming etc. Our abuse policies will result in overall reduction of these forms of abuses within .Web resulting in a considerable reduction in global costs spent towards combating these abuses. We also strongly believe that introduction of new gTLDs will result in increased competition which will drive significant innovation as well as competitive pressures for everyone in the industry to improve their abuse mitigation processes resulting in overall cost reduction for end-users

\* The value of a Registrant getting the name they want is immeasurably larger than any costs resulting from expansion of the namespace. DotWeb Inc. is a subsidiary within the Directi Group which owns and operates several ICANN

Accredited Registrars. Our stats show that 70% of the users who check for a .com domain name do not get their desired name. Until this launch of the new gTLD program there were very limited alternatives and none very viable/desirable for Registrants to choose from. .Web will expand the namespace thus providing a higher probability for new Registrants to obtain names they desire

\* In general increased competition always results in pricing benefits for Registrants. .Web will provide additional options to new Registrants resulting in overall benefits to Registrants

This completes our response to Q18(c).

## Community-based Designation

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

No

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

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

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

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

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

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

Attachments are not displayed on this form.

## Geographic Names

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

No

## Protection of Geographic Names

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

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. This response describes protection of geographic names as implemented by ARI.

1. PROTECTION OF GEOGRAPHIC NAMES

In accordance with Specification 5 of the New gTLD Registry Agreement, we will initially reserve all geographic names at the second level, and at all other levels within the TLD at which the registry operator provides for registrations.

ARI supports this requirement by using the following internationally recognised lists to develop a comprehensive master list of all geographic names that are initially reserved:

- The 2-letter alpha-2 code of all country and territory names contained on the ISO 3166-1 list, including all reserved and unassigned codes  
[[http://www.iso.org/iso/support/country\\_codes/iso\\_3166\\_code\\_lists/iso-3166-1\\_decoding\\_table.htm](http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166-1_decoding_table.htm)].

- The short form (in English) of all country and territory names contained on the ISO 3166-1 list, including the European Union, which is exceptionally reserved on the ISO 3166-1 List, and its scope extended in August 1999 to any application needing to represent the name European Union  
[[http://www.iso.org/iso/support/country\\_codes/iso\\_3166\\_code\\_lists/iso-3166-1\\_decoding\\_table.htm#EU](http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166-1_decoding_table.htm#EU)].

- The United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardisation of Geographical Names, Part III Names of Countries of the World. This lists the names of 193 independent States generally recognised by the international community in the language or languages used in an official capacity within each country and is current as of August 2006 [[http://unstats.un.org/unsd/geoinfo/ungegn/docs/pubs/UNGEGN%20tech%20ref%20manual\\_m87\\_combined.pdf](http://unstats.un.org/unsd/geoinfo/ungegn/docs/pubs/UNGEGN%20tech%20ref%20manual_m87_combined.pdf)].

- The list of UN member states in six official UN languages prepared by the

Working Group on Country Names of the United Nations Conference on the standardisation of Geographical Names  
[[http://unstats.un.org/unsd/geoinfo/UNGEEN/docs/9th-uncsgn-docs/econf/9th\\_UNCSGN\\_e-conf-98-89-add1.pdf](http://unstats.un.org/unsd/geoinfo/UNGEEN/docs/9th-uncsgn-docs/econf/9th_UNCSGN_e-conf-98-89-add1.pdf)].

Names on this reserved list in ARI's registry system are prevented from registration.

A corresponding list of geographic names will also be available to the public via our website, to inform Registrars and potential registrants of reserved names. The lists noted above, are regularly monitored for revisions, therefore the reserved list (both within the registry and publicly facing) will be continually updated to reflect any changes.

In addition to these requirements, ARI are able to support the wishes of the Governmental Advisory Council (GAC) or any individual Government in regard to the blocking of individual terms on a case by case basis. ARI's registry system allows such additions to be made by appropriately authorised staff, with no further system development changes required.

The following applies to all Domain Names contained within the registry's reserved list:

- Attempts to register listed Domain Names will be rejected.
- WhoIs queries for listed Domain Names will receive responses indicating their reserved status.
- Reserved geographic names will not appear in the TLD zone file.
- DNS queries for reserved domain names will result in an NXDOMAIN response.

## 2. PROCEDURES FOR RELEASE

We understand that if we wish to release the reserved names at a later date, this will require agreement from the relevant government(s) or review by the GAC, and subsequent approval from ICANN.

This completes our response to Q22.

# Registry Services

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

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. This response describes the Registry Services for our TLD, as provided by ARI.

### 1. INTRODUCTION

ARI's Managed TLD Registry Service is a complete offering, providing all of the required Registry services. What follows is a description of each of those services.

### 2. REGISTRY SERVICES

The following sections describe the registry services provided. Each of these services has, where required, been designed to take into account the requirements of consensus policies as documented here:

[<http://www.icann.org/en/resources/Registrars/consensus-policies>]

## 2.1 RECEIPT OF DATA FROM REGISTRARS

The day-to-day functions of the Registry, as perceived by Internet users, involves the receipt of data from Registrars and making the necessary changes to the SRS database. Functionality such as the creation, renewal and deletion of domains by Registrars, on behalf of Registrants, is provided by two separate systems:

- \* An open protocol -based provisioning system commonly used by Registrars with automated domain management functionality within their own systems.
- \* A dedicated website providing the same functionality for user interaction.

Registrants (or prospective Registrants) who wish to manage their existing domains or credentials, register new domains or delete their domains will have their requests carried out by Registrars using one of the two systems described below.

ARI operates Extensible Provisioning Protocol (EPP) server software and distributes applicable toolkits to facilitate the receipt of data from Registrars in a common format. EPP offers a common protocol for Registrars to interact with SRS data and is favoured for automating such interaction in the Registrar's systems. In addition to the EPP server, Registrars have the ability to use a web -based management interface (SRS Web Interface), which provides functions equivalent to the EPP server functionality.

### 2.1.1 EPP

The EPP software allows Registrars to communicate with the SRS using a standard protocol. The EPP server software is compliant with all appropriate RFCs and will be updated to comply with any relevant new RFCs or other new standards, as and when they are finalised. All standard EPP operations on SRS objects are supported.

Specifically, the EPP service complies with the following standards:

- \* RFC 5730 Extensible Provisioning Protocol (EPP).
- \* RFC 5731 Extensible Provisioning Protocol (EPP) Domain Name Mapping.
- \* RFC 5732 Extensible Provisioning Protocol (EPP) Host Mapping.
- \* RFC 5733 Extensible Provisioning Protocol (EPP) Contact Mapping.
- \* RFC 5734 Extensible Provisioning Protocol (EPP) Transport over TCP.
- \* RFC 5910 Domain Name System (DNS) Security Extensions for the Extensible Provisioning Protocol (EPP).
- \* RFC 3915 Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (EPP).
- \* Extensions to ARI's EPP service comply with RFC 3735 Guidelines for Extending the Extensible Provisioning Protocol (EPP).

#### 2.1.1.1 SECURITY FOR EPP SERVICE

To avoid abuse and to mitigate potential fraudulent operations, the EPP server software uses a number of security mechanisms that restrict the source of incoming connections and prescribe the authentication and authorisation of the client. Connections are further managed by command rate limiting and are restricted to only a certain number for each Registrar, to help reduce unwanted fraudulent and other activities. Additionally, secure communication to the EPP interface is required, lowering the likelihood of the authentication mechanisms being compromised.

The EPP server has restrictions on the operations it is permitted to make to the data within the Registry database. Except as allowed by the EPP protocol, the EPP server cannot update the credentials used by Registrars for access to the SRS. These credentials include those used by Registrars to login to ARI's SRS Web Interface and the EPP service.

Secure communication to the EPP server is achieved via the encryption of EPP sessions. The Registry system and associated toolkits support AES 128 and 256 via TLS.

All communication between the Registrar or the Registrars systems and the SRS is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57. The Production and Operational Testing and Evaluation (OTE) EPP service is protected behind a secure firewall that only accepts connections from registered IP addresses. Registrars are required to supply host IP addresses that they intend to use to access the EPP service.

Certificates are used for encrypted communications with the Registry. Registrars require a valid public/private key pair signed by the ARI CA to verify authenticity. These certificates are used to establish a TLS secure session between client and server.

EPP contains credential elements in its specification which are used as an additional layer of authentication. In accordance with the EPP specification, the server does not allow client sessions to carry out any operations until credentials are verified.

The EPP server software combines the authentication and authorisation elements described above to ensure the various credentials supplied are associated with the same identity. This verification requires that:

- \* The username must match the common name in the digital certificate.
- \* The certificate must be presented from a source IP listed against the Registrar whose common name appears in the certificate.
- \* The username and password must match the user name and password listed against the Registrar's account with that source IP address.

To manage normal operations and prevent an accidental or intentional Denial of Service, the EPP server can be configured to rate limit activities by individual Registrars.

Further details are provided for in Q24 and Q25.

#### 2.1.1.2 STABILITY CONSIDERATIONS

The measures that restrict Registrars to a limit of connections and operations for security purposes also serve to keep the SRS and the EPP server within an acceptable performance and resource utilisation band. Therefore, scaling the service is an almost linear calculation based on well-defined parameters.

The EPP server offers consistent information between Registrars and the SRS Web Interface. The relevant pieces of this information are replicated to the DNS within seconds of alteration, thus ensuring that a strong consistency between the SRS and DNS is maintained at all times.

#### 2.1.2 SRS WEB INTERFACE

The Registry SRS Web Interface offers Registrars an alternative SRS interaction mechanism to the EPP server. Available over HTTPS, this interface can be used to carry out all operations which would otherwise occur via EPP, as well as many others. Registrars can use the SRS Web Interface, the EPP server interface or both – with no loss of consistency within the SRS.

##### 2.1.2.1 SECURITY AND CONSISTENCY CONSIDERATIONS FOR SRS WEB INTERFACE

The SRS Web Interface contains measures to prevent abuse and to mitigate fraudulent operations. By restricting access, providing user level authentication and authorisation, and protecting the communications channel, the application limits both the opportunity and scope of security compromise.

Registrars are able to create individual users that are associated with their

Registrar account. By allocating the specific operations each user can access, Registrars have full control over how their individual staff members interact with the SRS. Users can be audited to identify which operations were conducted and to which objects those operations were applied.

A secure connection is required before credentials are exchanged and once authenticated. On login, any existing user sessions are invalidated and a new session is generated, thereby mitigating session-fixation attacks and reducing possibilities that sessions could be compromised.

All communication between the Registrar or the Registrars systems and the SRS is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57.

### 2.1.3 SECURING AND MAINTAINING CONSISTENCY OF REGISTRY-REGISTRAR INTERACTION SYSTEMS

ARI ensures all systems through which Registrars interact with the SRS remain consistent with each other and apply the same security rules. Additionally, ARI also ensures that operations on SRS objects are restricted to the appropriate entity. For example:

- \* In order to initiate a transfer a Registrar must provide the associated domain password (authinfo) which will only be known by the Registrant and the current sponsoring Registrar.

- \* Only sponsoring Registrars are permitted to update Registry objects. All operations conducted by Registrars on SRS objects are auditable and are identifiable to the specific Registrar's user account, IP address and the time of the operation.

### 2.2 DISSEMINATE STATUS INFORMATION OF TLD ZONE SERVERS TO REGISTRARS

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

Normal operations are those when:

- \* DNS servers respond within SLAs for DNS resolution.

- \* Changes in the SRS are reflected in the zone file according to the DNS update time SLA.

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

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

#### 2.2.1 COMMUNICATION POLICY

ARI maintains close communication with Registrars regarding the performance and consistency of the TLD zone servers.

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

Communication using the Registrar contact information discussed above will occur prior to any maintenance that has the potential to effect the access to, consistency of, or reliability of the TLD zone servers. If such maintenance is



required within a short time frame, immediate communication occurs using the above contact information. In either case, the nature of the maintenance and how it affects the consistency or accessibility of the TLD zone servers, and the estimated time for full restoration, are included within the communication.

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

#### 2.2.2 SECURITY AND STABILITY CONSIDERATIONS

ARI restricts zone server status communication to Registrars, thereby limiting the scope for malicious abuse of any maintenance window. Additionally, ARI ensures Registrars have effective operational procedures to deal with any status change of the TLD nameservers and will seek to align its communication policy to those procedures.

#### 2.3 ZONE FILE ACCESS PROVIDER INTEGRATION

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

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

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

#### 2.4 ZONE FILE UPDATE

To ensure changes within the SRS are reflected in the zone file rapidly and securely, ARI updates the zone file on the TLD zone servers using software compliant with RFC 2136 (Dynamic Updates in the Domain Name System (DNS UPDATE)) and RFC 2845 (Secret Key Transaction Authentication for DNS (TSIG)).

This updating process follows a staged but rapid propagation of zone update information from the SRS, outwards to the TLD zone servers - which are visible to the Internet. As changes to the SRS data occur, those changes are updated to isolated systems which act as the authoritative Primary server for the zone, but remain inaccessible to systems outside ARI's network. The primary servers notify the designated Secondary servers, which service queries for the TLD zone from the public. Upon notification, the secondary servers transfer the incremental changes to the zone and publicly present those changes.

The protocols for dynamic update are robust and mature, as is their implementation in DNS software. The protocols' mechanisms for ensuring consistency within and between updates are fully implemented in ARI's TLD zone update procedures. These mechanisms ensure updates are quickly propagated while the data remains consistent within each incremental update, regardless of the speed or order of individual update transactions. ARI has used this method for updating zone files in all its TLDs including the .au ccTLD, pioneering this method during its inception in 2002.

Mechanisms separate to RFC 2136-compliant transfer processes exist; to check and ensure domain information is consistent with the SRS on each TLD zone server within 10 minutes of a change.

## 2.5 OPERATION OF ZONE SERVERS

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

### 2.5.1 SECURITY AND OPERATIONAL CONSIDERATIONS OF ZONE SERVER OPERATIONS

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

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

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

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

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

## 2.6 DISSEMINATION OF CONTACT OR OTHER INFORMATION

Registries are required to provide a mechanism to identify the relevant contact information for a domain. The traditional method of delivering this is via the Whois service, a plain text protocol commonly accessible on TCP port 43. ARI also provides the same functionality to users via a web -based Whois service. Functionality remains the same with the web -based service, which only requires a user to have an Internet browser.

Using the Whois service, in either of its forms, allows a user to query for domain -related information. Users can query for domain details, contact details, nameserver details or Registrar details.

A Whois service, which complies with RFC 3912, is provided to disseminate contact and other information related to a domain within the TLD zone.

### 2.6.1 SECURITY AND STABILITY CONSIDERATIONS

ARI ensures the service is available and accurate for Internet users, while limiting the opportunity for its malicious use. Many reputation and anti-abuse services rely on the availability and accuracy of the Whois service, However the potential for abuse of the Whois service exists.

Therefore, certain restrictions are made to the access of Whois services, the nature of which depend on the delivery method - either web -based or the

traditional text -based port 43 service. In all cases, there has been careful consideration given to the benefits of Whois to the Internet community, as well as the potential harm to Registrants - as individuals and a group - with regard to Whois access restrictions.

The Whois service presents data from the Registry Database in real time. However this access is restricted to reading the appropriate data only. The Whois service does not have the ability to alter data or to access data not related to the Whois service. The access limitations placed on the Whois services prevent any deliberate or incidental denial of service that might impact other Registry Services.

Restrictions placed on accessing Whois services do not affect legitimate use. All restrictions are designed to target abusive volume users and to provide legitimate users with a fast and available service. ARI has the ability to 'whitelist' legitimate bulk users of Whois, to ensure they are not impacted by standard volume restrictions.

The data presentation format is consistent with the canonical representation of equivalent fields, as defined in the EPP specifications and ICANN agreement.

#### 2.6.1.1 PORT 43 WHOIS

A port 43 -based Whois service complying with RFC 3912 is provided and will be updated to meet any other relevant standards or best practice guidelines related to the operation of a Whois service.

While the text -based service can support thousands of simultaneous queries, it has dynamic limits on queries per IP address to restrict data mining efforts. In the event of identified malicious use of the service, access from a single IP address or address ranges can be limited or blocked.

#### 2.6.1.2 WEB -BASED WHOIS

ARI's web -based Whois service provides information consistent with that contained within the SRS.

The web -based Whois service contains an Image Verification Check (IVC) and query limits per IP address. These restrictions strike a balance between acceptable public usage and abusive use or data mining. The web -based Whois service can blacklist IP addresses or ranges to prevent abusive use of the service.

#### 2.6.1.3 SEARCHABLE WHOIS

ARI will provide a Web-based Searchable Whois Service for the identification of domain names having similar registration data. This service, deployed as a web-interface alongside the SRS Web Interface, is restricted to pre-authorized clients.

The service is made available to authorized third parties. ARI will perform relevant background checks on a user before providing them with access to the searchable whois. The user will be required to change their password on first successful login, and every 6 months thereafter. Clients that have not used the service in a 3-month period will have their access revoked. ARI will periodically review the information submitted by the client to ensure that contact and usage information is up to date.

Access is logged and monitored to protect against abuse of this service. All searches are logged with the client and timestamp of the request. IP address, port, and browser information is collected in the event that this information is required to assist in identifying the user. The use of HTTPS is enforced for the entire service to prevent exposure of the information from client-side or middle-box caches.

ARI will conduct periodic audits of query logs to identify usage patterns and

identify potential occurrences of data mining. Usage patterns will be matched back to the client's specified reason for use. The client may be suspended from use of the service if ARI believes that abuse is occurring.

Further details on this service are described in the answer to Question 262.7  
IDNs- Internationalised Domain Names

An Internationalised Domain Name (IDN) allows registrants to register domains in their native language and have it display correctly in IDN aware software. This includes allowing a language to be read in the manner that would be common for its readers. For example, an Arabic domain would be presented right to left for an Arabic IDN aware browser.

The inclusion of IDNs into the TLD zones is supported by ARI. All the Registry services, such as the EPP service, SRS Web Interface and RDPS (web and port 43), support IDNs. However there are some stability and security considerations related to IDNs which fall outside the general considerations applicable individually to those services.

#### 2.7.1 STABILITY CONSIDERATIONS SPECIFIC TO IDN

To avoid the intentional or accidental registration of visually similar chars, and to avoid identity confusion between domains, there are several restrictions on the registration of IDNs.

##### 2.7.1.1 PREVENT CROSS LANGUAGE REGISTRATIONS

Domains registered within a particular language are restricted to only the chars of that language. This avoids the use of visually similar chars within one language which mimic the appearance of a label within another language, regardless of whether that label is already within the DNS or not.

##### 2.7.1.2 INTER-LANGUAGE AND INTRA-LANGUAGE VARIANTS TO PREVENT SIMILAR REGISTRATIONS

ARI restricts child domains to a specific language and prevents registrations in one language being confused with a registration in another language, for example Cyrillic a (U+0430) and Latin a (U+0061).

#### 2.8 DNSSEC

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

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

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

Recommendation 26 calls for DNSSEC deployment at each zone and subsequent sub-zones at Registry, Registrar and Registrant level. Our compliance wrt the same is detailed in Q43.

## 2.8.1 STABILITY AND OPERATIONAL CONSIDERATIONS FOR DNSSEC

### 2.8.1.1 DNSSEC PRACTICE STATEMENT

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

### 2.8.1.2 RECEIPT OF PUBLIC KEYS FROM REGISTRARS

The public key for a child domain is received by ARI from the Registrar via either the EPP or SRS Web Interface. ARI uses an SHA-256 digest to generate the DS Resource Record (RR) for inclusion into the zone file.

### 2.8.1.3 RESOLUTION STABILITY

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

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

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

## 3. APPROACH TO SECURITY AND STABILITY

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

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

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

This completes our response to Q23.

## Demonstration of Technical & Operational Capability

## 24. Shared Registration System (SRS) Performance

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q24 - ARI Background & Roles.pdf'. This response describes the SRS as implemented by ARI.

### 1. INTRODUCTION

ARI has demonstrated delivery of an SRS with exceptional availability, performance and reliability. ARI's SRS has successfully supported a large group of Registrars for ASCII and IDN based TLDs. ARI's SRS meets the following requirements:

- \* Resilient to wide range of security & availability threats
- \* Consistently exceeds performance & availability SLAs
- \* Allows capacity increase with minimal impact to service
- \* Provides fair & equitable provisioning for all Registrars

### 2. CAPACITY

ARI's SRS infrastructure was built to sustain 20M domain names at less than 50% utilization. Based on ARI's experience and industry analysis, ARI were able to calculate the conservative characteristics of a registry of this size.

Through conservative statistical analysis of the .au registry and data presented in the May 2011 ICANN reports for the .com & .net, .org, .mobi, .info, .biz and .asia [<http://www.icann.org/en/resources/registries/reports>] we know there is:

- \* An average of 70 SRS TPS per domain, per month; and
- \* A ratio of 3 query to 2 transform txs

For a Registry with 20M domains this indicates an expected monthly transaction volume of 1,400M txs (840M query and 560M transforms).

Through conservative comparison of .au registry numbers and the .net RFP response - specifically <http://archive.icann.org/en/tlds/net-rfp/applications/sentan.htm> we also know:

- \* The peak daily txs is 6% of the monthly total (.au:6%, .net: 5%)
- \* The peak 5 min txs is 5% of the peak daily (.au and .net: 5%)

Hence for 20M domains we expect a peak EPP tx rate of 14,000 TPS (5,600 transform TPS and 8,400 query TPS)

Through conservative statistical analysis of the .au registry we additionally know:

- \* The avg no. of contacts/domain is 3.76 (overall not assigned)
- \* The avg no. of hosts/domain is 2.28 (overall not assigned)

This translates into a requirement to store 75.2M contacts and 45.6M hosts. Finally through real world observations of the .au registry, which has a comprehensive web interface when compared to those offered by current gTLD registries, we know that there is an avg of 0.5 HTTP requests/sec to the SRS web interface per registrar. We also know that this behaviour is reasonably flat. To support an estimated 1000 Registrars, would require into a HTTP request load of 500 requests/second.

For perspective on the conservativeness of this, the following was taken from data in the May 2011 ICANN reports referenced above:

- \* .info: ~7.8M. domain names peaks at ~1,400 TPS (projected peak TPS of ~3,600 with 20M)

\* .com: ~98M domain names peaks at ~41,000 TPS (projected peak TPS of ~8,300 TPS with 20M)

\* .org: ~9.3M domain names, peaks at ~1,400 TPS (projected peak TPS of ~3,100 with 20M)

After performing this analysis the projected TPS for .com was still the largest value seen. ARI's estimated value of 14,000 TPS for a registry with 20M Domains is roughly twice that of the .com projected peak of ~8300 TPS.

ARI benchmarked their SRS infrastructure and used the results to calculate the required computing resources for each of the tiers within the SRS architecture; allowing ARI to accurately estimate the required CPU, IOPS, storage and memory requirements for each server in the architecture, and the network bandwidth & and packet throughput requirements for the anticipated traffic. These capacity numbers were then doubled to account for unanticipated traffic spikes, errors in predictions, and headroom. Despite doubling numbers, effective estimated capacity is still reported as 20M. The technical resource allocations are explored in Q32.

ARI understand the limitations of these calculations but they serve as a best estimate of probable transaction load. Over and above this ARI has built significant overcapacity of resources and as the numbers themselves are more conservative than real world observations, we are confident these capacity numbers are sufficient.

.Web is projected to reach 471,482 domains at its peak volume and will generate 330 EPP TPS. This will consume 2.36% of the resources of the SRS infrastructure. As is evident ARI's SRS can easily accommodate this TLD's growth plans. See attachment 'Q24 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI expects to provide Registry services to 100 TLDs and a total of 12M domains by end of 2014. With all the TLDs and domains combined, ARI's SRS infrastructure will be only 60% utilized in 2014. The SRS infrastructure capacity can also be easily scaled as described in Q32

### 3. SRS ARCHITECTURE

ARI's SRS has the following major components:

- \* Network Infrastructure
- \* EPP Application Servers
- \* SRS Web Interface Application Servers
- \* SRS Database

Attachment 'Q24 - SRS.pdf' shows the SRS systems architecture and data flows. Detail on this architecture is in our response to Q32. ARI provides two distinct interfaces to the SRS: EPP and SRS Web. Registrar SRS traffic enters the ARI network via the redundant Internet link and passes (via the firewall) to the relevant application server for the requested service (EPP or SRS Web). ARI's EPP interface sustains high volume and throughput domain provisioning transactions for a large number of concurrent Registrar connections. ARI's SRS Web interface provides an alternative to EPP and provides features additional to those provided by the EPP interface.

#### 3.1 EPP

ARI's EPP application server is based on EPP as defined in RFCs 5730 - 5734. Registrars send XML based transactions to a load balanced EPP interface which forwards to one of the EPP application servers. The EPP application server then processes the XML and converts the request into database calls that retrieve or modify registry objects in the SRS database. The EPP application server tier comprises of 3 independent servers with dedicated connections to the Registry

database. Failure of any one of these servers will cause Registrar connections to automatically re-establish with one of the remaining servers. All EPP servers accept EPP both IPv4 & IPv6.

### 3.2 SRS WEB

The SRS Web application server is a Java web application. Registrars connect via the load balancer to a secure HTTPS listener running on the web servers. The SRS web application converts HTTPS requests into database calls which query or update objects in the SRS database. The SRS Web application server tier consists of 2 independent servers that connect to the database via JDBC. If one of these servers is unavailable the load balancer re-routes requests to the surviving server. These servers accept both IPv4 & IPv6.

### 3.3 SRS DATABASE

The SRS database provides persistent storage for domains and supporting objects. It offers a secure way of storing and retrieving objects provisioned within the SRS and is built on the Oracle 11g Enterprise Edition RDBMS. The SRS Database tier consists of four servers clustered using Oracle Real Application Clusters (RAC). In the event of failure of a database server, RAC will transparently transition its client connections to a surviving database host.

The SRS database is stored on a storage area network concurrently accessed by all of the database servers which supports N+N redundancy. The SAN consists of 2 switches, 20 control enclosures (each with dual controllers), and 2 expansion enclosures per control enclosure. Each database server host is configured with two 4-port Fibre Channel Host Bus Adaptors (HBAs). Each HBA has 2 SAN fabric connections, one to each SAN switch – providing a total of 4 fabric connections per database server.

Each SAN switch has dual redundant connections to each controller in each Control Enclosure. All disks under the control of a Control Enclosure are configured in a highly resilient RAID 10 array. The Storwize V7000 uses SAN mirroring technology to duplicate data across Control Enclosures. This SAN design provides protection against failure of any component within the Storage Area Network including complete loss of a Control Enclosure and associated expansion enclosures.

### 3.4 NUMBER OF SERVERS

**EPP Servers** - The EPP cluster consists of 3 EPP servers that can more than handle the anticipated 20M. .Web will utilize 2.36% of this at its peak volume. As the utilization increases ARI will add additional EPP servers ensuring the total utilization doesn't exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime and does not impact the infrastructure.

**SRS Web Servers** - The SRS Web cluster consists of 2 SRS Web servers that can more than handle the anticipated 20M. .Web will utilize 2.36% of this at its peak volume. As the utilization increases ARI will add additional SRS Web servers ensuring total utilization doesn't exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime and does not impact the infrastructure.

**SRS DB Servers** - The SRS DB cluster consists of 4 SRS DB servers that can more than handle the anticipated 20M. .Web will utilize 2.36% of this at its peak volume. As the utilization increases ARI will add additional SRS DB servers ensuring total utilization doesn't exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime and does not impact the infrastructure.

### 3.5 SRS SECURITY



ARI adopts a multi-layered security solution to protect the SRS. An industry leading firewall is deployed behind the edge router and is configured to only allow traffic on the minimum required ports and protocols. Access to the ARI EPP service is restricted to a list of known Registrar IPs.

An Intrusion Detection device is in-line with the firewall to monitor and detect suspicious activity.

All servers are configured with restrictive host based firewalls, intrusion detection, and SELinux. Direct root access to these servers is disabled and all access is audited and logged centrally.

The SRS database is secured by removal of non-essential features and accounts, and ensuring all remaining accounts have strong passwords. All database accounts are assigned the minimum privileges required to execute their business function.

All operating system, database, and network device accounts are subject to strict password management controls such as validity & complexity requirements.

Registrar access to the SRS via EPP or the Web interface is authenticated and secured with multi-factor authentication (NIST Level 3) and digital assertion as follows:

- \* Registrar's source IP address must be allowed by the front-end firewalls. This source IP address is received from the Registrar via a secure communication channel from within the SRS Web interface;
- \* Registrar must use a digital certificate provided by ARI;
- \* Registrar must use authentication credentials that are provided by to the Registrar via encrypted email.

All communication between the Registrar or the Registrars systems and the SRS is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57.

### 3.6 SRS HIGH AVAILABILITY

SRS availability is of paramount importance. Downtime is eliminated or minimised where possible. The infrastructure contains no single points of failure. N+1 redundancy is used as a minimum, which not only protects against unplanned downtime but also allows ARI to execute maintenance without impacting service.

Redundancy is provided in the network with hot standby devices & multiple links between devices. Failure of any networking component is transparent to Registrar connections.

N+N redundancy is provided in the EPP and SRS Web application server tiers by the deployment of multiple independent servers grouped together as part of a load -balancing scheme. If a server fails the load balancer routes requests to the remaining servers.

N+N redundancy is provided in the database tier by the use of Oracle Real Application Cluster technology. This delivers active/active clustering via shared storage. This insulates Registrars from database server failure.

Complete SRS site failure is mitigated by the maintenance of a remote standby site - a duplicate of the primary site ready to be the primary if required.

The standby site database is replicated using real time transaction replication from the main database using Oracle Data Guard physical standby. If required the Data Guard database can be activated quickly and service resumes at the standby site.

### 3.7 SRS SCALABILITY

ARI's SRS scales efficiently. At the application server level, additional computing resource can be brought on-line rapidly by deploying a new server online. During benchmarking this has shown near linear.

The database can be scaled horizontally by adding a new cluster node into the RAC cluster online. This can be achieved without disruption to connections. The SRS has demonstrated over 80% scaling at the database level, but due to the distributed locking nature of Oracle RAC, returns are expected to diminish as the number of servers approaches double digits. To combat this ARI ensures that when the cluster is 'scaled' more powerful server equipment is added rather than that equal to the current members. Capacity can be added to the SAN at any time without downtime increasing storage and IOPs.

Additional capacity can be added to the SAN at anytime without downtime. This would result in increasing storage and IOPs.

### 3.8 SRS INTER-OPERABILITY AND DATA SYNCHRONISATION

The SRS interfaces with a number of related Registry systems as part of normal operations.

#### 3.8.1 DNS UPDATE

Changes made in the SRS are propagated to the DNS via an ARI proprietary DNS Update process. This process runs on the 'hidden' primary master nameserver and waits on a queue. It is notified when the business logic inserts changes into the queue for processing. The DNS Update process reads these queue entries and converts them into DNS update (RFC2136) commands that are sent to the nameserver. The process of synchronizing changes to SRS data to the DNS occurs in real-time.

#### 3.8.2 WHOIS

The provisioned data supporting the SRS satisfies Whois queries. Thus the Whois and SRS share data sets and the Whois is instantaneously updated. Under normal operating conditions the Whois service is provided by the infrastructure at the secondary site in order to segregate the load and protect SRS from Whois demand (and vice versa). Whois queries that hit the standby site will query data stored in the standby database – maintained in near real-time using Oracle Active Data Guard. If complete site failure occurs Whois and SRS can temporarily share the same operations centre at the same site (capacity numbers are calculated for this).

#### 3.8.3 ESCROW

A daily Escrow extract process executes on the database server via a dedicated database account with restricted read-only access. The results are then transferred to the local Escrow Communications server by SSH.

## 4. OPERATIONAL PLAN

ARI follow defined policies/procedures that have developed over time by running critical Registry systems. Some principals captured by these are:

- \* Conduct all changes & upgrades under strict and well-practised change control procedures
- \* test, test and test again
- \* Maintain Staging environments as close as possible to production infrastructure/configuration
- \* Eliminate all single points of failure
- \* Conduct regular security reviews & audits
- \* Maintain team knowledge & experience via skills transfer/training

- \* Replace hardware when no longer supported by vendor
- \* Maintain spare hardware for all critical components
- \* Execute regular restore tests of all backups
- \* Conduct regular capacity planning exercises
- \* Monitor everything from multiple places but ensure monitoring is not 'chatty'
- \* Employ best of breed hardware & software products & frameworks (such as ITIL, ISO27001 and Prince2)
- \* Maintain two distinct OT&E environments to support pre\*production testing for Registrars

## 5. DESCRIPTION OF SLA, RELIABILITY & COMPLIANCE

ARI's SRS adheres to and goes beyond the scope of Specification 6 and Specification 10 of the Registry Agreement

ARI's EPP service is XML compliant and XML Namespace aware. It complies with the EPP protocol defined in RFC5730, and the object mappings for domain, hosts & contacts are compliant with RFC 5731, 5732 & 5733 respectively. The transport over TCP is compliant with RFC5734. The service also complies with official extensions to support DNSSEC, RFC5910, & Redemption Grace Period, RFC 3915. ARI's SRS is sized to sustain a peak transaction rate of 14,000 TPS while meeting strict internal Service Level Agreements (SLAs). The monthly -based SLAs below are more stringent than those in Specification 10 (Section 2).

EPP Service Availability: 100%

EPP Session Command Round Trip Time (RTT): <=1000ms for 95% of commands

EPP Query Command Round Trip Time (RTT): <=500ms for 95% of commands

EPP Transform Command Round Trip Time (RTT): <=1000ms for 95% of commands

SRS Web Interface Service Availability: 99.9%

ARI measures the elapsed time of every query, transform and session EPP transaction, and calculate the percentage of commands that fall within SLA on a periodic basis. If percentage value falls below configured thresholds on-call personnel are alerted.

SRS availability is measured by ARI's monitoring system which polls both the EPP and SRS Web services status. These checks are implemented as full end to end monitoring scripts that mimic user interaction, providing a true representation of availability. These 'scripts' are executed from external locations on the Internet.

## 6. RESOURCES

This function will be performed by ARI. ARI staff are industry leading experts in domain name registries with the experience and knowledge to deliver outstanding SRS performance.

The SRS is designed, built, operated and supported by the following ARI departments:

- \* Products and Consulting team (7 staff)
- \* Production Support Group (27 staff)
- \* Development Team (11 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q24 - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

ARI provides registry backend services to 5 TLDs and has a vast wealth of experience in estimating the number of resources required to support a Registry System.

Based on past experience ARI estimates that the existing staff is adequate to support a Registry System that is supporting at least 50M domains. Since .Web projects 471,482 domains, 0.94% of these resources are allocated to this TLD. See attachment 'Q24 - Registry Scale Estimates & Resource Allocation.xlsx' for

more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

## 7. FINANCIAL COSTS

The usage of the ARI's staff and Registry Systems is included in our contract with ARI attached to Q46. This cost is shown in the financial answers.

This completes our response to Q24.

## 25. Extensible Provisioning Protocol (EPP)

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q25 - ARI Background & Roles.pdf'. This response describes the Extensible Provisioning Protocol (EPP) interface as implemented by ARI.

### 1. INTRODUCTION

ARI's EPP service is XML compliant and XML Namespace aware. The service complies with the EPP protocol defined in RFC5730, and the object mappings for domain, hosts and contacts are compliant with RFC5731-3 respectively. The transport over TCP is implemented in compliance with RFC5734. The service also complies with the official extensions to support DNSSEC, RFC5910 and Redemption Grace Period, RFC3915. ARI implemented EPP draft version 0.6 in 2002, then migrated to EPP RFC 1.0 on its publishing in 2004. The system has operated live since 2002 in the .au ccTLD.

Descriptions in this response follow the terminology used in the EPP RFCs. when referring to the software involved in the process, ARI's EPP interface is called the server, and the software used by Registrars is called the client.

### 2. TRANSPORT LAYER

The ARI EPP service implements the RFC5734 - EPP Transport over TCP. Connections are allowed using TLSv1 encryption, optionally supporting SSLv2 Hello for compatibility with legacy clients. AES cipher suites for TLS as described in RFC3268 are the only ones allowed.

#### 2.1 AUTHENTICATION

Registrar access to the EPP interface is authenticated and secured with multi-factor authentication (NIST Level 3) and digital assertion as follows. Registrars must:

- \* Present a certificate, during TLS negotiation, signed by the ARI Certificate Authority (CA). The server returns a certificate also signed by the ARI CA. Not presenting a valid certificate results in session termination. ARI requires that the Common Name in the subject field of the certificate identifies the Registrar.

- \* Originate connections from an IP address that is known to be assigned to the Registrar with that Common Name.

- \*\* Registrar must use authentication credentials provided to the Registrar via encrypted email

\* Registrars aren't able to exceed a fixed number of concurrent connections. The connection limit is prearranged and designed to prevent abuse of Registrars' systems from affecting the Registry. The limit is set to reasonable levels for each Registrar, but can be increased to ensure legitimate traffic is unaffected. If any of the above conditions aren't met the connection is terminated.

All communication between the Registrars and the EPP service is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57.

## 2.2 CONNECTION CLOSE

The server may close the connection as a result of a logout, an error where the state of the connection is indeterminate, or after a timeout. Timeout occurs where no complete EPP message is received on the connection for 10 minutes.

## 3. EPP PROTOCOL

This section describes the interface relating to the EPP protocol described in RFC5730. This includes session management, poll message functionality and Object mappings for domains, hosts and contacts.

### 3.1 SESSION MANAGEMENT

Session management refers to login and logout commands, used to authenticate and end a session with the SRS. The Login command is used to establish a session between the client and the server. This command succeeds when:

- The username supplied matches the Common Name in the digital certificate used in establishing the TLS session.
- The provided password is valid for the user.
- The user's access to the system isn't suspended.

The Logout command is used to end an active session. On processing a logout the server closes the underlying connection. The Hello command can be used as a session keep-alive mechanism.

### 3.2 SERVICE MESSAGES

Offline notifications pertaining to certain events are stored in a queue. The client is responsible for polling this queue for new messages and to acknowledge read messages. Messages include notification about server modification of sponsored objects, transfer operations, and balance thresholds.

## 4. EPP OBJECT MAPPINGS

This section covers the interface for the 3 core EPP objects; domain, host and contact objects, as per RFC5731, 5732, & 5733 respectively.

The EPP domain, contact and host object mapping describes an interface for the check, info, create, delete, renew (domain only), transfer (domain & contact only) and update commands. For domain objects The server doesn't support the use of host attributes as described by RFC5731, but rather uses host objects as described by RFC5731 and RFC5732. Details of each command are:.

\* Check command: checks availability of 1 or more domain, contact or host objects in the SRS. Domain names will be shown as unavailable if in use, invalid or reserved, other objects will be unavailable if in use or invalid.

\* info command: retrieves the information of an object provisioned in the SRS. Full information is returned to the sponsoring client or any client that provides authorisation information for the object. Non-sponsoring clients are returned partial information (no more than is available in the WhoIs).

- \* Create command: provisions objects in the SRS. To ascertain whether an object is available for provisioning, the same rules for the check command apply.
- \* Delete command: begins the process of removing an object from the SRS. Domain names transition into the redemption period and any applicable grace periods are applied. domain names within the Add Grace Period are purged immediately. All other objects are purged immediately if they are not linked.
- \* Renew command (domain only): extends the registration period of a domain name. The renewal period must be between 1 to 10 years inclusive and the current remaining registration period, plus the amount requested in the renewal mustn't exceed 10 years.
- \* Transfer command (domain and contact only): provides several operations for the management of the transfer of object sponsorship between clients. clients that provide correct authorisation information for the object can request transfers. Domain names may be rejected from transfer within 60 days of creation or last transfer. The requesting client may cancel the transfer, or the sponsoring client may reject or approve the transfer. Both the gaining and losing clients may query the status of the current pending or last completed transfer.
- \* Update command: updates authorisation information, delegation information (domains), and registration data pertaining to an object.

## 5. NON-PROPRIETARY EPP MAPPINGS

ARI's EPP service implements 2 non-proprietary EPP mappings, to support the required domain name lifecycle and to provide & manage DNSSEC information. The relevant schema documents aren't provided as they are published as RFCs in the RFC repository.

### 5.1 GRACE PERIOD MAPPING

The Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (as per RFC 3915) is used to support the domain name lifecycle as per existing TLDs. The update command is extended by the restore command to facilitate the restoration of previously deleted domains in the redemption period. This command defines 2 operations, request & report, described here:

- \* Request operation: requests the restoration of a domain.
- \* Report operation: completes the restoration by specifying the information supporting the restoration of the domain. The restore report must include a copy of the Whois information at both the time the domain was deleted & restored, including the restore reason.

### 5.2 DNSSEC MAPPING

The Domain Name System (DNS) Security Extensions Mapping for EPP, as per RFC5910, is used to support the provisioning of DNS Security Extensions. ARI requires clients use the Key Data Interface. Clients may associate a maximum of 4 keys per domain. The Registry system generates the corresponding DS data using the SHA-256 digest algorithm for the domain and any active variant domains.

ARI is aware of issues DNSSEC causes when transferring DNS providers - a transfer of Registrar usually means a change in DNS provider. DNSSEC key data won't be removed from the SRS or the DNS if a transfer occurs. It is the responsibility of and requires the cooperation of the Registrant, Registrars, and DNS providers, to provide a seamless transition. ARI observes progress with this issue and implements industry agreed solutions as available. DNSSEC information is included in info responses when the secDNS namespace in login.

## 6. PROPRIETARY MAPPING

The Registry system supports 3 additional EPP extensions where no published standard for the required functionality exists. Developed to conform to the requirements specified in RFC3735, these extensions include the provisioning of Internationalised Domain Names and domain name variants, and the association of arbitrary data with a domain name. These 3 extensions are introduced below, and further described in the attached schema documentation.

### 6.1 INTERNATIONALISED DOMAIN NAMES

ARI has developed an extension to facilitate the registration and management of Internationalised Domain Names as per RFCs 5890-5893 (collectively known as the IDNA 2008 protocol). This extension extends the domain create command and the info response.

The create command is extended to capture the language table identifier that identifies the corresponding IDN language table for the domain name. Additionally the extension requires the Unicode form to avoid an inconsistency with DNS-form, as per RFC 5891.

The domain info command is extended to identify the language tag and Unicode form provided in the initial create command. This information is disclosed to all querying clients that provided the extension namespace at login. This extension is documented in the attachment 'Q25 - idnadomain-1.0.pdf'.

### 6.2 VARIANT

ARI has developed an extension to facilitate the management of Domain Name variants. This extension extends the domain update command and the domain create and info responses. The domain update command is extended to allow the addition (activation) and removal (de-activation) of domain name variants subject to registry operator policy.

The domain create and info responses are extended to return the list of activated domain name variants. This information is disclosed to all querying clients that provided the extension namespace at login. The extension is documented in the attachment 'Q25 - variant-1.1.pdf'.

### 6.3 KEY-VALUE

ARI has developed an extension to facilitate the transport of arbitrary data between clients and the SRS without the need for developing EPP Extensions for each specific use-case. This extension extends the domain create and domain update transform commands and the domain info query command. This extension is documented in the attachment 'Q25 - kv-1.0.pdf'.

## 7. ADDITIONAL SECURITY

The Registry system provides additional mechanisms to support a robust interface. The use of command rate limiting enables the Registry to respond to and withstand erroneous volumes of commands, while a user permission model provides fine-grained access to the EPP interface. These 2 mechanisms are described below.

### 7.1 RATE LIMITING

The Registry system supports command and global rate limits using a token-bucket algorithm. Limits apply to each connection to ensure fair and equitable use by all. Clients that exceed limits receive a command failed response message indicating breach of the limit.

### 7.2 USER PERMISSION MODEL

The Registry system supports a fine-grained permission model controlling access

to each specific command. By default, clients receive access to all functionality; however it is possible to remove access to a specific command in response to abuse or threat to stability of the system. Clients that attempt a command they have lost permission to execute, receive an EPP command failed response indicating loss of authorisation.

## 8. COMPLIANCE

Compliance with EPP RFCs is achieved through design and quality assurance (QA). The EPP interface was designed to validate all incoming messages against the respective XML Schema syntax. The XML Schema is copied directly from the relevant RFCs to avoid any ambiguity on version used. Inbound messages that are either malformed XML or invalid are rejected with a 2400 response. Outbound messages are validated against the XML Schema, and if an invalid response is generated, it is replaced with a known valid pre-composed 2400 response, and logged for later debugging.

A QA process provides confidence that changes don't result in regressions in the interface. Automated build processes execute test suites that ensure every facet of the EPP service (including malformed input, commands sequencing and synchronisation, and boundary values) is covered and compliant with RFCs and the EPP service specification. These tests are executed prior to committing code and automatically nightly. The final deliverable is packaged and tested again to ensure no defects were introduced in the packaging process.

New versions of the EPP Service follow a deployment schedule. The new version is deployed into an OT&E environment for Registrar integration testing. Registrars are encouraged during this stage to test their systems operate correctly. After a fixed time in OT&E without issue, new versions are scheduled for production deployment. This ensures incompatibilities with RFCs that made it through QA processes are detected in test environments prior reaching production.

ARI surveys Registrars for information about the EPP client toolkit. These surveys indicated that while many Registrars use ARI toolkits, several Registrars use either their own or that from another registry. The ability for Registrars to integrate with the ARI EPP service without using the supplied toolkit indicates the service is compliant with RFCs.

ARI is committed to providing an EPP service that integrates with third party toolkits and as such tests are conducted using said toolkits. Any issues identified during testing fall into the following categories:

- \* Third-party toolkit not compliant with EPP
- \* EPP service not compliant with EPP
- \* Both third-party toolkit and EPP service are compliant, however another operational issue causes an issue

Defects are raised and change management processes are followed. Change requests may also be raised to promote integration of third-party toolkits and to meet common practice.

## 9. CAPACITY

.Web is projected to reach 471,482 domains at its peak volume and will generate 330 EPP TPS. This will consume 2.36% of the EPP resources of the SRS infrastructure. ARI's SRS can easily accommodate this. These numbers were described in considerable detail in the capacity section of Q24.

## 10. RESOURCES

This function will be performed by ARI. ARI provides a technical support team to support Registrars and also provides Registrars with a tool kit (in Java and C++) implementing the EPP protocol. Normal operations for all Registry Services



are managed by ARI's Production Support Group (PSG), who ensure the EPP server is available and performing appropriately.

Faults relating to connections with or functionality of the EPP server are managed by PSG. ARI monitors EPP availability and functionality as part of its monitoring practices, and ensures PSG staff are available to receive fault reports from Registrars any time. PSG has the appropriate network, Unix and application (EPP and load balancing) knowledge to ensure the EPP service remains accessible and performs as required. these ARI departments support EPP:

- \* Products and Consulting Team (7 staff)
- \* Production Support Group (27 staff)
- \* Development Team (11 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q25 - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

ARI provides registry backend services to 5 TLDs and has a vast wealth of experience in estimating the number of resources required to support a Registry System.

Based on past experience ARI estimates that the existing staff is adequate to support a Registry System that is supporting at least 50M domains. Since .Web projects 471,482 domains, 0.94% of these resources are allocated to this TLD. See attachment 'Q25 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

## 11. FINANCIAL COSTS

The usage of the ARI's staff and Registry Systems is included in our contract with ARI attached to Q46. This cost is shown in the financial answers.

This completes our response to Q25.

## 26. Whois

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. For more background information on ARI please see the attachment 'Q26 - ARI Background & Roles.pdf'. This response describes the Whois interface as implemented by ARI.

### 1. INTRODUCTION

ARI's Whois service is for all domain names, contacts, nameservers and Registrars provisioned in the Registry database. This response describes the port 43, web and searchable whois interfaces, security controls to mitigate abuse, compliance with bulk access requirements for registration data, and the architecture delivering the service.

### 2. PORT 43 WHOIS SERVICE

Whois is available on TCP port 43 in accordance with RFC3912. Requests are made in semi-free text format and terminated by an ASCII CR & LF. The server

responds with a semi-free text format, terminating the response by closing the connection.

To support Internationalised Domain Names and Localised Registration Data we assume the query is encoded in UTF-8 and sends responses encoded in UTF-8. UTF-8 is backwards compatible with the ASCII charset and its use is consistent with the IETF policy on charsets as defined in BCP 18 [<http://tools.ietf.org/html/bcp18>].

## 2.1 Query Format

By default Whois searches for domains. To facilitate the queries of other objects a keyword must be included before the search string. Supported keywords are:

- \* Domain
- \* Host/Nameserver
- \* Contact
- \* Registrar

Keywords are case-insensitive. The remainder of the input is the search string. Wildcard chars may be used in search strings to match zero or more chars (%), or match exactly one char. Wildcard chars must not appear in the first 5 chars.

## 2.2. RESPONSE FORMAT

The response consists -

- \* An object-specific response represented by multiple key/value pairs. Where no object could be found the response is 'No Data Found'
- \* query-related meta-information to identify data freshness
- \* legal disclaimer

This format is consistent with that prescribed in the Registry agreement.

## 2.3, DOMAIN DATA

Domain data is returned in response to a query with the keyword omitted, or with the 'domain' keyword. Domain queries return information on domains that are provisioned in the Registry database.

The IDN domains may be specified in either the ASCII-compatible encoded form or the Unicode form. Clients are expected to perform any mappings, in conformance with relevant guidelines such as those specified in RFC5894 and UTS46.

Variant domains may be specified in the search string and Whois will match (using case-insensitive comparison) and return information for the primary registered domain.

For queries containing wildcard chars, If only one domain name is matched its details are returned, If more than one domain name is matched then the first 50 matched domain names are listed.

### 2.3.1. INTERNATIONALISED DOMAIN NAMES

The Whois response format, prescribed in Specification 4, does not provide a mechanism to identify active variant domain names. ARI will include active variant domain names in Whois responses until a common approach for handling and display of variant names is determined.

### 2.3.2. RESERVED DOMAIN NAMES

Domain names reserved from allocation will have a specific response that indicates the domain is not registered but also not available.

## 2.4. NAMESERVER DATA

Nameserver data is returned in response to a query where the 'nameserver' or 'host' keywords have been used. Nameserver queries return information on hosts that are provisioned in the Registry.

The search string for a nameserver query can be either a hostname or IP. Queries using the hostname produce one result unless wildcards are used.

Queries using the IP produce one or more results depending on the number of hostnames that match that address. Queries for the hostname are matched case-insensitively.

The quad-dotted notation is expected for IPv4 and the RFC3513 - IPv6 Addressing Architecture format for IPv6. Wildcards cannot be used for IP queries.

## 2.5. CONTACT DATA

Contact data is returned in response to a query where the 'contact' keyword was used. Contact queries return information on contacts that are provisioned in the Registry.

The search string for a contact query is the contact identifier. Contact identifiers are matched using a case-insensitive comparison. Wildcards cannot be used.

## 2.6. REGISTRAR DATA

Registrar data is returned in response to a query where the 'Registrar' keyword was used. Registrar queries return information on Registrar objects that are provisioned in the Registry.

The search string for a Registrar query can be name or IANA id. Queries using the name or the IANA id produce only one result. Queries for the name are matched using a case-insensitive comparison. Wildcards cannot be used.

## 2.7. NON-STANDARD DATA

The SRS supports domain-related data beyond that above. It may include information used to claim eligibility to participate in the sunrise process, or other arbitrary data collected using the Key-Value Mapping to the EPP. This information will be included in the Whois response after the last object-specific data field and before the meta-information.

## 3. WEB-BASED WHOIS SERVICE

Whois is also available via port 80 using HTTP, known as Web-based Whois. This interface provides identical query capabilities to the port 43 interface via an HTML form.

## 4. SECURITY CONTROLS

Whois has an in-built mechanism to blacklist malicious users for a specified duration. Blacklisted users are blocked by source IP address and receive a specific blacklisted notification instead of the normal Whois response. Users may be blacklisted if ARI's monitoring system determines excessive use. A whitelist is used to facilitate legitimate use by law enforcement agencies and other reputable entities.

## 5. BULK ACCESS

The Registry system complies with the requirements for the Periodic Access to Thin Registration Data and Exceptional Access to Thick Registration Data as described in Specification 4.

### 5.1. PERIODIC ACCESS TO THIN REGISTRATION DATA

ARI shall provide ICANN with Periodic Access to Thin Registration Data. The data will contain the elements as specified by ICANN. The format of the data will be consistent with the format specified for Data Escrow. The Escrow Format prescribes an XML document encoded in UTF-8. The generated data will be verified to ensure that it is well formed and valid.

The data will be generated every Monday for transactions committed up to and on Sunday unless otherwise directed by ICANN. The generated file will be made available to ICANN using SFTP. Credentials, encryption material, and other parameters will be negotiated between ARI and ICANN using an out-of-band

mechanism.

## 5.2 Exceptional Access to Thick Registration Data

If requested by ICANN, ARI shall provide exceptional access to thick registration data for a specified Registrar. The data will contain full information for the following objects:

- \* Domain names sponsored by the Registrar
  - \* Hosts sponsored by the Registrar
  - \* Contacts sponsored by the Registrar
  - \* Contacts linked from domain names sponsored by the Registrar
- As above The format of the data will be consistent with the format specified for Data Escrow. And will be made available to ICANN using SFTP.

## 6. CAPACITY

ARI's Whois infrastructure is built to sustain 20M domain names at less than 50% utilization. Based on ARI's experience running a high volume ccTLD registry (.au) and industry analysis, ARI were able to calculate the conservative characteristics of a registry of this size.

Through conservative statistical analysis of the .au registry and data presented in the May 2011 ICANN reports for the .com & .net, .org, .mobi, .info, .biz and .asia [<http://www.icann.org/en/resources/registries/reports> we know there is:

- \* An average of 30 Whois txs per domain, per month.

Which indicates an expected monthly transaction volume of 600M txs For a registry with 20M DUMs

Through conservative comparison of .au registry numbers and the .net RFP response - specifically <http://archive.icann.org/en/tlds/net-rfp/applications/sentan.htm> we also know:

- \* The peak daily transactions is 6% of the monthly total (.au:6%, .net: 5%)
- \* The peak 5 min is 5% of the peak day (.au:5%, .net: 0.6%)

Thus we expect a peak WhoIs tx rate of 6,000 TPS.

For perspective on the conservativeness of this, the following numbers were taken from data in the May 2011 ICANN reports referenced above:

- \* .info ~7.8M domain names, peaks at ~1,300 TPS (projected peak TPS of ~3,400 with 20M names).
- \* .mobi ~1M domain names, peaks at ~150 TPS (projected peak TPS of ~3,000 TPS with 20M names).
- \* .org ~9.3M domain names, peaks at ~1,300 TPS (projected peak TPS of ~2,800 with 20M names).

After performing this analysis the projected TPS for .info was still the largest value seen. ARI's estimated value of 6,000 TPS for a registry with 20M Domains is roughly twice that of the .info projected peak of ~3400 TPS.

ARI benchmarked their WhoIs infrastructure and used the results to calculate the required computing resources for each of the tiers within the WhoIs architecture - allowing ARI to accurately estimate the required CPU, IOPS, storage and memory requirements for each server within the architecture, as well as the network bandwidth and packet throughput requirements for the anticipated traffic. These capacity numbers were then doubled to account for unanticipated traffic spikes, errors in predictions and head room for growth. Despite doubling numbers, effective estimated capacity is still reported as 20 million domain names. The technical resource allocations are explored in

question 32.

ARI understand the limitations of these calculations but they serve as a best estimate of probable transaction load. Over and above this ARI has built significant overcapacity of resources and as the numbers themselves are more conservative than real world observations, we are confident these capacity numbers are sufficient.

.Web is projected to reach 471,482 domains at its peak volume and will generate 141 WhoIs transactions per second. This will consume 2.36% of the resources of the WhoIs infrastructure. As is evident ARI's WhoIs can easily accommodate this TLD's growth plans. See attachment 'Q26 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI expects to provide Registry services to 100 TLDs and a total of 12M domains by end of 2014. With all the TLDs and domains combined, ARI's WhoIs infrastructure will be only 60% utilized. The WhoIs infrastructure capacity can also be easily scaled as described in question 32

## 7. ARCHITECTURE

Whois uses a separate replica database independent of the SRS database. Oracle Data Guard ensures the two databases are synchronised in real-time. The Whois service is operated live from the SRS 'failover' site, with the SRS 'primary' site serving as the 'failover' site for the Whois service. Both sites have enough capacity to run both services simultaneously. The architecture and data flow diagrams are described below and shown in the attachment 'Q26 - WhoIs.pdf'

Traffic enters the network from the Internet through border routers and then firewalls. All traffic destined for this service except for TCP ports 43, 80 & 443 is blocked. Load balancers forward the request to one of the application servers running ARI built Whois software. Each server is connected to the database cluster through another firewall further restricting access to the. Each server uses a restricted Oracle user that has read only access to the Registry data and can only access the data that is relevant to the Whois queries. This ensures that in the unlikely event of an application server compromise the effects are limited.

All components are configured and provisioned to provide N+1 redundancy. Multiple Internet providers with separate upstream bandwidth suppliers are used. At least one additional component of all hardware exists, enabling maintenance without downtime. This configuration provides a service exceeding the availability requirements in Specification 10.

The use of load balancing allows addition of application servers with no downtime. From a database perspective, the ability to scale is enabled by utilising Oracle RAC database clustering.

The entire service, including routers, firewalls and application layer is IPv6 compatible and Whois is offered on both IPv4 and IPv6 interfaces. Detail about this architecture is available in our response to Question 32.

### 7.1. SYNCHRONIZATION

The Whois database is synchronised with the SRS database using Oracle Data Guard. Committed transactions in the SRS database are reflected in the Whois database in real-time. Should synchronisation break, Whois continues to operate with the latest available data until the issue is reconciled. The channel between the two sites consists of two independent dedicated point to point links as well as the Internet. Replication traffic flows via the dedicated links or if both links fail replication traffic flows over Internet tunnels.

### 7.2. INTERCONNECTIVITY WITH OTHER SERVICES

The WhoIs service is not directly interconnected with other registry services or systems. The software has been developed to provide the WhoIs service

exclusively and retrieve response information from a database physically separate to the SRS transactional database. This database is updated as described in 'Synchronisation' above. The WhoIs servers log every request to a shared central repository that is logically separate from the WhoIs database. This repository is used for query counts, detection of data mining and statistical analysis on query trends.

### 7.3. IT AND INFRASTRUCTURE RESOURCES

The WhoIs service is provided utilizing Cisco networking equipment, IBM application servers &, IBM database servers and SAN. They are described in the attachment 'Q26 - WhoIs.pdf'. For more information on the IT infrastructure including server specifications and database capabilities please see Q32 & Q33.

## 8. COMPLIANCE

Compliance with WhoIs RFCs is achieved through design and QA.

QA processes provide confidence that any changes to the service don't result in regression issues. Automated build processes execute test suites, prior to the committing of code and nightly, that ensure every facet of the WhoIs service is covered and compliant with RFCs. The final deliverable is packaged and tested again.

New versions follow a deployment schedule. The new version is deployed into an OT&E environment for registrar integration testing. After a fixed time in OT&E without issue, they are scheduled for production deployment. This ensures incompatibilities with RFCs that made it through QA processes are detected in test environments.

ARI is committed to providing a WhoIs service that integrates with third party tools without issue and as such tests are conducted using third party tools such as jWhoIs, a popular UNIX command line WhoIs client.

Defects are raised and follow the change management process for all issues where the WhoIs service has been determined to not comply with the RFCs.

## 9. SEARCHABLE WHOIS

ARI will provide a Web-based Searchable Whois Service restricted to pre-authorized clients.

### 9.1. DESCRIPTION OF SERVICE

The service provides search capabilities defined in Specification 4 and allows for:

- \* Exact-match on the registrar id, name server name, and name server's IP address;
- \* Partial-match on domain name, contacts, address (street, city, state or province, postcode, country); and
- \* Boolean search capabilities.

Matches for contact name and all postal address fields are case-insensitive. The client is restricted to one concurrent search to prevent unnecessary load on the system. The results include a list of domain names that match the criteria. The service allows for addition or removal of search criterion to meet local laws.

### 9.2. AUTHORISATION OF CLIENTS

Potential clients will request access to this service by providing the following on fax:

- \* Name
- \* Organisation
- \* Position
- \* Contact information
- \* Reason

- \* Query volume
- \* IP address

Access will be approved after background checks. Access is logged and monitored to protect against abuse. The use of HTTPS is enforced for the entire service.

Periodic audits of query logs will be used to identify any occurrences of data mining to suspend abusive clients.

## 10. RESOURCES

This function will be performed by the following ARI departments:

- \* Products and Consulting team (7 staff)
  - \* Production Support Group (27 staff)
  - \* Development Team (11 staff)
  - \* Legal, Abuse and Compliance Team (6 staff)
- and the following departments outsourced to the Directi Group:
- \* Abuse and Compliance Team (20 staff)

The products and consulting team is responsible for product management of the Whois solution including working with clients and the industry to identify new features or changes required to the system.

ARI employ a development team responsible for the maintenance and continual improvement of the Whois software

ARI's Production Support Team ensures the successful operation of the Whois system. The team comprises Database Administrators, Systems Administrators and Network Administrators. This team routinely checks and monitors bandwidth, disk and CPU usages to plan and respond to expected increases in the volume of queries, and perform maintenance of the system including security patches and failover and recovery testing.

The Directi Group and ARI Abuse and compliance teams provide abuse monitoring detection mechanisms to block data mining. Additionally the support team in conjunction with both the Compliance teams administer requests for listing on the Whitelist, as well as requests for access to the searchable whois

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q26 - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within. A detailed list of the Abuse and Compliance desk of Directi is provided in Q28.

ARI provides registry backend services to 5 TLDs and has a vast wealth of experience in estimating the number of resources required to support a Registry System.

Based on past experience ARI estimates that the existing staff is adequate to support a Registry System that is supporting at least 50M domains. Since .Web projects 471,482 domains, 0.94% of these resources are allocated to this TLD. See attachment 'Q26 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

The Directi Group is protected against loss of staff due to its scale of operations. This is described in further detail in Q39

## 11. FINANCIAL COSTS

The usage of the ARI's staff and Registry Systems is included in our contract with ARI attached to Q46. This cost is shown in the financial answers.

The usage of Directi Group's staff is included in our contract with Directi attached to Q46. This cost is shown in the financial answers.

This completes our response to Q26.

## 27. Registration Life Cycle

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. For more background please see attachment 'Q27 - ARI Background & Roles.pdf'. This response describes the Registration Lifecycle as implemented by ARI.

### 1. INTRODUCTION

The lifecycle described matches current gTLD registries. All states, grace periods and transitions are supported by the EPP protocol as described in RFC5730 - 5734 & the Grace Period Mapping published in RFC3915. An overview is in attachment 'Q27 - Registration Lifecycle.pdf'.

### 2. REGISTRATION PERIODS

The Registry supports registration up to 10 years and renewals for 1 to 10 years. Transfers extend registration by 1 year. The total validity period can't exceed 10 years.

### 3. STATES

The states that a domain can exist in are: Registered, Pending Transfer, Redemption, Pending Restore & Pending Delete.

All domain name statuses (RFC 3915, 5730-5734 and 5910) are covered below

#### 3.1 REGISTERED

EPP Status: ok

In DNS: Yes

Allowed Operations: Update, Renew, Transfer (request) & Delete

The default state of a domain - No pending operations. The Sponsoring Registrar may update the domain.

#### 3.2 PENDING TRANSFER

EPP Status: pendingTransfer

In DNS: Yes

Allowed Operations: Transfer (cancel, reject, approve)

another Registrar has requested transfer of the domain and it is not yet completed all transform operations, other than those to cancel, reject, or approve the transfer are rejected.

#### 3.3 REDEMPTION

EPP Status: pendingDelete

RGP Status: redemptionPeriod

In DNS: No

Allowed Operations: Restore (request)

Domain has been deleted. The sponsor may request restoration of the domain. The domain continues to be withheld from the DNS unless restored. No transform



operations other than restore allowed.

### 3.4 PENDING RESTORE

EPP Status:pendingDelete  
RGP Status:pendingRestore  
In DNS:No

Allowed Operations:Restore (report)

a restore request is pending. Sponsor must submit a restore report. The domain remains withheld from the DNS. No transform operations other than restore report allowed.

### 3.5 PENDING DELETE

EPP Status:pendingDelete  
RGP Status:pendingDelete  
In DNS:No

Allowed Operations:None

the Redemption Grace Period has lapsed and the domain is pending purge from the Registry. This state prohibits the sponsor from updating, restoring or modifying the domain for 5 days. At the end of this period the domain is purged and made available for registration.

## 4. GRACE PERIODS

The Registry system supports 4 grace periods: add, renew, auto-renew, and transfer, described below with consideration for overlap of grace periods. States described here are additional to those above.

### 4.1 ADD GRACE PERIOD

Length:5 days

RGP Status:addPeriod

Allows for the no-cost cancellation of a domain to rectify errors within 5 days from registration. The following rules apply for operations during this period:

- \* Delete: Sponsoring Registrar may delete the domain with immediate effect and receive a refund subject to the Add Grace Period Limits consensus policy.
- \* Renew: sponsor may renew the domain and is charged for the operation. The total period is extended by the renewal term, limited to 10 yr maximum.
- \* Transfer: The Registry system rejects transfers in the first 60 days after the initial registration as per ICANN Policy.
- \* Bulk Transfers: A bulk transfer is permitted during the Add Grace Period as per ICANN policy, and causes the Add Grace Period to not apply.

### 4.2 RENEW GRACE PERIOD

Length:5 days

RGP Status:renewPeriod

Allows the Sponsoring Registrar to undo a renewal within 5 days of the renewal command. The following rules apply for operations during this period:

- \* Delete: Sponsoring Registrar may delete the domain and receive a refund. The extension caused by the preceding renew is reversed and unless the domain is also in the Add Grace Period, the domain enters the Redemption state. If in the Add Grace Period it is deleted with immediate effect and available for registration.
- \* Renew: sponsor can renew a domain again and is charged for the operation, causing a second independent Renewal Grace Period to start. The total period is extended by the renewal term, limited to 10 yr maximum.
- \* Transfer: an approved transfer command ends the current Renew Grace Period without a refund and begins a Transfer Grace Period.
- \* Bulk Transfers: cause the Renew Grace Period to end without a refund, consequently registration periods are not changed.

#### 4.3 AUTO-RENEW GRACE PERIOD

Length:45 days

RGP Status:autoRenewPeriod

Allows for domains to remain in the DNS past expiration giving time for the Registrar to obtain renewal confirmation from the Registrant.

This period lasts for 45 days after expiration. The following rules apply for operations during this period:

\* Delete: the Registrar, may delete the domain and receive a refund. The domain enters the Redemption state.

\* Renew: the Registrar can renew a domain again and is charged for the operation, causing a second independent Renewal Grace Period to start. The total period is extended by the renewal term, limited to 10 yr maximum.

\* Transfer: an approved transfer command ends the current Auto-Renew Grace Period with a refund to the losing Registrar and begins a Transfer Grace Period. The registration period auto-renew extension is reversed and the registration is extended by the period specified in the transfer.

\* Bulk Transfers: bulk transfers cause the Auto-Renew Grace Period to end without a refund consequently registration periods are not changed.

#### 4.4 TRANSFER GRACE PERIOD

Length: 5 days

RGP Status:transferPeriod

Transfer Grace Period allows the Sponsoring Registrar to undo the registration period extension (due to a transfer command), via the deletion of a domain within 5 calendar days. The following rules apply for operations during this period:

\* Delete: the Registrar may delete the domain and receive a transfer fee refund. The extension to the registration period of the preceding transfer is reversed and the Redemption state is entered.

\* Renew: the Registrar can renew the domain causing a Renewal Grace Period to begin. The Registrar is charged and the total period is extended by the renewal term, limited to 10 yr maximum

\* Transfer: The Registry system rejects transfers in the first 60 days after the initial registration as per ICANN Policy. Special situations requiring a transfer back to the losing Registrar are dealt with case by case manually.

\* Bulk Transfers: bulk transfers cause the Transfer Grace Period to end without a refund; consequently registration periods are not changed.

The Transfer Grace Period does not have any impact on other commands.

#### 4.5 REDEMPTION GRACE PERIOD

Length:30 days

RGP Status:as described in Redemption state

Redemption Grace Period refers to the period of time the domain spends in the Redemption state, starting after a domain is deleted. The Redemption state description provides information on operations during this period.

#### 4.6 OVERLAP OF GRACE PERIODS

The 4 possible overlapping grace periods are:

\* Add Grace Period with 1 or more Renew Grace Periods.

\* Renew Grace Period with 1 or more other Renew Grace Periods.

\* Transfer Grace Period with 1 or more Renew Grace Periods.

\* Auto-Renew Grace Period with 1 or more Renew Grace Periods.

These are treated independently with respect to timelines however action that is taken has the combined effects of all grace periods still current.

##### 4.6.1 TRANSFER CLARIFICATION

If several billable operations, including a transfer, are performed on a domain and it is deleted in the operations' grace periods, only those operations performed after/including the latest transfer are eligible for refund.

## 5. TRANSITIONS

### 5.1. AVAILABLE › REGISTERED

Triggered by the receipt of a create command to register the domain. The Sponsoring Registrar is charged for the creation amount. this transition begins the Add Grace Period.

### 5.2 REGISTERED › PENDING TRANSFER

Triggered by the receipt of a request transfer command. The transfer must result in domain registration extension – the gaining Registrar is charged for the transfer. Requests to transfer the domain within 60 days of creation or a previous transfer are rejected.

### 5.3 PENDING TRANSFER › REGISTERED

Triggered by 1 of 4 operations:

- \* Cancel: the Gaining Registrar may cancel a transfer
- \* Reject: the Losing Registrar may reject the transfer
- \* Approve: the Losing Registrar may approve the transfer.
- \* Auto-Approve: If after 5 days, no action has been taken, the system approves the transfer.

In case of Cancel/Reject. The Gaining Registrar is refunded the transfer fee. The registration period remains unchanged and all grace periods existing at the time of transfer request remain in effect if not elapsed.

In case of Approve / Auto-Approve if the transfer was requested during the Auto-Renew Grace Period, the extension to the registration period is reversed and the Losing Registrar is refunded the auto-renew. The registration period is extended by the amount specified. This begins the Transfer Grace Period.

### 5.4 REGISTERED › DELETED

On receipt of a delete command if the domain is in the Add Grace Period, it is purged from the Database and immediately available for registration.

### 5.5 REGISTERED › REDEMPTION

On receipt of a delete command if the domain is not in the Add Grace Period, it transitions to the Redemption Period state and all grace periods in effect are considered.

### 5.6 REDEMPTION › PENDING RESTORE

On receipt of a restore command if the Redemption Period has not lapsed, the domain transitions to the Pending Restore state. The Sponsoring Registrar is charged a fee for the restore request.

### 5.7 PENDING RESTORE › REGISTERED

During the Pending Restore period the Sponsoring Registrar may complete the restore via a restore report containing the Whois information – submitted prior to the deletion, the Whois information at the time of the report, and the reason for the restoration.

### 5.8 PENDING RESTORE › REDEMPTION

Seven calendar days after the transition to the Pending Restore state, if no restore report is received the domain transitions to the Redemption state, which begins a new redemption period. The restore has no refund.

#### 5.9 Redemption ) Pending Delete

Thirty calendar days after the transition to the Redemption state, if no restore request is received the domain transitions to the Pending Delete state.

#### 5.10 PENDING DELETE ) DELETED

Five calendar days after the transition to the Pending Delete state, the domain is removed from the Database and is immediately available for registration.

### 6. LOCKS

Locks may be applied to the domain to prevent specific operations. The Sponsoring Registrar may set the locks prefixed with 'client' while locks prefixed with 'server' are added and removed by the Registry Operator. Locks are added and removed independently but they can be combined to facilitate the enforcement of higher processes, such as 'Registrar Lock', and outcomes required as part of UDRP. All locks are compatible with EPP RFCs. The available locks are:

- \* clientDeleteProhibited, serverDeleteProhibited - Requests to delete the object are rejected: - clientHold, serverHold - : DNS information is not published
- \* clientRenewProhibited, serverRenewProhibited - : Requests to renew the object are rejected. Auto-renew is allowed
- \* clientTransferProhibited, serverTransferProhibited - : Requests to transfer the object are rejected
- \* clientUpdateProhibited, serverUpdateProhibited - : Requests to update the object are rejected, unless the update removes this status

### 7. TYPICAL REGISTRATION LIFECYCLE

A typical domain is provisioned immediately on registration. The domain name may be updated over its lifetime to reflect changes in contact or delegation information. The domain name will remain active in the registry by automatic renewals once the registration period has lapsed however Registrars may elect to explicitly renew the domain before the automatic renewal or to extend the registration period by more than one year. The registrar may delete the domain following non-payment or request from the registrant resulting in the immediate removal from the DNS. A time-delayed set of server events will result in the purging of the name from the registry database if the name is not restored during a 30-day redemption period.

### 8. SPECIAL CONSIDERATIONS

#### 8.1 ICANN-APPROVED BULK TRANSFERS

ICANN-Approved Bulk Transfers performed in accordance with Part B of the Inter-Registrar Transfer Policy do not follow the typical transfer lifecycle. Existing grace periods are invalidated and no refunds are credited to the Losing Registrar. The prohibition of transfer period on domains created or transferred within 60 days does not apply.

#### 8.2 UNIFORM RAPID SUSPENSION

In the Uniform Rapid Suspension (URS) process, as described in the 'gTLD Applicant Guidebook' the following modification to the above processes is required.

Remedy allows for the addition of a year to the registration period, limited to the 10 year maximum. During this time no transform operations may be performed

other than to restore the domain as allowed by Appeal. At the expiration of the registration period the domain is not automatically renewed, but proceeds to the Redemption state as per the lifecycle described above, and it is not eligible for restoration.

#### 9. UPDATE/DNS

The update command does not impact the state of the domain through the Registration Lifecycle, however the command can be used to add and remove delegation information, which changes the DNS state of the domain.

#### 10. RESOURCES

This function will be performed by the following ARI departments:

- \* Products and Consulting team (7 staff)

- \* Development Team (11 staff)

the following departments outsourced to the Directi Group:

- \* Abuse and Compliance Team (20 staff)

ARI's Registry performs all time-based transitions automatically and enforces all other business rules – without requiring human resources for normal operation. If changes to the automatic behaviours or restrictions enforced by the policy system are required, ARI has a development team for this.

Domain Name Lifecycle aspects requiring human resources to manage are included in the ARI outsourcing include:

- \* Processing Add Grace Period exemptions as requested by Registrars.

- \* Processing restore reports provided by Registrars.

- \* Meeting the Registry Operators obligations under ICANN's Transfer Dispute Policy.

- \* Performing exception processing in the case of approved transfers during the 60 day transfer prohibition window.

The Products and Consulting team is responsible for product management of the Registration Lifecycle, including working with clients and the industry to identify new features or changes required to the system.

The automated aspects of the Registration lifecycle are supported by ARI's Domain Name Registry software. ARI has a development team for maintenance and improvement of the software

Most manual tasks fall to the Abuse and Compliance teams of the Directi Group, with staff experienced in development of policy for policy rich TLD environments. They have the required legal and industry background to perform this function.

The Compliance team outsourced to the Directi Group is responsible for any abuse of the registration policies within .Web and supervising the role of any external agency involved in validation

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q27 - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within. A detailed list of the Abuse and Compliance desk of Directi is provided in Q28.

ARI provides registry backend services to 5 TLDs and has a vast wealth of experience in estimating the number of resources required to support a Registry System.

Based on past experience ARI estimates that the existing staff is adequate to support a Registry System that is supporting at least 50M domains. Since .Web projects 471,482 domains, 0.94% of these resources are allocated to this TLD. See attachment 'Q27 - Registry Scale Estimates & Resource Allocation.xlsx' for

more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

The Directi Group is protected against loss of staff due to its scale of operations. This is described in further detail in Q39

#### 11. FINANCIAL COSTS

The usage of the ARI's staff and Registry Systems is included in our contract with ARI attached to Q46. This cost is shown in the financial answers.

The usage of Directi Group's staff is included in our contract with Directi attached to Q46. This cost is shown in the financial answers.

This completes our response to Q27.

## 28. Abuse Prevention and Mitigation

DotWeb Inc. is a wholly owned subsidiary within the Directi Group. The Directi Group runs various businesses including several ICANN Accredited Domain Registrars (including ResellerClub.com and BigRock.com) and Web Hosting companies. The Directi Group manages centralized functions for all its businesses. We have outsourced our Abuse and Compliance functions to the Directi Group and our Abuse and Compliance desk will be staffed as a cost center by them.

This response aims to provide a 360 degree perspective on our policies and processes to prevent abusive activities, and ensure swift mitigation when abuse does occur. We have prepared this plan based on over a decade's experience of fighting abuse as a Registrar, learnings through active industry participation, best-practices from existing registry operators and expert inputs from our back-end technical partner ARI (AusRegistry International).

#### 1. ABUSE MITIGATION EXPERIENCE AND CAPABILITIES

With over four million active domain names registered through its registrars, Directi has significant experience (over 10 years) of managing domain names and is fully cognizant of the threat that stems from their abuse.

As one of the world's top ten registrars, we equally understand our ability to make a sizable contribution towards curbing internet abuse, and believe that mitigating this threat is one of our foremost responsibilities. By instituting policies, processes and services which go significantly above and beyond our obligation as a registrar, Directi has taken various initiatives to make the Internet a safer ground.

To drive this effort, Directi has a committed function working towards identifying abusive domain names and enforcing its policies. Our Abuse Desk functions 24/7 and takes prompt and effective action (both reactively and proactively) against domains reported or co-networked to be involved in any sort of online abuse. Complaints ranging from phishing, spam, malware perpetration, 419 scams, child pornography, copyright infringement and varied forms of abuse are subject to investigation at our Abuse Desk on a daily basis. The nature of abuse and the types of complaints received are varied in nature and intensity, and are documented in more detail further.

On average we already address, 15000 reported or detected abuse cases per year. Abuse cases are addressed within pre-determined SLAs, and our team is committed to ensure that each incident is resolved satisfactorily. The Directi abuse team

has been heralded on many occasions by various security groups, law enforcement organizations and the general anti-abuse community for the manner in which abuse mitigation has been handled by us. Additionally, we have always become highly involved, and continue to remain committed to industry-wide efforts to address organized abuse such as botnets (see below) and large scale phishing attacks, and any other malfeasances.

#### 1.1 NOTABLE INSTANCES OF DIRECTI'S SUCCESSFUL ABUSE MITIGATION INITIATIVES

Our abuse mitigation team has developed strong relationships with many security groups and individuals in the abuse mitigation community, with the aim of sharing intelligence and facilitating quick action on abusive domain names. These sources provide us actionable intelligence on domains bought through our registrar. We have also participated in coordinated takedowns with such agencies in the past and are committed to doing so in the future. Please refer to Attachment 'Q28\_Recommendations' which showcases letters from several global agencies including the IRS, commending our work and cooperation on several fronts. Following are some examples of cases where our efforts paid great results in abuse mitigation -

##### 1.1.1 MARIPOSA WORKING GROUP

Directi was part of the Mariposa Working Group which was responsible for taking down the largest known botnet network at the time.

(Ref: [http://defintel.com/docs/Mariposa\\_White\\_Paper.pdf](http://defintel.com/docs/Mariposa_White_Paper.pdf))

"Directi is BY FAR THE BEST registrar we have ever worked with at taking down criminal domains in a timely, efficient and professional manner. Your team was absolutely key to the Mariposa Working Group taking down one of the largest Botnets in the history of the Internet. You and your team should be VERY proud of that :)" -- Christopher Davis, Former CEO of Defence Intelligence

##### 1.1.2 IM WORM BOTNET TAKEDOWN COORDINATED BY IID

Since 1996, IID (Internet Identity) has been providing technology and services that secure the Internet presence for an organization and its extended enterprise. It recently introduced a number of unique approaches to secure organizations' use of Internet infrastructure with ActiveTrust® BGP, ActiveTrust DNS, and ActiveTrust Resolver with TrapTrace. Directi worked with IID, acting against problematic domain names and sharing intelligence to take down a notorious botnet that was plaguing the internet for quite some time.

"Thank you for your exceptional coordination with our team and the other providers ... during the simultaneous shutdown. We wanted to follow up with you and let you know that despite the last minute unanticipated scramble, the takedown was a success and the botnet has been shutdown." -- Lauren Lamp, Manager / Service Delivery - internetidentity.com

##### 1.1.3 FAKE PHARMACY TAKEDOWNS COORDINATED BY LEGITSCRIPT

LegitScript is the leading source of information for patients, Internet users, physicians, businesses and other third parties who need to know if an Internet pharmacy is acting in accordance with the law and accepted standards of ethics and safety. LegitScript is identified by the National Association of Boards of Pharmacy as the only Internet pharmacy verification service that adheres to its standards. After affiliating with LegitScript, we have witnessed a steep downfall in fake pharma-related registrations. ResellerClub (referred below) is our wholesale registrar brand.

(Ref:<http://legitscriptblog.com/2009/03/directi-no-safe-haven-for-rogue-internet-pharmacies/>)

"Some registrars claim that they cannot shut down dangerous 'no-prescription-required' and fake online pharmacies. ResellerClub has proven that

this is not true. By refusing to profit from dangerous, criminal activity at the expense of Internet users, ResellerClub has established itself as a responsible example for the rest of the Internet community." John Horton, President, LegitScript.com

We have enclosed a commendation letter from LegitScript in Attachment 'Q28\_Recommendations', which speaks of our leadership in fighting fake and rouge pharmacies.

#### 1.1.4 419 FEEDBACK LOOP WITH ARTISTS AGAINST 419 (AA419.ORG)

An honorary member of the APWG (Anti-Phishing Working Group), Artists Against 419 is a premier organization with expertise in identifying, cataloging, and terminating fraud sites. Our tie-up with them has been greatly successful in eliminating fraudulent registrations within our portfolio. (Ref: <http://blog.aa419.org/?p=134>)

"Many registrars do respond to abuse reports and take action against them. However none do it as quickly and efficiently as Directi. If all registrars and hosters take this approach, it might then be possible to reduce internet fraud." -- aa419.org

We have enclosed a letter from Artists Against 419 in Attachment 'Q28\_Recommendations' commending the speed and impact of our proactive abuse mitigation activities.

## 2. PROPOSED ABUSE POLICY FOR .WEB

We have fully adopted the definition of abuse developed by the Registration Abuse Policies Working Group (Registration Abuse Policies Working Group Final Report 2010).

Our abuse policies described in this section apply to initial and ongoing domain registrations, ie any domain name must comply with these policies during registration and throughout its tenure.

Abusive behaviour in a TLD may relate can be categorized into:

### 2.1 REGISTRATION POLICY VIOLATIONS

.Web adopts certain Registration policies and any violations of these policies would be treated as an Abuse.

#### 2.1.1 SUNRISE POLICY VIOLATION

.Web will have a sunrise period as described in the response to Question 29. Our sunrise policy will have an overarching goal to protect interests of IP holders globally, and be based on best practices seen in previous TLD launches. We will implement the Trademark Claim Service and partner with experienced service providers to run the TM verification, Sunrise Challenge and Auction processes. All Sunrise domain names will be validated before they are activated. Hence the possibility of a Sunrise policy violation is low. However the Sunrise process provides for a Sunrise Dispute Resolution Policy, and any disputes that fall within its scope will be referred to the Sunrise Dispute Resolution provider. If the abuse desk receives any complaints concerning a sunrise domain which violates the Sunrise eligibility policy the abuse desk will direct the complainant to the Sunrise Dispute Resolution provider

#### 2.1.2 WHOIS INACCURACY

.Web requires Whois accuracy as per its contracts. Any domain name with inaccurate whois information will be deemed to be in violation of its contract



and hence will be deemed as an abuse and handled in the manner described ahead.

### 2.1.3 TRADEMARK INFRINGEMENT VIOLATION AND UDRP

.Web requires registrants to abide by UDRP. If the abuse desk receives any complaints concerning a domain name which infringes upon the trademark right of a 3rd party, the abuse desk will direct the complainant to the Uniform Dispute Resolution provider.

All names registered under .Web will be subject to the UDRP and URS processes. We believe that URS will deter cybersquatting, and some malicious activities that illegitimately use brand names. We will seek to expeditiously process all URS cases, and are already equipped with mature processes and tracking systems to manage and keep track of all cases.

The URS process will be run by our compliance team, who has significant experience in processing UDRP complaints for our Registrar businesses.

While Registrars will be responsible for processing all UDRP cases related to the .Web, we will reserve the right to act on their behalf when necessary, and process all court orders that are directed to us.

## 2.2 ACCEPTABLE USAGE RELATED VIOLATIONS

.Web adopts certain Content and Acceptable usage policies and any violations of these would be treated as an Abuse. The following are deemed as violations of our content and acceptable usage policy

### 2.2.1 INTELLECTUAL PROPERTY, TRADEMARK, COPYRIGHT, AND PATENT VIOLATIONS, INCLUDING PIRACY

Intellectual property (IP) is a term referring to a number of distinct types of creations of the mind for which a set of exclusive rights are recognized—and the corresponding fields of law. Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual property rights include copyrights, trademarks, patents, industrial design rights and trade secrets in recognized jurisdictions. Any act resulting in theft, misuse, misrepresentation or any other harmful act by any individual or a company is categorized as Intellectual Property violation.

### 2.2.2 SPAMMING

The use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Web sites and Internet forums. Unsolicited emails advertising legitimate and illegitimate products, services, and/or charitable requests and requests for assistance are also considered as spam.

### 2.2.3 PHISHING (and various forms of identity theft)

Fraudulent web services and applications meant to represent/confuse or mislead internet users into believing they represent services or products for nefarious purposes, such as illegally gaining login credentials to actual legitimate services.

### 2.2.4 PHARMING AND DNS HIJACKING

Redirection of DNS traffic from legitimate and intended destinations, by compromising the integrity of the relevant DNS systems. This leads unsuspecting Internet users to fraudulent web services and applications for nefarious purposes, such as illegally gaining login credentials to actual legitimate

services.

#### 2.2.5 DISTRIBUTION OF VIRUSES OR MALWARE

Most typically the result of a security compromised web service where the perpetrator has installed a virus or "malevolent" piece of software meant to infect computers attempting to use the web service in turn. Infected computers are then security compromised for various nefarious purposes such as gaining stored security credentials or personal identity information such as credit card data. Additionally compromised computers can sometimes be remotely controlled to inflict harm on other internet services (see botnet below).

#### 2.2.6 CHILD PORNOGRAPHY

Child pornography refers to images or films (also known as child abuse images) and, in some cases, writings depicting sexually explicit activities involving a minor.

#### 2.2.7 USING FAST FLUX TECHNIQUES

A methodology for hiding multiple source computers delivering malware, phishing or other harmful services behind a single domain hostname, by rapidly rotating associated IP addresses of the sources computers through related rapid DNS changes. This is typically done at DNS zones delegated below the level of a TLD DNS zone.

#### 2.2.8 RUNNING BOTNET COMMAND AND CONTROL OPERATIONS

A Botnet is a significant coordinated net of compromised (sometimes tens of thousands) computers running software services to enact various forms of harm - ranging from unsanctioned spam to placing undue transaction traffic on valid computer services such as DNS or web services. Command and control refers to a smaller number of computers that issue/distribute subsequent commands to the Botnet. Compromised botnet computers will periodically check in with a command and control computer that hides behind a list of date triggered, rotating domain registrations, which are pre-loaded in the compromised computer during its last check-in.

Registries play a key role in breaking this cycle of pre-determined domain registrations by deactivating said registrations prior to the compromised computers being able to use them to contact the command and control computer. Successful intervention results in the botnet losing contact with their command and control computers, leaving them inactive and reducing potential harms.

#### 2.2.9 HACKING

Hacking constitutes illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of other individuals. Also includes any activity that might be used as a precursor to an attempted system penetration.

#### 2.2.10 FINANCIAL AND OTHER CONFIDENCE SCAMS

Financial scams, including but not limited to the cases defined below, are operated by fraudsters to lure investors into fraudulent money making schemes. Prominent examples that will be treated as abusive are -

1. Ponzi Schemes. A Ponzi scheme is essentially an investment fraud wherein the operator promises high financial returns or dividends that are not available through traditional investments. Instead of investing victims' funds, the operator pays "dividends" to initial investors using the principle amounts "invested" by subsequent investors. The scheme generally falls apart when the operator flees with all of the proceeds, or when a sufficient number of new investors cannot be found to allow the continued payment of "dividends."
2. Money Laundering. Money laundering, the metaphorical "cleaning of money"

with regard to appearances in law, is the practice of engaging in specific financial transactions in order to conceal the identity, source, and/or destination of money, and is a main operation of the underground economy.

3. 419 Scams. "419" scam (aka "Nigeria scam" or "West African" scam) is a type of fraud named after an article of the Nigerian penal code under which it is prosecuted. It is also known as "Advance Fee Fraud". The scam format is to get the victim to send cash (or other items of value) upfront by promising them a large amount of money that they would receive later if they cooperate.

#### 2.2.11 ILLEGAL PHARMACEUTICAL DISTRIBUTION

Distribution and promotion of drugs, locally within a nation or overseas, without prescription and appropriate licenses as required in the country of distribution are termed illegal.

#### 2.2.12 OTHER VIOLATIONS

Other violations that will be expressly prohibited under the .Web include

- \* Network attacks
- \* Violation of applicable laws, government rules and other usage policies

### 3. PROCEDURES TO MINIMIZE ABUSIVE REGISTRATIONS

#### 3.1 BUILDING A ZERO-TOLERANCE REPUTATION

Our Anti-Abuse Policy will put Registrants on notice of the ways in which we will identify and respond to abuse and serve as a deterrent to those seeking to register and use domain names for abusive purposes. The policy will be made easily accessible on the Abuse page of our Registry website which will be accessible and have clear links from the home page along with FAQs and contact information for reporting abuse.

Directi has vast experience in minimizing abusive registrations. Our zero tolerance procedures and aggressive proactive takedown measures as a Domain Registrar have resulted in a white-hat reputation discouraging abusive registrations to begin with. We intend on following the same approach with respect to Registry operations for .Web. Our proactive abuse procedures are geared towards building a reputation that discourages miscreants and malicious intent. Once it is known that abusive registrations and registrations in violation of our policies are suspended rapidly, both abusive registrations and abusive behavior will be discouraged.

Our Abuse policies described in section 2 above apply to new and ongoing registrations.

#### 3.2 BUILDING AWARENESS OF OUR ANTI-ABUSE POLICY

The Abuse Policy will be published on the abuse page of our Registry website which will be accessible and have clear links from the home page. The abuse page of our Registry website will emphasize and evidence our commitment to combating abusive registrations by clearly identifying what our policy on abuse is and what effect our implementation of the policy may have on registrants. We anticipate that the clear message, which communicates our commitment to combating abusive registrations, will further serve to minimize abusive registrations in our TLD.

#### 3.3 ICANN PRESCRIBED MEASURES

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

\* DNSSEC deployment, which reduces the opportunity for pharming and other man-in-the-middle attacks. We will encourage registrars and Internet Service Providers to deploy DNSSEC capable resolvers in addition to encouraging DNS hosting providers to deploy DNSSEC in an easy to use manner in order to facilitate deployment by registrants. DNSSEC deployment is further discussed in the context of our response to Question 43;

\* Prohibition on Wild Carding as required by section 2.2 of specification 6 of the Registry Agreement

\* Removal of Orphan Glue records: ICANN requires a policy and procedure to take action to remove orphan glue records from the zone when provided with evidence that the glue is indeed present and aiding malicious conduct. The ARI Managed TLD Registry SRS database does not allow orphan records. Glue records are removed when the delegation point NS record is removed. Other domains that need the glue record for correct DNS operation may become unreachable or less reachable depending on their overall DNS service architecture. It is the Registrant's responsibility to ensure that their domain name does not rely on a glue record that has been removed and that it is delegated to a valid name server. The removal of glue records upon removal of the delegation point NS record mitigates the potential for use of orphan glue records in an abusive manner

### 3.4 REGISTRANT DISQUALIFICATION

Abusive domain registration has historically attracted a small number of individuals and organisations that engage in high volume registrations, driven by the marginal profitability of individual abusive registrations. As specified in our Anti-Abuse Policy, we reserve the right to deny registration of a domain name to a Registrant who has repeatedly engaged in abusive behaviour in our TLD or any other TLD.

Registrants, their agents or affiliates found through the application of our Anti-Abuse Policy to have repeatedly engaged in abusive registration will be disqualified from maintaining any registrations or making future registrations. This will be triggered when our records indicate that a Registrant has had action taken against it an unusual number of times through the application of our Anti-Abuse Policy.

Registrant disqualification provides an additional disincentive for qualified registrants to maintain abusive registrations in that it puts at risk even otherwise non-abusive registrations through the possible loss of all registrations.

In addition, name servers that are found to be associated only with fraudulent registrations will be added to a local blacklist and any existing or new registration that uses such fraudulent NS record will be investigated.

The disqualification of 'bad actors' and the creation of blacklists mitigates the potential for abuse by preventing individuals known to partake in such behaviour from registering domain names.

### 3.5 PROACTIVE DETERMINATION OF POTENTIAL ABUSE

There are several tell-tale signs which are indicative of abusive intent. The following are examples of the data variables will serve as indicators that we will monitor with the help of our registry technical partner.

\* Unusual Domain Name Registration Practices: practices such as registering hundreds of domains at a time, registering domains which are unusually long or complex or include an obvious series of numbers tied to a random word (abuse40, abuse50, abuse60) may when considered as a whole be indicative of abuse

\* Domains or IP addresses identified as members of a Fast Flux Service Network (FFSN): Our service provider ARI uses the formula developed by the University

of Mannheim and tested by participants of the Fast Flux PDP WG to determine members of this list. IP addresses appearing within identified FFSN domains, as either NS or A records shall be added to this list.

\* An Unusual Number of Changes to the NS record: the use of fast-flux techniques to disguise the location of web sites or other Internet services, to avoid detection and mitigation efforts, or to host illegal activities is considered abusive in the TLD. Fast flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. As such an unusual number of changes to the NS record may be indicative of the use of fast-flux techniques given that there is little, if any, legitimate need to change the NS record for a domain name more than a few times a month.

\* Results of Monthly Checks: The random monthly checks to promote Whois accuracy (described ahead) are not limited to serving that purpose but may also be used to identify abusive behaviour given the strong correlation between inaccurate Whois data and abuse.

\* Analysis of Cross Validation of Registrant Whois data against Whois Data Known to be Fraudulent.

\* Analysis of Domain Names belonging to Registrant subject to action under the Anti-Abuse policy: in cases where action is taken against a registrant through the application of our Anti-Abuse policy, we will also investigate other domain names by the same registrant (same name, nameserver IP address, email address, postal address etc).

#### 4. PROCEDURES FOR HANDLING COMPLAINTS

##### 4.1 MECHANISMS FOR REPORTING COMPLAINTS

In order to make it easy for security agencies, law enforcement bodies and vigilant users to report incidents of abusive behavior within .Web, we shall enable several channels of communication.

###### 4.1.1 SINGLE POINT OF CONTACT

In accordance with section 4.1 of specification 6 of the Registry Agreement we will establish a single abuse point of contact (SAPOC) responsible for addressing and providing a timely response to abuse complaints concerning all names registered in the TLD through all registrars of record, including those involving a reseller. Complaints may be received from members of the general public, other registries, registrars, LEA (Law Enforcement Agencies), government and quasi governmental agencies and recognised members of the anti-abuse community.

The SAPOC's accurate contact details (email, fax and mailing address) will be provided to ICANN and published on the abuse page of our Registry website. The SAPOC will in turn represent the entire compliance desk operated by the Directi group on behalf of .Web as an outsourced function.

The Registry website will additionally also include:

- \* All public facing policies in relation to the TLD including the Anti-Abuse Policy described in section 2
- \* A web based submission service for reporting inaccuracies in Whois information
- \* Registrant Best Practices
- \* Conditions that apply to proxy registration services and direction to the SAPOC to report domain names that violate the conditions

As such, the SAPOC may receive complaints regarding a range of matters concerning the abuse policy defined in section 2

The SAPOC will be the primary method by which we will receive notification of abusive behaviour from third parties. It must be emphasised that the SAPOC will be the initial point of contact following which other processes will be triggered depending on the identity of the reporting organization and the type of abuse. Accordingly, separate processes for identifying abuse will exist for reports by LEA/government and quasi governmental agencies and members of the general public.

When any party makes a report via the Abuse POC e-mail address or the abuse web form, he or she will receive back a ticket number from a ticketing system. Our abuse team will then examine these reports, and use a ticketing system to track each issue. This process will leverage a dedicated software that we have used for handling abuse reports to our registrar businesses. It is our goal to provide a timely response to all abuse complaints concerning domains registered in the TLD, as per the SLAs defined by us.

#### 4.1.2 LAW ENFORCEMENT AGENCIES

We recognise that LEA, governmental and quasi governmental agencies may be privy to information beyond the reach of others which may prove critical in the identification of abusive behaviour in our TLD. As such, we will provide an expedited process which serves as a channel of communication for law enforcement, government and quasi-governmental agencies to, amongst other things, report illegal conduct in connection with the use of the TLD.

The process will involve prioritization and prompt investigation of reports identifying abuse from those organizations. The steps in the expedited process are summarised as follows:

1. We will identify relevant LEA, government and quasi governmental agencies who may take part in the expedited process
2. We will establish back channel communication with each of the identified agencies in order to obtain information that may be used to verify the identity of the agency upon receipt of a report utilising the expedited process;
3. We will publish contact details on the abuse page of the Registry website for the SAPOC to be utilised by only those taking part in the expedited process;
4. All calls to this number will be responded to by a member of our 24/7 Compliance Team
5. We will verify the identity of the reporting agency employing methods specific to that agency established during back channel communication;
6. Upon verification of the reporting agency, we will obtain the details necessary to adequately investigate the report of abusive behaviour in the TLD;
7. Reports from verified agencies may be provided in the Incident Object Description Exchange Format (IODEF) as defined in RFC 5070. Provision of information in the IODEF will improve our ability to resolve complaints by simplifying collaboration and data sharing
8. The report identifying abuse will then be dealt with in accordance to our process defined in subsequent sections of this answer

#### 4.2 EVALUATION OF COMPLAINTS

The next step is for our abuse desk staff to review each complaint. The abuse team looks at the facts of each complaint in order to verify the complaint. The goals are accuracy, good record-keeping, and a zero false-positive rate so as not to harm innocent registrants while at the same time, taking timely action to mitigate abusive behaviour and to minimize impact.

Evaluation of complaints thus forms a very important part of the process. The following factors are considered for each case:

\* Type, Severity and immediacy of the abuse: Upon initial review, all incoming complaints will face an initial evaluation on the basis of severity and harm

cased due to the abuse. While we will adhere to the SLAs laid down for our abuse mitigation processes, regardless of the type of complaint, there will be some complaints that will be considered relatively more severe and of greater malicious impact than others. Complaints with a higher severity-malicious impact and immediacy will be processed with greater urgency than others.

\* Determining the origin of the complaint: a credible complainant e.g. a law enforcement agency, a security group etc. automatically lends genuineness to a complaint while a complaint from a previously unknown source will require a background check to ensure that the complaint is not from a miscreant looking to create unnecessary trouble for a domain owner. Thus while we may take immediate action complaints from reliable sources, those from other sources, not backed by enough evidence, may require further due-diligence before action is taken.

\* Evaluating proof submitted along with a complaint: A complaint is also evaluated based on the supporting evidence provided which further determines the validity of a complaint. At this stage we will also attempt to establish a clear link between the activity reported and the alleged type of abusive behaviour. This is done to ensure that addressing the reported activity will address the abusive behaviour. In some cases the abuse is evident, which will result in immediate processing of the complaint from our side without much further due-diligence. In some cases, where the abuse may not be evident upfront, our desk will rely on supplementary evidence provided by the complainant which may be further ratified. While not limited to this list, supporting evidence could range from links, screen-shots of websites, copy right / trademark details, emails, email headers, whois information, ID proof etc.

\* Evaluating historical data: As mentioned before, we will maintain a log of all complaints received, including the contact details of complainants, the whois details of the abusers, the nameservers of abusive domain registrations, the type of domain names, the IPs of spamming domains etc. This will further help us in establishing trends for further action as required. A registration that re-sounds alarms from previously seen abusive trends will ascertain the necessary pre-emptive mitigation processes.

Assessing abuse reports requires good judgment, and we will rely upon our, specially trained abuse desk staff.

While we recognise that each incident of abuse represents a unique security threat and should be mitigated accordingly, we also recognise that prompt action justified by objective criteria are key to ensuring that mitigation efforts are effective. With this in mind, we have categorised the actions that we may take in response to various types of abuse by reference to the severity and immediacy of harm. This categorisation will be applied to each validated report of abuse and actions will be taken accordingly. It must be emphasised that the actions to mitigate the identified type of abuse in the section/s below are merely intended to provide a rough guideline and may vary upon further investigation.

#### 4.3 CATEGORIZATION OF COMPLAINTS

Each confirmed case of abuse is bucketed into one of the following categories

##### 4.3.1 CATEGORY 1

Probable Severity or Immediacy of Harm - Low

Examples of types of abusive behaviour - Small Scale Spam, Whois Inaccuracy

Mitigation steps:

1. Preliminary Investigation
2. Delegate to Registrar

3. Monitor response time-frame vis-à-vis SLA
4. Take direct action in case of Registrar non-conformance.

#### 4.3.2 CATEGORY 2

Probable Severity or Immediacy of Harm - Medium

Examples of types of abusive behaviour - Medium scale spam, inactive botnets and other forms of abuse which have a higher degree of impact than the ones bucketed as category 1, but still relatively limited in terms of potential damage.

Mitigation steps:

1. Preliminary Investigation
2. Delegate to Registrar
3. Monitor response time-frame vis-à-vis SLA
4. Take direct action in case of Registrar non-conformance.

#### 4.3.3 CATEGORY 3

Probable Severity or Immediacy of Harm - High

Examples of types of abusive behaviour - Fast Flux Hosting, Phishing, Large scale hacking, Pharming, Botnet command and control, Child Pornography and all other cases deemed to carry a very high risk of large scale impact

Mitigation steps for Abuse policy violation:

1. Suspend domain name
2. Investigate
3. Restore or terminate domain name

### 4.4 MITIGATION OF COMPLAINTS

The mitigation steps for each category will now be described:

#### 4.4.1 CATEGORY 1

Types of abusive behaviour that fall into this category include those that represent a low severity or immediacy of harm to registrants and internet users. These generally include behaviours that result in the dissemination of unsolicited information or the publication of illegitimate information. While undesirable, these activities do not generally present such an immediate threat as to justify suspension of the domain name in question. Each of these cases will be delegated down to the Registrar and the registrar's performance, in terms of response and resolution rate, will be monitored and recorded by us. In case of non-conformance by the Registrar, we will take-over the issue.

We will also continually monitor the issue to track possible increases in the severity of harm. In case the threat level is above what was originally anticipated, we will escalate the issue to category two or three and act in accordance.

#### 4.4.2 CATEGORY 2

Types of abusive behaviour that fall into this category include those that represent a medium severity or immediacy of harm to registrants and internet users. These generally include medium scale spam, network intrusion, inactive botnets etc. Following the notification of the existence of such behaviours, our compliance team will delegate the issue to registrars and invoke the more aggressive SLAs that apply to this category of risk.

As was the case with category 1, we will continue to monitor the registrar's conformance with the SLAs and take direct action when necessary. We will also



check for possible increases in risk levels and escalate the abuse category if required.

#### 4.4.3 CATEGORY 3

Highly serious, sensitive and large scale issues like phishing, child pornography and large-scale botnet are considered to be a serious violation of the Anti-Abuse Policy owing to its fraudulent exploitation of consumer vulnerabilities, high level of risk and far-reaching consequences. Given the direct relationship between the uptime of these activities, and extent of harm caused, we recognise the urgency required to execute processes that handle these cases directly, without any delegation.

As soon as the abuse is substantiated, we will proceed to suspend the domain name pending further investigation to determine whether the domain name should be unsuspended or cancelled. Cancellation will result if upon further investigation, the behaviour is determined to be one of the types of abuse defined in the Anti Abuse Policy.

In some cases we may change the nameservers associated with the domain and/or use EPP prohibited statuses in appropriate combinations to restrict activity against the domain such as contact updates, deletes or transfers.

In the past we have modified Nameservers to sinkhole malicious domains, so research partners can measure botnets and monitor malware activity. We believe this to be an extremely effective mechanism which takes down large scale attacks from the source, and assists researchers to build processes and tools which prevent future attacks from the same source. Our team will follow the same process for domains belonging to our registry.

We have built special systems to suspend individual and bulk batches of domains. This will allow us to quickly take care of cases where criminals have obtained bulk batches of domain names. This will be of use if malware designers use generation algorithms to register domains.

Reactivation of the domain name will result where further investigation determines that abusive behaviour, as defined by the Anti Abuse Policy, does not exist and that the domain name is not causing any harm.

#### 4.5 PROPOSED RESOLUTION METRICS AND SERVICE LEVEL AGREEMENTS

##### SLA RESPONSE CONSIDERATIONS FOR REPORTED ABUSE CASES

As described earlier, each abuse case and goes into one of three response categories depending on the severity and immediacy of the harm caused by the abuse. In the case of any failed SLA responses, the Registry reserves the right to act directly to suspend and/or lock the domains associated with a given abuse case. Additionally, highly serious, sensitive and large scale issues are ranked as category 3 and prioritized above all other cases.

Attachment 'Q28\_Abuse Mitigation SLA', shows the flowchart and SLA response for each category of abuse complaint

##### 4.5.1 CATEGORY 1

Some examples of abuses cases that will be categorized as 1 include:

- \* Low scale Spam
- \* Whois Inaccuracy
- \* Low scale Malware
- \* Any other abuse case deemed as low risk

RESPONSE SLA COMMITMENTS:

- \* Initial Registry Response to Complainant: 2 business days from the time of receipt of the complaint
- \* Registry Notification to Registrar: 2 business days from the time of receipt of the complaint
- \* Initial Response from Registrar: 3 business days from the time that the complaint notification is sent to the Registrar
- \* Update from Registrar as action taken or intended: 7 business days from the time that the complaint notification is sent to the Registrar
- \* Final Resolution: 15 business days from the time the issue was reported to us

#### 4.5.2 CATEGORY 2

Some examples of abuses cases that will be categorized as 2 include:

- \* Medium scale Spam
- \* Confirmed but inactive botnet domains
- \* All other abuse cases deemed as medium scale

#### RESPONSE SLA COMMITMENTS:

- \* Initial Registry Response to Complainant: 2 business days from the time of receipt of the complaint
- \* Registry Notification to Registrar: 2 business days from the time of receipt of the complaint
- \* Initial Response from Registrar: 2 business days from the time that the complaint notification is sent to the Registrar by the Registry
- \* Update from Registrar as action taken or intended: 3 business days from the time that the complaint notification is sent to the Registrar by the Registry
- \* Final Resolution: 8 business days from the time of receipt of the complaint

#### 4.5.3 CATEGORY 3

Some examples of abuses cases that will be categorized as 3 include:

- \* Confirmed Cases of child pornography
- \* Confirmed cases of Phishing
- \* Confirmed and active botnets domains
- \* Any other case deemed as large scale

#### RESPONSE SLA COMMITMENTS:

- \* Initial Registry Response to Complainant: 1 business day from the time of receipt of the complaint
- \* Registry time to direct takedown: 3 business days from the time of receipt of the complaint

#### 4.6 FOLLOW-UP AND CAPTURE OF METRICS

The abuse staff will track each abuse complaint ticket to resolution. Our ticketing system allows us to capture many metrics. We will measure resolution times, and we can see what percentage of abuse reports could be confirmed. We will also capture how many domains were suspended, and we will break down statistics by registrar in the TLD. This will help us identify registrars that have regular problems, and we can work with them to systematically identify and act against bad actors.

#### 4.7 CONTRACTUAL PROVISIONS

As the registry operator, we will use the Registry-Registrar Agreement (RRA) to establish the registry's right to act against abusive registrations as described in the preceding sections. We will also use the contract to impose certain obligations on the registrars, and make some obligations binding on the registrants by obligating specific terms in the registrar-registrant contract.

The contract will be a mandatory part of the Registrar accreditation process with the Registry. Production access to the Registry will not be granted until the contract is duly signed AND the registrar has provided copy of their Registry Registrant Agreement to demonstrate the inclusion of any required pass-through provisions. The registrar is also fully obligated to their accreditation contracts with ICANN (via the RAA) which includes elements such as the UDRP.

In general, the contracts will establish that the registry operator may reject a registration request, or can delete, revoke, update, suspend, cancel, or transfer a registration for violations of our anti-abuse policies. The terms in our proposed agreement will empower us to take necessary action including, but not limited to:

- \* Discretionary action against domain names that are not accompanied by complete and accurate information as required by ICANN Requirements and/or Registry Policies or where required information is not updated and/or corrected as required by ICANN Requirements and/or Registry Policies;
- \* Action as may be required to protect the integrity and stability of the Registry, its operations, and the TLD system;
- \* Action as may be required to comply with any applicable law, regulation, holding, order, or decision issued by a court, administrative authority, or dispute resolution service provider with jurisdiction over the Registry;
- \* Action as may be required to establish, assert, or defend the legal rights of the Registry or a third party or to avoid any civil or criminal liability on the part of the Registry and/or its affiliates, subsidiaries, officers, directors, representatives, employees, contractors, and stockholders;
- \* Action as may be required to correct mistakes made by the Registry or any Accredited Registrar in connection with a registration; or
- \* Enforcement of Registry policies and ICANN requirements; each as amended from time to time;
- \* Actions as otherwise provided in the Registry-Registrar Agreement and/or the Registry-Registrant Agreement.

Below are some additional points that we will look to cover in the RRA. These clauses will enable us to enforce some additional, proactive measures to curb and deter abuse:

- \* We will reserve the right to deny registration of a domain name to a registrant who has repeatedly engaged in abusive behaviour in our TLD or any other TLD.
- \* We will reserve the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.
- \* We may amend or otherwise modify this policy to keep abreast of changes in consensus policy or new and emerging types of abusive behaviour in the Internet.
- \* Relevant language that enforces Registrars to conform with the SLAs provided for abuse cases delegated to them and provides the Registry with rights to take relevant actions in those cases.
- \* Relevant language for sanctions against a Registrar leading to termination with respect to repeated offences and violations of their obligations with respect to abuse mitigation.
- \* Relevant language that requires Registrars to provide for the following in

their agreement with the Registrants

\*\* Whois accuracy provisions

\*\* Acceptable content and usage policy

\*\* Sunrise policy and submission to SDRP

\*\* UDRP

\*\* Rights granted to the Registrar and Registry to take necessary action wrt abuse prevention including sharing information with regulatory bodies and LEA and domain takedowns where appropriate

\*\* Indemnification

All of the contracts above will be regularly reviewed (atleast once a year) based on the experience gained by the Registry during actual operation and any relevant changes required to mitigate abuse will be appropriately introduced in consultation with ICANN and the Registrars

#### 4.8 ADDITIONAL MITIGATION MEASURES

Based on our experience of running a leading Registrar, we have also devised some powerful mechanisms which will prevent possible abuse, and quickly diffuse abusive domains. These mechanisms include:

##### 4.8.1 PROFILING & BLACKLISTING

This process, currently in practice for our registrar businesses within the Directi Group, is used for gathering intelligence on known offenders. We maintain abuse ratios for each of the 1,000,000 plus registrants and 65,000 plus resellers who use Directi.

Experience has enabled us to use these ratios accurately to uncover registrants who are known and repeated offenders. Expert offenders rarely reuse the same registrant profile and often maintain a myriad number of profiles to mask their true identity. Through pattern mapping we try and group registrant profiles that we believe belong to the same operator.

The same process is followed at the reseller level too, to identify those resellers who are knowingly harboring offenders, or are themselves involved in abuse.

When a registrant profile is confirmed to be involved in organized abuse, including but not limited to cybersquatting, phishing, pharming etc., our immediate step is to suspend that customer's control over his abusive domain portfolio. Our compliance team then carefully analyzes each domain name to identify those which are abusive and not already taken-down. The necessary action is undertaken to diffuse any ongoing abuse.

We plan to adopt the 'Profiling and Blacklisting' process within our registry operations. Since all of our compliance resources will be trained and experienced in running this process, its implementation into .Web will be simple. Specifics of this policy and process, as it applies to our registry business, will be drawn out.

##### 4.8.2 PROACTIVE QUALITY REVIEW

As a preventive safeguard against abusive domain registration, we follow a consistent review process for domain registrations on our registrar, where a sample of newly registered domain names are analyzed for potential abusive activity. Coupled with our profiling process (described above), it enables us to take proactive measures against domain names that are registered solely to perpetrate malicious activities such as phishing, or otherwise infringe on the rights of others. This helps us curb abusive activity before it can affect too many Internet users. We shall seek to implement similar safeguards for .Web, and encourage registrars to incorporate this practice as part of their abuse mitigation processes.

#### 4.9 INDUSTRY COLLABORATION AND INFORMATION SHARING

Upon obtaining Registry Accreditation, we will join the Registry Internet Safety Group (RISG), whose mission is to facilitate data exchange and promulgate best practices to address internet identity theft, especially phishing and malware distribution. In addition, Directi coordinates with the Anti-Phishing Working Group (APWG), other DNS abuse prevention organizations and is subscribed to the NXdomain mailing list. Directi's strong participation in the industry facilitates collaboration with relevant organizations on abuse related issues and ensures that Directi is responsive to new and emerging domain name abuses.

The information shared as a result of this industry participation will be used to identify domain names registered or used for abusive purposes. Information shared may include a list of registrants known to partake in abusive behavior in other TLDs. While presence on such lists will not directly constitute grounds for registrant disqualification, we will investigate domain names registered to those listed registrants and take appropriate action. In addition, information shared regarding practices indicative of abuse will facilitate detection of abuse by our own monitoring activities.

#### 5. PROMOTING AND ENSURING WHOIS ACCURACY

All registrants shall be required, via required language in every Registrar - Registrant Agreement, to provide accurate Registrar Data Directory Services, RDDS (WHOIS) contact details, and to keep those details current. Additionally, Registrars shall have direct responsibility to ensure Whois accuracy through their accreditation contracts with ICANN. Whois Data Reminder Policy or WDRP is an example of a direct Registrar/ICANN contractual obligation to monitor that RDDS (WHOIS) information is accurate and up to date - it includes requiring Registrars to notify their registrants at least once a year to ensure their RDDS (WHOIS) data is correct and up to date.

The threat of inaccurate Whois information significantly hampers the ability to enforce policies in relation to abuse in the TLD by allowing the registrant to remain anonymous. In addition, LEA's rely on the integrity and accuracy of Whois information in their investigative processes to identify and locate wrongdoers.

In recognition of this, we propose that .Web have the following measures to promote RDDS (WHOIS) accuracy.

##### 5.1 WHOIS INACCURACY REPORTING SYSTEM

On the abuse page of our Registry website, we will provide a web based submission service for reporting Whois accuracy issues. Each of these issues will then be resolved as per the process detailed in the previous sections.

##### 5.2 REGULAR MONITORING & SAMPLING

Registrants of randomly selected domain names will be contacted by telephone using the provided Whois information by a member of our team in order to verify the phone number and confirm other Whois information. Where the registrant is not contactable by telephone, alternative contact details (email, postal address) will be used to contact the registrant who must then provide a contact number that is verified by our team. In the event that the registrant is not able to be contacted by any of the methods provided in Whois, the domain name will be cancelled following five contact attempts or one month after the initial contact attempt (based on the premise that a failure to respond is indicative of inaccurate Whois information and is grounds for terminating the registration agreement)

##### 5.3 ANALYSIS OF REGISTRY DATA

We will adopt some processes to identify patterns and correlations indicative

of inaccurate Whois (e.g. repetitive use of fraudulent details).

#### 5.4 PROMOTING ACCURATE WHOIS DATA

WDRP (Whois Data Reminder Policy) implemented by ICANN at the Registrar level, mandates regular e-mail communication to registrants reminding them to keep their whois data accurate and updated. In addition, we will also identify effective mediums to remind registrants to update Whois information and inform them of the ramifications of a failure to respond to our random monthly checks. Ramifications include but are not limited to termination of the registration agreement.

#### 5.5 ENFORCEMENT AT REGISTRAR LEVEL

Registrars will also be contractually required to promptly investigate reports of RDDS (WHOIS) accuracy submitted to them, and resolve each case within a predefined time-frame stipulated through our SLA.

For all cases where inaccuracy is confirmed, we will record the registrar from whom the domain was sourced. We will use this data to capture the ratio of inaccuracies as a percentage of total domains managed, and identify the registrars that seem to attract an abnormally high number of inaccuracy issues. We will then work with those registrars to find potential ways in which they can progressively reduce the number of whois inaccuracy incidents.

The measures to promote Whois accuracy described above strike a balance between the need to maintain the integrity of the Whois service, which facilitates the identification of those taking part in illegal or fraudulent behaviour, and the operating practices of the Registry Operator and Registrars which aim to offer domain names to registrants in an efficient and timely manner.

Awareness among registrants that we will actively take steps to maintain the accuracy of Whois information mitigates the potential for abuse in the TLD. It deters abusive behaviour given that registrants may be identified, located and held liable for all actions in relation to their domain name.

#### 5.6 PROXY / PRIVACY PROTECTION

We have designed a policy that will maximize the legitimate use of proxy and privacy services, and will minimize use by criminals and abusers.

.Web will allow the use of proxy and privacy services, where permitted by ICANN policies and requirements. These services have legitimate uses. Millions of registrants use them to protect their privacy and personal data from spammers and other parties that mine zone files and RDDS (WHOIS) data.

It is undeniable that criminals also use whois proxy services, to hide their true identities. To deter that practice, our policy will require that:

- \* Registrants must use only a privacy/proxy service operated, contracted or owned by the domain's sponsoring registrar, and cannot use third-party proxy services unaffiliated with the domain's sponsoring registrar. This means that a domain's sponsoring registrar will always be in possession of the underlying contact data.

- \*. Registrars and resellers must provide the underlying registrant information to the registry operator upon request, and/or upon a legitimate law-enforcement request, within 24 hours. The registry operator will keep this data confidential, unless #3 below applies.

- \* Registrars and resellers must remove the proxy protection and publish the underlying registrant information in the RDDS (WHOIS) if it is determined by the registry operator and/or the registrar that the registrant has breached any terms of service, such as anti-abuse policies.

The registrar obligations outlined above shall apply with equal force to all registrations sponsored by a registrar, whether those registrations were placed directly with the registrar or through a reseller.

These conditions will be implemented contractually by inclusion of corresponding clauses in the RRA as well as being published on the abuse page of our Registry website. Individuals and organisations will be encouraged through our abuse page to report any domain names they believe violate the restriction on the availability of proxy registrations, following which appropriate action may be taken by us. Publication of these conditions on the abuse page of our Registry website ensures that registrants are aware that despite utilisation of a proxy registration service, actual Whois information will be provided to LEA upon request in order to hold registrants liable for all actions in relation to their domain name. The certainty of Whois disclosure of domain names which draw the attention of LEA, deters those seeking to register domain names for abusive purposes.

## 6. CONTROLS FOR PROPER ACCESS TO DOMAIN FUNCTIONS

We realize that registrants often do not willfully use their domain names for abusive purposes, but domain names end up being compromised because of a lapse in security. Though this cannot always be controlled or mitigated by the registry, we are nevertheless committed to ensure that adequate safeguards are implemented to prevent domain names from being compromised and thereby making them prone to abuse.

### 6.1 MULTI-FACTOR AUTHENTICATION AND SECURE CONNECTIVITY FOR REGISTRARS

Through the contractual agreement with the registry, registrars will be expected to develop and employ in their domain name registration business, all necessary technology and restrictions to ensure that their connection to the registry is secure. All data exchanged between the registrar's system and the registry shall be protected to avoid unintended disclosure of information. Each EPP session shall be authenticated and encrypted using two-way secure socket layer ("SSL") protocol. Registrars will also agree to authenticate every EPP client connection with the registry using both an X.509 server certificate issued by a commercial Certification Authority identified by the registry and their registrar password, disclosed only to their respective employees on a need-to-know basis. Registrars will also access the SRS Web interface by utilizing an additional two-factor authentication token. Further details on this is provided in the response to Question 24 and 25

### 6.2 ENFORCEMENT OF STRONG AUTHCODES

Every domain name will have a strong authorization (authinfo) code, composed of alphabets, numerals, and special characters. An inter-registrar domain name transfer will not be permitted unless the registrant provides this authorization code at the time of executing the transfer process.

### 6.3 NOTIFICATION FOR EVERY UPDATE

We plan to notify the domain name holder upon any update made to a domain name. The notification will be committed through email to either or both of the registrant and technical contact of the domain name.

### 6.4 REGISTRY LOCK

Certain mission-critical domain names such as transactional sites, email systems and site supporting applications may warrant a higher level of security. 'Registry locking' is a feature which allows registrants to prohibit any updates at the Registry Operator level. This service will be available programmatically via EPP, so all registrars will be able to offer it in real-time to their registrants. The feature will prevent unintentional transfer,

modification or deletion of the domain name, and mitigates the potential for abuse by prohibiting any unauthorised updates that may be associated with fraudulent behaviour. For example, an attacker may update name servers of a mission critical domain name, thereby redirecting customers to an illegitimate website without actually transferring control of the domain name. This is described in detail in our response to Question 27

## 6.5 AWARENESS PROGRAMS

In accordance with our commitment to operating a secure and reliable TLD, we will attempt to improve registrant awareness of the threats of domain name hijacking, registrant impersonation and fraud, and emphasize the need for registrants to keep registration information accurate and confidential. Awareness will be raised by:

- \* Publishing the necessary information on the Abuse page of our Registry website in the form of videos, presentations and FAQs;
- \* Developing and providing to registrants, resellers and Registrars Best Common Practices that describe appropriate use and assignment of domain auth info codes and risks of misuse when the uniqueness property of this domain name password is not preserved.

## 7. RESOURCING PLANS

### 7.1 PERSONNEL

Functions described herein will be performed by -

- \* Directi Group staff under contract with us -
- \*\* Abuse & Compliance Team
- \* Dispute Resolution Service Providers that are selected wrt UDRP and SDRP

Directi Group possesses an exemplary track record of diffusing abuse on 4 million plus domains under their Registrar. The abuse mitigation function of our Registry will be handled by the same team that currently manages this process for the registrar businesses.

The existing compliance team comprises of:

- \* 1 Compliance Manager
- \* 1 Team Supervisor
- \* 4 Cyber Security Analysts
- \* 9 Compliance Officers

The compliance function is staffed on a 24/7/365 basis and capable of handling up to a peak of 52,800 unique abuse incidents per year. Each incident by itself can relate to a few to hundreds of domain names.

While this team is trained to investigate and verify all types of issues, they can also fall back on support from our technical staff when required. Similarly, abuse cases following new or unexpected parameters may also be escalated to legal support staff for expert counsel.

Our estimates of resource sizing are directly derived from the abuse case incident volumes currently experienced. On a base of 4 million domains across our Registrar businesses within Directi, each year we experience approximately:

- \* 6000 malware related abuses
- \* 1600 phishing abuses
- \* 1200 spam cases
- \* 600 pharmacy related abuses
- \* 5600 large botnet related abuse cases annually

This averages an incident rate of approximately 15,000 cases of abuse per year or 3.75 incidents per 1000 names



Since registries delegate a large portion of their abuse responsibilities to registrars, it is fair to assume that our registry's abuse incident ratio will be lower than what we experience as registrars. In fact, in our case 2/3 categories of incidents will be delegated to the registrar and our direct involvement is expected in only 25%-35% of all incidents. However, given our proactive approach, importance on ensuring a clean and secure namespace, and aggressive SLAs, we choose to be conservative by assuming that we will be involved in 75% of all incidents.

Based on our projections, we expect .Web to reach 471,482 domain names at the end of the 3rd year. Extrapolating from our current rate of 3.75 incidents per 1000 names, we can expect around 1,768 abuse incidents yearly and be involved in 1,326 (75%) of them. Including the estimated 78 RPM incidents (details in our response to Q29), brings our total projected incident count to 1,404. This conservative estimate also accounts for the aggressive SLAs at multiple levels, law enforcement interfacing and having a single POC available at all times.

The Compliance desk works as a centralized team and all team members are responsible for all abuse complaints across all businesses of Directi. Costs of the Compliance team are then allocated to each business based on the % utilization of the compliance team by each business. We have assumed 25% of 2 compliance officers' time towards .Web. Given that our 15 people team has the capacity to handle 52,800 incidents yearly, 2 officers with 25% of their time, will have a total capacity to handle 1,760 incidents annually. . It is important to point out that 25% of the 2 officers is merely a cost allocation method and in actuality all 15 members and more of the Compliance team will be available to resolve abuse issues for TLD.

Our planning provides us redundant capacity of 250%+ in Y1, 85% in Y2 and 25% in Y3, to handle both abuse as well as RPM related cases such as those involving URS. This leaves substantial headroom for rapid growth of domains under management, or a sudden surge in abuse incident rates per domain.

It is also important to note that there exists some economies of scale in our operations since a large number of these cases are dealt with in bulk, or large batches, as they relate to the same instigator(s).

The abuse team has a structured training program in place which enables them to rapidly scale-up resources when required. Typically a team of recruits are given four weeks of training and two weeks on the floor before they are fully activated.

Given the rapid growth rate of Directi businesses, Directi will continue to hire and maintain a sizable buffer over and above anticipated growth.

## 7.2 FINANCIAL CONSIDERATIONS

The usage of Directi Group's staff is included in our contract with Directi attached to Q46 ('Q46\_References: Service and Facilities Commitment Agreement'). This cost is shown in the financial answers.

This completes our response to Q28.

## 29. Rights Protection Mechanisms

DotWeb Inc. is a wholly owned subsidiary within the Directi Group. The Directi Group runs various businesses including several ICANN Accredited Domain Registrars (including ResellerClub.com and BigRock.com) and Web Hosting companies. At Directi, through our decade long experience as a domain name registrar, we have consciously strived to ensure that domain registrations

through our platform do not violate the intellectual property or other rights of any person or organization.

Our experience as a domain name registrar gives us insight into the necessity and importance of rights protection, and the mechanisms that must be employed to assure it. With .Web, we shall leverage our experience to implement a comprehensive set of policies and procedures that will uphold intellectual property rights to the greatest possible extent.

The protection of trademark rights is a core goal of .Web. .Web will have a professional plan for rights protection. It will incorporate best practices of existing TLDs, going above and beyond the ICANN mandated RPs to prevent abusive registrations and rapidly take-down abuse when it does occur.

## 1. PREVENT ABUSIVE REGISTRATIONS

We will put into place the following measures to ensure prevention of registrations that infringe the IP rights of others

### 1.1 SUNRISE PROCESS

Our sunrise registration service will provide trademark holders with at least a 30-day priority period in which to register their trademarks as domain names.

#### Sunrise Timeline -

Day 1: Single sunrise round opens

Day 30: Sunrise round closes

Day 31: Sunrise allocation begins and Sunrise period ends

#### 1.1.1 SUNRISE POLICY SUMMARY AND SDRP SUMMARY

This section provides a summary of our Sunrise Policy and SDRP. We have formulated our policies and processes based on existing guidance concerning Sunrise and TMCH provided by ICANN. Any additional guidance in the future that requires changes to our process and policies will be implemented.

Through our Sunrise Policy we will offer at least one 30-day sunrise round in which trademark holders satisfying the Sunrise eligibility requirements proposed in the 'gTLD Applicant Guidebook' will be eligible to apply for a domain name. This sunrise period will be the first opportunity for registration of domain names in .Web. Trademarks upon which sunrise applications are based must meet the criteria defined in the 'gTLD Applicant Guidebook' and be supported by an entry in the TMCH.

Sunrise allocation will start at the end of the 30-day sunrise period. If one validated application is received for a domain name, the same will be allocated to the applicant in the 10-day period following the end of the sunrise period. Where multiple validated applications are received for a domain name, the name will be allocated by auction. Domain names registered during the sunrise period will have a min. term of 2 yrs.

We will adopt a Sunrise Dispute Resolution Policy ('SDRP') to allow any party to raise a challenge on the four grounds identified in the 'gTLD Applicant Guidebook'. All registrants will be required to submit to proceedings under the SDRP. SDRP claims may be raised at any time after registration of a domain name.

#### 1.1.2 IMPLEMENTATION

##### 1.1.2.1 SUNRISE PRICING

We plan to charge a non-refundable Sunrise application fee or validation fee of \$80 for every Sunrise application. We have arrived at the fee to offset the cost of the trademark validation and other administrative over-heads.

#### 1.1.2.2 SUNRISE IMPLEMENTATION PLAN

1. Prior to sunrise, trademark holders should apply for inclusion of their marks in the TMCH database.
  2. Our Sunrise Policy and SDRP will be published on our website.
  3. A trademark holder satisfying the sunrise eligibility requirements will pay the non-refundable sunrise application fee and submit its application corresponding to its TMCH entry to a registrar along with evidence of the corresponding TMCH entry.
  4. Registrars will send the sunrise applications to ARI. They will be charged the application fee at this time.
  5. ARI will perform standard checks to ensure that the domain name is technically valid and hold the application for subsequent allocation.
  6. Upon conclusion of the 30-day sunrise period, ARI will compile a list of applied-for names and reserve these from registration in land rush and general availability.
  7. Sometime during this process ARI or the registrar (as prescribed) will identify all sunrise applications which constitute an 'Identical Match' (as defined in the 'gTLD Applicant Guidebook') with a TMCH entry and provide notice to the holders of the filing of a sunrise registration.
  8. Where a single sunrise application exists for a particular domain name ARI will enable the sponsoring registrar to CREATE the domain name and we will charge the sunrise registration fee to the registrar.
  9. Where multiple sunrise applications exist for a domain name, ARI will compile and communicate to a 3rd-party auction services provider appointed by us a list of competing applicants, who will be invited to participate in an auction for the domain name.
  10. The auction services provider will facilitate the auction process and upon completion of the auction will notify all participants of the outcome and collect the auction payment from the winning participant.
  11. Upon payment of the auction bid, the auction services provider will communicate to ARI the details of the winning auction participant and will submit the revenue collected to ARI.
- ARI will validate the communication from the auction services provider and enable the sponsoring registrar to CREATE the domain name.

#### 1.1.1.3 SDRP IMPLEMENTATION PLAN

When a domain is awarded and granted to a registrant, that domain will be available for lookup in the public WHOIS.

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

SDRP filings will be handled by an appropriate service provider as per ICANN guidance and policy.

#### 1.1.1.4 IMPLEMENTATION THROUGH CONTRACTUAL RELATIONSHIPS

The following features of the Sunrise and SDRP implementation plans described above will be executed by the inclusion of corresponding clauses in our RRA, which will require inclusion in registrars' Domain Name Registration Agreements:

- \* By making a sunrise application the applicant agrees to purchase the domain name if that name is allocated to the applicant.
- \* The sunrise application fee is non-refundable.
- \* All sunrise applicants must submit to proceedings under the SDRP.

## 1.2 TRADEMARK CLAIMS SERVICE

For at least 60 days during general availability we will offer the trademark claims service as described in the 'gTLD Application Guidebook'.

### 1.2.1 IMPLEMENTATION

#### 1.2.1.1 TRADEMARK CLAIMS SERVICE IMPLEMENTATION PLAN

This process will be executed for at least the first 60 days of general availability:

1. an applicant will make an application to a registrar for a domain name.
2. Registrars will be required to communicate land rush application information to our registry backend provider - ARI.
3. ARI or Registrars (as prescribed) will interface with the TMCH to determine whether an applied-for domain name constitutes an 'Identical Match' with a trademark in the TMCH. If an 'Identical Match' is identified, the registrar will provide to the land rush applicant a Trademark Claims Notice in the form prescribed by the 'gTLD Applicant Guidebook'. Following receipt of this notice a land rush applicant must communicate to the registrar its decision either to proceed with or abandon the registration.
4. ARI or Registrar (as prescribed) will interface with the TMCH to promptly notify relevant mark holders of the registration of a domain name constituting an 'Identical Match' to their TMCH entry.

#### 1.2.1.2 IMPLEMENTATION THROUGH CONTRACTUAL RELATIONSHIPS

The following features of our Trademark Claims Service Implementation Plan described above will be executed by the inclusion of corresponding clauses in our RRA:

- \* Registrars must comply with the TMCH as required by ICANN and the TMCH Service Provider/s.
- \* Registrars must not in their provision of the trademark claims service make use of any other trademark information aggregation, notification or validation service other than the TMCH.
- \* In order to prevent a chilling effect on registration, registrars must ensure that land rush applicants are not prevented from registering domain names considered an 'Identical Match' with a mark in the TMCH.
- \* Registrars must provide clear notice in the specific form provided by the 'gTLD Applicant Guidebook' to the prospective registrant of relevant entries in the TMCH.
- \* Registrars must interface with the TMCH as prescribed to relevant mark holders of the registration of a domain name constituting an 'Identical Match' to their TMCH entry.

## 2. ONGOING RIGHTS PROTECTION AND ABUSE PREVENTION

Below we describe ongoing RPMs which we will implement to mitigate cybersquatting and other types of abusive behaviour such as phishing and pharming.

### 2.1 UNIFORM RAPID SUSPENSION (URS)

The URS (Uniform Rapid Suspension) procedure is a new RPM the implementation of which is mandated in all new gTLDs. Understanding that a fundamental aim of the URS is expediency, all of the steps in our Implementation Plan below will be undertaken as soon as practical but without compromising security or accuracy.

#### 2.1.1 IMPLEMENTATION

##### 2.1.1.1 URS IMPLEMENTATION PLAN

1. We will provide to each URS provider an email address to which URS-related correspondence can be sent. On an ongoing basis, our compliance desk will monitor this email address for receipt of communications from URS providers,

including the Notice of Complaint, Notice of Default, URS Determination, Notice of Appeal and Appeal Panel Findings.

2. We will validate correspondence from a URS provider to ensure that it originates from the URS Provider.
3. We will within 24 hours of receipt of a URS Notice of Complaint lock the domain name/s the subject of that complaint by restricting all changes to the registration data, including transfer and deletion of the domain name. The domain name will continue to resolve while in this locked status.
4. We will immediately notify the URS provider in the manner requested by the URS provider once the domain name/s have been locked.
5. Upon receipt of a favourable URS Determination we will unlock the domain name and redirect the nameservers to an informational web page provided by the URS provider. While a domain name is locked, our backend provider - ARI - will continue to display all of the WHOIS information of the original registrant except for the redirection of the nameservers and the additional statement that the domain name will not be able to be transferred, deleted or modified for the life of the registration.
6. Upon receipt of notification from the URS provider of termination of a URS proceeding we will promptly unlock the domain name and return full control to the registrant.
7. Where a default has occurred (because a registrant has not submitted an answer to a URS complaint in accordance with the 'gTLD Applicant Guidebook') and a Determination has been made in favour of the complainant, in the event that we receive notice from a URS provider that a Response has been filed in accordance with the 'gTLD Applicant Guidebook', we will as soon as practical restore a domain name to resolve to the original IP address while preserving the domain's locked status until a Determination from de novo review is notified to us.
8. We will ensure that no changes are made to the resolution of a registration the subject of a successful URS Determination until expiry of the registration or the additional registration year unless otherwise instructed by a UDRP provider.
9. We will make available to successful URS complainants an optional extension of the registration period for one additional year.

#### 2.1.1.2 IMPLEMENTATION OF THE URS THROUGH CONTRACTUAL RELATIONSHIPS

The following features of our URS Implementation Plan described above will be executed by the inclusion of corresponding clauses in our RRA:

- \* In the event that a Registrant does not submit an answer to a URS complaint in accordance with the 'gTLD Applicant Guidebook', registrars must prevent registrants from making changes to the WHOIS information of a registration while it is in URS default.
- \* Registrars must prevent changes to a domain name when a domain is in locked status to ensure that both the Registrar's systems and Registry's systems contain the same information for the locked domain name.
- \* Registrars must not take any action relating to a URS proceeding except as in accordance with a validated communication from us or a URS provider.

#### 2.2 UDRP

The UDRP (Uniform Domain Name Dispute Resolution Policy) is applicable to domain name registrations in all new gTLDs. It is available to parties with rights in valid and enforceable trade or service marks and is actionable on proof of all of the following three grounds:

1. The registrant's domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights.
2. The registrant has no rights or legitimate interests in respect of the domain name.
3. The registrant's domain name has been registered and is being used in bad faith.

The remedies offered by the UDRP are cancellation of a domain name or transfer

of a domain name registration to a successful UDRP claimant.

### 2.2.1 IMPLEMENTATION

#### 2.2.1.1 UDRP IMPLEMENTATION PLAN

We have two responsibilities in order to facilitate registrars' implementation of the UDRP -

1. Our backend provider - ARI - will maintain awareness of UDRP requirements and be capable of taking action when required and sufficiently skilled and flexible to respond to any changes to UDRP policy arising from future consensus policy reviews.
2. We will provide EPP and the SRS web interfaces to enable registrars to perform required UDRP functions in accordance with the Policy on Transfer of Registrations between Registrars.

#### 2.2.1.2 IMPLEMENTATION OF THE UDRP THROUGH CONTRACTUAL RELATIONSHIPS

The UDRP is applicable to domain name registrations in all new gTLDs by force of a contractual obligation on Registry Operators to use only ICANN-accredited registrars, who in turn are contractually required to incorporate the UDRP in their Domain Name Registration Agreements.

### 3. ADDITIONAL RIGHTS PROTECTION MECHANISMS

The protection of trademark rights is a core goal of .Web. Our Right Protection Mechanisms, policies and procedures go significantly above and beyond the minimum mandated RPMs to prevent abusive registrations, rapidly take-down abuse when it occurs, and foster a clean namespace for .Web

This section describes several other RPMs that .Web will implement that exceed the minimum requirements for RPMs and align with our goal of creating a namespace that provides maximum protection to trademark holders.

#### 3.1 OPTIONAL TRADEMARK DECLARATION

This is a unique feature of our .Web TLD. During General Availability, we will continue to make available, the EPP Trademark extension fields that are provided during sunrise. Registrants will be able to specify their IPR details against their domain names even after sunrise. The fields will include - word mark, registration number, applied date, registration date, jurisdiction, class. These fields will be editable by the Registrant and visible in Whois.

The ability for a Registrant to voluntarily declare Trademark data even during general availability will reduce potential confusion amongst mark holders and the general public and reduce unnecessary UDRP procedures.

#### 3.2 PROFILING & BLACKLISTING

This process, currently in practice for our registrar businesses within the Directi Group, is used for gathering intelligence on known offenders. We maintain abuse ratios for each of the 1,000,000 plus registrants and 65,000 plus resellers who use Directi.

Experience has enabled us to use these ratios accurately to uncover registrants who are known and repeated offenders. Expert offenders rarely reuse the same registrant profile and often maintain a myriad number of profiles to mask their true identity. Through pattern mapping we try and group registrant profiles that we believe belong to the same operator.

The same process is followed at the reseller level too, to identify those resellers who are knowingly harboring offenders, or are themselves involved in abuse.

When a registrant profile is confirmed to be involved in organized abuse, including but not limited to cybersquatting, phishing, pharming etc., our immediate step is to suspend that customer's control over his abusive domain portfolio. Our compliance team then carefully analyzes each domain name to identify those which are abusive and not already taken-down. The necessary action is undertaken to diffuse any ongoing abuse.

We plan to adopt the 'Profiling and Blacklisting' process within our registry operations. Since all of our compliance resources will be trained and experienced in running this process, its implementation into .Web will be simple. Specifics of this policy and process, as it applies to our registry business, will be drawn out.

### 3.3 PROACTIVE DOMAIN QUALITY ASSURANCE

As a preventive safeguard against abusive domain registration, we follow a consistent review process for domain registrations on our registrar, where a sample of newly registered domain names are analyzed for potential abusive activity. Coupled with our profiling process (described above), it enables us to take proactive measures against domain names that are registered solely to perpetrate malicious activities such as phishing, or otherwise infringe on the rights of others. This helps us curb abusive activity before it can affect too many Internet users. We shall seek to implement similar safeguards for .Web, and encourage registrars to incorporate this practice as part of their abuse mitigation processes.

### 3.4 INDUSTRY COLLABORATION

#### 3.4.1 ACTIVE INVOLVEMENT WITH SECURITY AGENCIES

In order to mitigate abuse of domain names on our registrar business, our abuse team has active involvement in helping security vendors and researchers fight domain abuse. They provide us a constant feed of abuse instances and help us identify domain names involved in activities like phishing or pharming. Some of the prominent organizations we work with include PhishLabs (phishing), LegitScript (illegal pharmaceutical distribution), Artists Against 419 (financial scams), Knujon (spam) etc. We will leverage these relationships to ensure oversight for all domain names registered within .Web.

#### 3.4.2 APWG REVIEW

Every six months, the Anti-Phishing Working Group (APWG) publishes its latest Global Phishing Survey [See <http://www.apwg.org/resources.html#apwg>]. This study contains an analysis of phishing per TLD. We will review the performance of our anti-abuse program against the APWG reports, and other metrics created by the security community. We will work closely with APWG to combat phishing within .Web

#### 3.4.3. MESSAGE OF ZERO TOLERANCE

Our Anti-Abuse Policy will put Registrants on notice of the ways in which we will identify and respond to abuse and serve as a deterrent to those seeking to register and use domain names for abusive purposes. The policy will be made easily accessible on the Abuse page of our Registry website which will be accessible and have clear links from the home page along with FAQs and contact information for reporting abuse.

The Directi Group has vast experience in minimizing abusive registrations. Our zero tolerance procedures and aggressive proactive takedown measures as a Domain Registrar have resulted in a white-hat reputation discouraging abusive registrations to begin with. We intend on following the same approach with respect to Registry operations for .Web. Our proactive abuse procedures are geared towards building a reputation that discourages miscreants and malicious intent. Once it is known that abusive registrations and registrations in

violation of our policies are suspended rapidly, this will directly result in discouraging abusive registrations and creating a clean namespace. While following this path will mean a higher compliance and abuse vigilance cost for us, we believe this effort will pay us long term rewards through abusers keeping away and .Web becoming recognized as a reputable namespace.

#### 4. REDUCING PHISHING AND PHARMING

All of the measures we have described in the preceding sections significantly reduce phishing and pharming within .Web. These include RPMS like URS and UDRP.

Over and above this our coordination with APWG, Industry Collaboration, Profiling and Blacklisting processes and Proactive measures described in Section 3 above will go a long way in ensuring a clean namespace for .Web and considerably reduced phishing and pharming activities.

#### 5. PREVENTING TRADEMARK INFRINGEMENT IN OPERATING THE REGISTRY

We take seriously our responsibilities in running a registry and we understand that while offering a sunrise registration service and the trademark claims service during start-up of our TLD and the URS and UDRP on an ongoing basis serves to minimise abuse by others, this does not necessarily serve to minimise trademark infringement in our operation of the TLD. This responsibility is now clearly expressed and imposed upon registries through the new Trademark PDDRP [Post-Delegation Dispute Resolution Procedure], which targets infringement arising from the Registry Operator's manner of operation or use of its TLD.

Whilst we will as required under the Registry Agreement agree to participate in all Trademark PDDRP procedures and be bound by the resulting determinations, we will also have in place procedures to identify and address potential conflicts before they escalate to the stage of a Trademark PDDRP claim.

##### 5.1 IMPLEMENTATION

1. We will notify to the Trademark PDDRP provider's contact details to which communications regarding the Trademark PDDRP can be sent.
2. We will publish our Anti-Abuse Policy on a website specifically dedicated to abuse handling in our TLD.
3. Using the single abuse point of contact discussed in detail in our response to Q28, a complainant can notify us of its belief that that one or more of its marks have been infringed and harm caused by our manner of operation or use of our TLD
4. We will receive complaints submitted through the single abuse point of contact.
5. The Compliance Team will acknowledge receipt of the complaint and commence investigation of the subject matter of the complaint and good faith negotiations with the complainant in accordance with the 'gTLD Applicant Guidebook'.
6. On an ongoing basis, our Compliance Team will monitor the email address notified to the Trademark PDDRP provider's for all communications from the Trademark PDDRP provider, including the threshold determination, Trademark PDDRP complaint, complainant's reply, notice of default, expert panel determinations, notice of appeal and determinations of an appeal panel.
7. In the event that a complaint cannot be resolved and a Trademark PDDRP claim is made, we will do the following:

- \* File a response to the complaint in accordance with Trademark PDDRP policy section 10 (thus avoiding, whenever possible, a default situation).

- \* Where appropriate, make and communicate to the Trademark PDDRP provider decisions regarding the Trademark PDDRP proceeding, including whether to request a three-person Trademark PDDRP Expert Panel, request discovery, request and attend a hearing, request a de novo appeal, challenge an ICANN-imposed Trademark PDDRP remedy, initiate dispute resolution under the Registry Agreement, or commence litigation in the event of a dispute arising under the



Trademark PDDRP.

\* Where appropriate, undertake discovery in compliance with Trademark PDDRP policy section 15, attend hearings raised under section 16 if required, and gather evidence in compliance with sections 20.5 and 20.6.

8. We will upon notification of an Expert Panel finding in favour of the Claimant (Trademark PDDRP policy section 14.3), reimburse the Trademark PDDRP Claimant.

9. We will implement any remedial measures recommended by the expert panel pursuant to Trademark PDDRP policy and take all steps necessary to cure violations found by the expert panel and notified by ICANN.

## 6. RESOURCING PLANS

### 6.1 PERSONNEL

Functions described herein will be performed by:

\* Directi Group Abuse and Compliance team under contract with us -

\*\* Overseeing Sunrise process

\*\* URS

\*\* Abuse complaints concerning RPM

\* ARI's backend Registry

\* Service Providers that are selected wrt TMCH, UDRP, URS and SDRP

\* Director of Technology at .Web & Account Management staff at .Web

\*\* Overseeing Sunrise process

\*\* Communication of the sunrise process to Registrars

Directi Group possesses an exemplary track record of diffusing abuse on 4 million plus domains under their Registrar business. The Rights protection and abuse mitigation function of our Registry will be handled by the same team that currently manages this process for the registrar businesses.

The existing compliance team comprises of:

\* 1 Compliance Manager

\* 1 Team Supervisor

\* 4 Cyber Security Analysts

\* 9 Compliance Officers

The compliance function is staffed on a 24/7/365 basis and capable of handling up to a peak of 52,800 unique abuse incidents per year. Each incident by itself can relate to a few to hundreds of domain names.

While this team is trained to investigate and verify all types of issues, they can also fall back on support from our technical staff when required.

Similarly, abuse cases following new or unexpected parameters may also be escalated to legal support staff for expert counsel.

Our estimates of resource sizing are directly derived from the abuse case incident volumes currently experienced. On a base of 4 million domains as a Registrar, we experience approximately the following incidents per year:

\* UDRP Cases - 200

\* Other RPM incidents - 20 cases

This averages an incident rate of approximately 220 cases of abuse per year or 0.055 incidents per 1000 names. Given that this is based on a more mature base of names, it would be prudent to assume a higher rate of activity for .Web. Based on our experience we have assumed the increase in activity rate to be three fold (300% of the current rate) and increase it to 0.165 per 1000 names.

Based on our projections, we expect .Web to reach 471,482 domain names at the end of the third year. Extrapolating from our estimated rate of 0.165 incidents

per 1000 names, we can expect around 78 incidents yearly. Including the estimated 1,326 Abuse incidents that the registry will handle (details in our response to Q28), brings our total projected incident count to 1404.

The Compliance desk works as a centralized team and all team members are responsible for all abuse complaints across all businesses of Directi. Costs of the Compliance team are then allocated to each business based on the % utilization of the compliance team by each business. We have assumed 25% of 2 compliance officers' time towards .Web. Given that our 15 people team has the capacity to handle 52,800 incidents yearly, 2 officers with 25% of their time, will have a total capacity to handle 1,760 incidents annually which is more than adequate for the Registry. It is important to point out that 25% of the 2 officers is merely a cost allocation method and in actuality all 15 members and more of the Compliance team will be available to resolve abuse issues for TLD.

Our planning provides us redundant capacity of 250%+ in Y1, 85% in Y2 and 25% in Y3, to handle both abuse as well as RPM related cases such as those involving URS. This leaves substantial headroom for rapid growth of domains under management, or a sudden surge in abuse incident rates per domain.

It is also important to note that there exist some economies of scale in our operations since a large number of these cases are dealt with in bulk, or large batches, as they relate to the same instigator(s).

The Abuse and Compliance team has a structured training program in place which enables them to rapidly scale-up resources when required. Typically a team of recruits are given four weeks of training and two weeks on the floor before they are fully activated.

Given our rapid growth rate and business expansion plans, we will continue to hire and maintain a sizable buffer over and above anticipated growth.

## 6.2 FINANCIAL COSTS

The usage of Directi Group's staff is included in our contract with Directi attached to Q46. This cost is shown in the financial answers.

This completes our response to Q29.

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

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q30a - ARI Background & Roles.pdf'. This response describes Security as implemented by ARI under direction from us taking into account any specific needs for this TLD.

### 1. SECURITY POLICY SUMMARY

ARI operates an ISO27001 compliant Information Security Management System (ISMS) for Domain Name Registry Operations; see attachment 'Q30a - SAI Global Certificate of Compliance.pdf'. The ISMS is an organisation-wide system encompassing all levels of Information Security policy, procedure, standards, and records. Full details of all the policies and procedures included in the ISMS are included in the attachment to Question 30b.

#### 1.1 THE ISMS

ARI's ISMS's governing policy:

\* Defines the scope of operations to be managed (Domain Name Registry

Operations).

\* Designates the responsible parties (COO, CTO and Information Security Officer) for governance, Production Support Group for implementation and maintenance, and other departments for supporting services.

\* Requires a complete Risk Assessment (a developed Security Threat Profile for the Service - in this case registry services for the TLD - and a Risk Analysis tracing threats and vulnerabilities through to Risks) and Risk Treatment Plan (each major risk in the Risk Assessment references the Statement of Applicability indicating controls to be implemented, responsible parties, and the effectiveness metrics for each).

\* Includes a series of major sub policies governing security, which include but are not limited to:

\*\* ICT acceptable use policy and physical security policies.

\*\* PSG Security Policy which outlines the registry operations policies, the management of end-user devices, classification of networks and servers according to the classification of information they contain, networking, server & database configuration and maintenance guidelines, vulnerability and patch management, data integrity controls, access management, penetration testing, third party management, logging and monitoring, and cryptography.

\* Requires ongoing review:

\*\* Of risks, threats, the Risk Treatment Plan, client requirements and commitments, process and policy compliance, process and policy effectiveness, user etc.

\*\* Regular internal and external penetration testing & vulnerability scanning.

\*\* Ad-hoc review raised during normal operations, common sources being change management processes, scheduled maintenance or project debriefs, and security incidents.

\*\* Yearly review cycle which includes both internal and external audits, including external surveillance audits for compliance.

\*\* Additional yearly security controls assessment reviews, which include analysis of the security control implementations themselves (rather than compliance with any particular standard).

\*\* At 24 month intervals, external penetration testing of selected production services.

\*\* Periodic ISO reaccreditation

ARI's ISMS encompasses the following ARI standards:

\* Configuration standards for operating systems, networking devices and databases based on several key publications, including those released by NIST (e.g. SP800-123, SP800-44v2, SP-800-40, SP800-41) and the NSA, staff testing and experience, and vendor supplied standards.

\* Security Incident Classification, which identifies the various classifications of security incidents and events to ensure that events that qualify as security incidents.

\* Information Classification and Handling which specifies the information classification scheme and the specific requirements of handling, labelling, management and destruction for each level of classification.

## 1.2 SECURITY PROCESSES

Processes are used to implement the policies. These include, but are not limited to:

### 1.2.1 CHANGE MANAGEMENT

This includes change management and its sub-processes for access management, software deployment, release of small changes and scheduled maintenance. This process includes:

\* The classification of changes and the flow into sub processes by classification.

\* The release and deployment process for change control into production environments, outlining peer review, testing steps, approval points, checklist sets, staging requirements and communication requirements.

\* The software release and deployment process with its specific testing and staged rollout requirements.

- \* The scheduled maintenance process and its various review points.

#### 1.2.2 INCIDENT MANAGEMENT

This includes incident management process and its sub-process for unplanned outages. These outline:

- \* How incidents are managed through escalation points, recording requirements, communication requirements etc.
- \* The unplanned outage procedure which applies directly to situations where the registry itself or other critical services are unexpectedly offline.

#### 1.2.3 PROBLEM MANAGEMENT

The goal of problem management is to drive long term resolution of underlying causes of incidents. This process centres on finding and resolving the root causes of incidents. It defines escalation points to third parties or other ARI departments such as Development, as well as verification of the solution prior to problem closure.

#### 1.2.4 SECURITY INCIDENT MANAGEMENT

This process deals with the specific handling of security incidents. It outlines the requirements and decision points for managing security incidents. Decision points, escalation points to senior management and authorities are defined, along with evidence-gathering requirements, classification of incidents and incident logging.

#### 1.2.5 ACCESS MANAGEMENT

This process handles all access changes to systems. HR must authorize new users, and access changes are authorized by departmental managers and approved by the Information Security Officer.

When staff leave or significantly change roles, a separation process is followed which ensures all access that may have been granted during their employment (not just their initially granted access) is checked and where appropriate, revoked.

Finally, quarterly review of all access is undertaken by the ISO, reviewing and approving or rejecting (with an action ticket) as appropriate.

### 2. ARI's SECURITY INFRASTRUCTURE SOLUTIONS

ARI has developed a layered approach to IT security infrastructure. At a high level, some of the layers are as follows:

- \* DDoS countermeasures are employed outside ARI networks. These include routing traps for DDoS attacks, upstream provider intervention, private peering links and third party filtering services.

- \* Routing controls at the edge of the network at a minimum ensures that only traffic with valid routing passes into ARI networks.

- \* Over-provisioning and burstable network capabilities help protect against DoS and DDoS attacks.

- \* Network firewalls filter any traffic not pre-defined by network engineering staff as valid.

- \* Application layer firewalls then analyse application level traffic and filter any suspicious traffic. Examples of these would be an attempt at SQL injection, script injection, cross-site scripting, or session hijacking.

- \* Server firewalls on front-end servers again filter out any traffic that is not strictly defined by systems administrators during configuration as valid traffic.

- \* Only applications strictly necessary for services are running on the servers.

- \* These applications are kept up-to-date with the latest security patches, as are all of the security infrastructure components that protect them or that they run on.

- \* ARI infrastructure is penetration-tested by external tools and contracted security professionals for vulnerabilities to known exploits.

- \* ARI applications are designed, coded and tested to security standards such as OWASP and penetration-tested for vulnerabilities to common classes of exploits by external tools and contracted security professionals.
- \* ARI configures SELinux on its production servers. Specific details of this configuration is confidential; essentially any compromised application is extremely limited in what it can do.
- \* Monitoring is used to detect security incidents at all layers of the security model. Specifically
  - \*\* Network Intrusion Detection systems are employed to monitor ARI networks for suspicious traffic.
  - \*\* ARI maintains its own host-based Intrusion Detection system based on tripwire, which has now undergone four years of development. Specific details are confidential, but in summary, the system can detect any unusual activity with respect to configuration, program files, program processes, users, or network traffic.
  - \*\* More generic monitoring systems are used as indicators of security incidents. Any behaviour outside the norm across over 1,100 individual application, database, systems, network and environmental checks is investigated.
- \* Capacity management components of the monitoring suite are also used to detect and classify security incidents. Some examples are:
  - \*\* Network traffic counts, packet counts and specific application query counts.
  - \*\* Long term trend data on network traffic vs. specific incident windows.
  - \*\* CPU, Storage, Memory and Process monitors on servers.
- \* A second layer of hardware firewalling separates application and middle tier servers from database servers.
- \* Applications only have as much access to database information as is required to perform their function.
- \* Finally, database servers have their own security standards, including server-based firewalls, vulnerability management for operating system and RDBMS software, and encryption of critical data.

## 2.1 PHYSICAL SECURITY INFRASTRUCTURE

ARI maintains a series of physical security infrastructure measures including but not limited to biometric and physical key access control to secured areas and security camera recording, alarm systems and monitoring.

## 3. COMMITMENTS TO REGISTRANTS

We commit to the following:

- \* Safeguarding the confidentiality, integrity and availability of registrant's data.
- \* Compliance with the relevant regulation and legislation with respect to privacy.
- \* Working with law enforcement where appropriate in response to illegal activity or at the request of law enforcement agencies.
- \* Maintaining a best practice information security management system that continues to be ISO27001-compliant.
- \* Validating requests from external parties requesting data or changes to the registry to ensure the identity of these parties and that their request is appropriate. This includes requests from ICANN.
- \* That access to DNS and contact administrative facilities requires multi-factor authentication by the Registrar on behalf of the registrant.
- \*\* That Registry data cannot be manipulated in any fashion other than those permitted to authenticated Registrars using the EPP or the SRS web interface. Authenticated Registrars can only access Registry data of domain names sponsored by them.
- \*\* A Domain transfer can only be done by utilizing the AUTH CODE provided to the Domain Registrant.
- \* That emergency procedures are in place and tested to respond to extraordinary events affecting the integrity, confidentiality or availability of data within the registry.

#### 4. AUGMENTED LEVEL OF SECURITY

This TLD is a generic TLD and as such requires security considerations that are commensurate with its purpose. Our goal with this TLD is to provide registrants with adequate protections against unauthorized changes to their names, without making the registration process too onerous and thus increasing costs.

The following attributes describe the security with respect to the TLD:

- \* ARI, follows the highest security standards with respect to its Registry Operations. ARI is ISO 27001 certified and has been in the business of providing a Registry backend for 10 years. ARI have confirmed their adherence to all of the security standards as described in this application.

- \* Registrant will only be permitted to make changes to their domain name after authenticating to their Registrar.

- \* Registrants will only be able to access all interfaces for domain registration and management via HTTPS. A reputed digital certificate vendor will provide the SSL certificate of the secure site.

- \* Registrar identity will be manually verified before they are accredited within this TLD. This will include verification of corporate identity, identity of individuals involved / mentioned, and verification of contact information

- \* Registrars will only be permitted to connect with the SRS via EPP after a multi-factor authentication that validates their digital identity. This is described further ahead.

- \* Registrars will only be permitted to use a certificate signed by ARI to connect with the Registry systems. Self-signed certificates will not be permitted.

- \* The Registry is DNSSEC enabled and the TLD zone will be DNSSEC enabled. This is described in detail in our response to question 43.

- \* Registrar access to all Registry Systems will be via TLS and secured with multi-factor authentication. This is described in detail in our responses to Question 24 and Question 25.

Where these requirements put controls on Registrars these will be enforced through the RRA.

#### 5. RESOURCES

This function will be performed by ARI. The following resources are allocated to performing the tasks required to deliver the services described:

- \* Executive Management Team (4 staff)

- \* Production Support Group (27 staff)

ARI has ten years' experience designing, developing, deploying, securing and operating critical Registry systems, as well as TLD consulting and technology leadership.

As a technology company, ARI's senior management are technology and methodology leaders in their respective fields who ensure the organization maintains a focus on technical excellence and hiring, training and staff management.

Executive Management are heavily involved in ensuring security standards are met and that continued review and improvement is constantly undertaken. This includes the:

- \* Chief Operations Officer

- \* Chief Technology Officer

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q30a - ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system.

Based on past experience ARI estimates that the existing staff is adequate to support a registry system that supports in excess of 50M domains. Since this TLD projects 471,482 domains, 0.94% of these resources are allocated to this TLD. See attachment 'Q30a - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

The Production Support Group is responsible for the deployment and operation of TLD registries.

ARI employs a rigorous hiring process and screening (Police background checks for technical staff and Australian Federal Government 'Protected' level security clearances for registry operations staff).

This completes our response to Q30(a).

© ***Internet Corporation For Assigned Names and Numbers.***





# **Annex 5.**



## New gTLD Application Submitted to ICANN by: Charleston Road Registry Inc.

String: web

Originally Posted: 13 June 2012

Application ID: 1-1681-58699

### Applicant Information

#### 1. Full legal name

Charleston Road Registry Inc.

#### 2. Address of the principal place of business

Contact Information Redacted

#### 3. Phone number

Contact Information Redacted

#### 4. Fax number

Contact Information Redacted

## 5. If applicable, website or URL

## Primary Contact

### 6(a). Name

Sarah Falvey

### 6(b). Title

Senior Policy Analyst

### 6(c). Address

### 6(d). Phone Number

Contact Information Redacted

### 6(e). Fax Number

### 6(f). Email Address

Contact Information Redacted

## Secondary Contact

### 7(a). Name

Chris Iannuccilli

### 7(b). Title

Director of Marketing

**7(c). Address****7(d). Phone Number**

Contact Information Redacted

**7(e). Fax Number****7(f). Email Address**

Contact Information Redacted

**Proof of Legal Establishment****8(a). Legal form of the Applicant**

Corporation

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

State of Delaware (General Corporations Code)

**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.**

Google Inc.

**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**

Christine Flores	Director
------------------	----------

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

Donald S. Harrison	Assistant Secretary
James Marocco	CFO and Treasurer
Christine Flores	CEO, President, and Secretary

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

Google In.	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.**

web

**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.**

While the string for which Charleston Road Registry (CRR) is applying, .web, is not an IDN and, therefore, does not contain characters which require mixed right-to-left or left-to-right functionalities, CRR has nonetheless familiarized itself with the requirements and components of the IDNA protocol by reviewing the relevant RFCs and the relevant background information found on the ICANN IDN Wiki. CRR has also tested the .web string for rendering issues; none were found.

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

## Mission/Purpose

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

18.a. Mission/Purpose of the Proposed gTLD

Charleston Road Registry is an American company, wholly owned by Google, which was established to provide registry services to the Internet public. Google is an American multinational public corporation and global technology leader focused on improving the ways its hundreds of millions of users connect with information. Since its formation, Google has been developing technology that can improve upon existing ways of doing business on the Internet. Google provides a variety of services and tools for Internet users and advertisers of all sizes, from simple search features and local ads to enterprise-scale business applications and global advertising solutions. These tools make it easier for people to make use of the world's information and enable entrepreneurs and publishers around the world to grow their businesses.

In line with Google's general mission, Charleston Road Registry's mission is to help make information universally accessible by extending the utility of the DNS while enhancing the performance, security and stability of the Internet for users worldwide. Charleston Road Registry aspires to create unique web spaces where users can learn about products, services and information in a targeted manner and in ways never before seen on the Internet. Its business objective is to manage Google's gTLD portfolio and Google's registry operator business. As discussed further in the responses to questions 23 and 31, Charleston Road Registry intends to outsource all critical registry functions to Google Registry Services.

The proposed gTLD will provide the marketplace with a new all-purpose gTLD for second-level domain names, .web. The mission of this gTLD is to act as an alternative to current gTLDs, in particular .com and .net. This mission will enhance consumer choice by providing new availability in the second-level domain space and increasing competition amongst generic gTLDs. Charleston Road Registry believes that registrants will find value in associating with this gTLD, which could have a vast array of purposes for enterprises, small businesses, groups or individuals seeking a second-level domain name already registered in .com or .net, or those simply seeking a competitive alternative to existing gTLDs. This assertion is supported by industry data: over 375,000

new second-level domains were registered in January 2012 in the .com and .net gTLDs, and the two gTLDs support a total of 115 million second-level domains -- more than 80% of all second-level domains registered in one of the 6 open U.S. gTLDs (.com, .net, .info, .org, .biz, .us) [Source: <http://www.dailychanges.com/>].

The proposed gTLD will also provide Charleston Road Registry with the means to meet its business objectives.

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

### 18.b. Benefits to Registrants, Internet Users, and Others

#### 18.b.i.1 Specialty

The goal of the proposed gTLD is to create a new Internet environment that provides registrants, Internet users, and the public with the opportunity to associate with a meaningful term. Specialization will arise from this environment through market dynamics as entities align their offerings with the term.

The specialization goal of .web is to provide an alternative, general purpose gTLD that offers consumers more choices to align their web spaces to a generic gTLD than the existing options today.

#### 18.b.i.2 Service Levels

Through its association with Google, Charleston Road Registry is uniquely positioned to enable and support the proposed gTLD by providing its service reliability and speed of delivery as a part of its services. Google brings unique expertise and a proven record of excellence in infrastructure operations: Google now runs the largest DNS system in the world, has industry-leading uptime on its services, such as web search, and offers enterprise services on which governments and businesses depend.

Google is known for its high level of quality and speed, and Charleston Road Registry's service level goal for the proposed gTLD is to extend that high level of quality, speed, and service to registrars. Indeed, two of Google's core principles in providing Internet search and related goods and services are "focus on the user and all else will follow" and that "fast is better than slow."

Charleston Road Registry is committed to using the most technologically advanced, secure, and reliable registry services for all of the domain names in the gTLD so as to not compromise the service levels, security, and stability of the gTLD to users worldwide.

Charleston Road Registry will provide both Engineering and Customer Service support to registrars. All registrars will also have the same level of access to Charleston Road Registry resources to resolve disputes and technical and/or administrative customer service issues.

Charleston Road Registry will provide all registrars with 24-hours-a-day, 7-days-a-week Customer Support in the form of telephone, email, and/or web chat for technical and non-technical issues relating to the operation of the gTLD system. Charleston Road Registry will provide all registrars with the same level of access to customer support via telephone, email, and Charleston Road Registry's website; email and web-based interactions will be the primary method of provisioning customer service support to registrars.



Additionally, Charleston Road Registry will implement strict policies and procedures to minimize abusive domain name registrations and uses and other activities that have a negative impact on Internet users. It will dedicate ample resources for the purpose of responding promptly to abuse complaints from government, judicial and/or law enforcement.

#### 18.b.i.3 Reputation

Google has a proven record of providing high-quality, secure online services. Charleston Road Registry seeks to enhance Google's reputation for excellence, superior quality, and high level of security and become known as an exemplary domain name services provider. When registrants assess opportunities in the marketplace to obtain a name, they will have confidence in Charleston Road Registry's ability to meet ongoing needs as the registry operator for the proposed gTLD. When Internet users visit a domain name in the proposed gTLD environment, they will be able to reliably expect and experience the high level of security and quality on which Google's reputation has been built.

The registry will be structured so that Charleston Road Registry allows registrars to register and oversee second-level domain names in the proposed gTLD; that registrars develop and deploy a reasonable process for ensuring that those domain names are used for gTLD-relevant purposes as specified in the registry-registrar agreement; and per Specification 4 that the WHOIS is thick and reliable; and that the registry is responsive to legal rights owners (if applicable) who may have complaints about potentially abusive registrations.

In addition, Charleston Road Registry's operation of the new gTLD will provide the opportunity for registrars and registrants to build and/or bolster their unique brands and brand reputation in association with the proposed gTLD.

#### 18.b.ii.1 Competition

Charleston Road Registry supports the advancement of registry operators as a whole and the diffusion of gTLDs amongst diverse stakeholders to generate increased competition for the benefit of the Internet public. Increased competition will result in more competitive prices for consumers, generate efficiencies and increase productivity in enterprises, and spur innovation in the gTLD space.

The proposed gTLD, .web, will provide a new online structure for the aggregation of other level domain-specific content. As an alternative to existing second-level domains, Charleston Road Registry anticipates that the .web gTLD will increase competition among registrars by increasing consumer choice and creating new opportunities for registrar pricing differentiation. Charleston Road Registry also anticipates the .web gTLD will help grow the volume of entities and individuals offering content online, thereby increasing competition among such entities and individuals to provide new, unique, and more relevant content and offerings.

Managing this Internet space will allow Charleston Road Registry to provide to registrars and registrants the high level of technical operations quality and service for which Google is known, which in turn will incent other existing and new gTLDs to improve the quality of their offerings.

Charleston Road Registry will facilitate a fair and equitable registrar process, providing open access to any registrar who meets ICANN accreditation guidelines by fully complying with the Registry Operator Code of Conduct. Charleston Road Registry is committed to treating all registrars equitably and will not offer preferential treatment to Google in its capacity as registrar.

#### 18.b.ii.2 Differentiation

Charleston Road Registry believes in the commercial viability of alternatives to existing gTLDs such as .com and .net. The proposed gTLD will provide the

marketplace with opportunities for differentiation not currently available in the gTLD space.

The .web gTLD providers registrants with the opportunity to differentiate from other web spaces based on their word choice within the second-level domain name.

Given its association with Google, Charleston Road Registry offers a unique value proposition to registrars resulting from the strength of Google's trusted brand, technical leadership, and support for free speech on the Internet. Registrars will have the opportunity to leverage this brand in devising their own market positions.

#### 18.b.ii.3 Innovation

The proposed gTLD will foster innovation by creating a new space for the categorization and classification of online content. It will therein provide a mechanism by which registrars and registrants can better brand and manage their online presence by associating it with the .web namespace. This namespace delivers value to the public through the provision of new and differentiated content, goods, and services to Internet users.

The proposed gTLD provides registrars with the opportunity to create and offer tailored new products and services that benefit registrants and/or improve user experience in association with the registration of a second-level domain in the .web gTLD.

In addition, the proposed gTLD will promote innovation in the marketplace by providing additional second-level domain options for the public's use. This will invite new entrants to establish a domain name presence, facilitating innovation in their offerings, and their interactions with Internet users.

Charleston Road Registry considers the proposed gTLD to be a platform for innovation with existing and future Google products and services. Charleston Road Registry, therefore, may incorporate these new offerings into future registry service options (subject to the ICANN approval process), infusing new ideas into the gTLD for the betterment of the public.

Google consistently aims to improve upon technologies that connect people with information, as demonstrated by a proven record of innovation and iteration. Charleston Road Registry strives to offer its constituents this same level of continuous development in advancing its management and operation of the gTLD, engendering benefits to registrars, registrants, and end users.

#### 18.b.iii User Experience

Charleston Road Registry will strive to provide the highest level of user experience through operational stability, security, and performance to serve the interest of registrants in the proposed gTLD. Charleston Road Registry is uniquely positioned to provide this level of experience given its relationship with Google; Google invested over \$3 billion in its IT infrastructure in 2011 and maintains a record of excellence in infrastructure operations.

The proposed gTLD will provide registrants with the opportunity to differentiate their dedicated domain space such that the end users are able to discern the type of content intended to be found within the proposed gTLD. This will enable increased user visibility of registrants' offerings, as well as provide registrants with the opportunity to enhance their respective content offerings and innovate in new ways.

The proposed gTLD will provide a more trusted and user-friendly environment where domain names and content related to the .web gTLD can flourish. Charleston Road Registry seeks to have users deem the gTLD trustworthy and reliable and recognize it as an aggregated source of targeted goods, services,

and information.

The proposed gTLD, furthermore, facilitates an improved online user experience through greater structure and categorization on the Internet.

#### 18.b.iv Registration Policies

Charleston Road Registry believes that given its wide variety of uses, the .web gTLD will best add value to the gTLD space by remaining totally open and unencumbered by registrant restrictions. There will, therefore, be no restrictions on second-level domain name registrations in the proposed gTLD, .web.

Charleston Road Registry will make access to Registry Services, including the shared registration system, available to all ICANN-accredited registrars. Domain names within the proposed gTLD will be available to the general public for registration and use.

Charleston Road Registry is committed to implementing strong and integrated intellectual property rights protection mechanisms. Doing so is critical to Google's goals of model Internet citizenship and fostering Internet development, especially in emerging regions. Accordingly, Charleston Road Registry intends to offer a suite of rights protection measures, which builds upon ICANN's required policies while fulfilling our commitment to encouraging innovation, competition and choice on the Internet.

#### 18.b.v Protection of Privacy and Confidential Information

Charleston Road Registry will strive to ensure the appropriate level of privacy and security will be met for its users. Charleston Road Registry and its provider of registry services, Google, have imposed measures to achieve this protection; additional specifics regarding the practices for the registry include but are not limited to the following:

- All data transmitted from registrars to the registry will be encrypted using transport layer security (TLS) or other similar data protection schemes to ensure that third parties cannot access personally identifying information or other sensitive data as it crosses the Internet.

- Charleston Road Registry will attempt to prevent the misuse of WHOIS data for improper purposes such as spam, intellectual property theft, or phishing. Charleston Road Registry will attempt to identify patterns of abusive usage of the WHOIS and will appropriately use CAPTCHA, query throttling or other techniques to prevent information scraping.

- Google will restrict access to data and information systems maintained by the registry to a specific list of individuals involved with supporting the Google Registry system in production. Google will review this list on a periodic basis to ensure that the level of access granted to individuals is appropriate. Google uses two-factor authentication and other mechanisms to ensure that staff with access to user information are properly identified prior to using registry systems.

- Google data backups stored offsite are encrypted with passwords that are securely managed on Google's internal systems. Google can effectively remove the ability to access this data by destroying the relevant encryption password.

- Supplying Google account information will be optional for registrants unless the domain registration is directly associated with another Google product offering. Google will not disclose Google account information except for any contact information provided by the user that is required by ICANN (per Specification 4) to be displayed in response to a WHOIS query.

- Registrar billing and payment information will not be stored alongside domain

name registration information. All registrar billing and payment information will be stored in a payment card industry (PCI)-compliant billing system similar to that used by Google Ads.

- Data will not be shared with third parties without the permission of registrants, except as required for registry operations or as required under the law, such as in response to a subpoena, other such court order, or demonstrated official need by law enforcement.

Beyond these specific mechanisms, both Charleston Road Registry and Google will govern its approach to privacy by the Charleston Road Registry Privacy Policy. This policy applies to registrars, registrants and end users of registry services such as DNS zone publication and WHOIS data publication. The Privacy Policy is located at <http://charlestonroadregistry.com/privacy.html>.

#### 18.b.vi. Outreach and Communications Efforts

Once Charleston Road Registry begins developing public-facing resources in its gTLD, it intends to inform the public about the gTLD and the opportunity to obtain domain space there through investments in marketing and public relations.

Charleston Road Registry intends to promote gTLDs in its portfolio, such that the public gains an awareness and understanding of new gTLDs and the availability of new second-level domain space on the Internet. Charleston Road Registry believes that this approach will make the strongest impact in modifying consumer behavior and is the best path to achieving success for all new gTLDs collectively.

Charleston Road Registry will reach out to the Internet community via a number of different outreach and communications methods and venues to deliver its mission and message to the public, including but not limited to: press briefings, videos posted on various Internet sites, blogs and other social media, and paid advertising. In addition, when developing resources for localized Internet registrars in different global regions, Charleston Road Registry will use local marketing and communications platforms as needed.

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

#### 18.c. Minimizing Social Costs and Other Negative Consequences

##### 18.c.i

Registration will be managed by Charleston Road Registry in three phases.

Phase 1 - The first phase will be an extended 60-day sunrise phase. Only owners of trademarks listed in the Trademark Clearinghouse may participate in this phase, and such owners may register domain names that consist of an identical match to their listed trademarks. If multiple qualified parties express an interest in registering the same domain name, Charleston Road Registry will award the domain name through an auction or other predetermined process that will be published prior to the Sunrise Period. At the end of the sunrise phase, at a minimum, Charleston Road Registry will follow ICANN rules for subsequent attributions of trademarked second-level domains and will offer other protections for trademark owners, including but not limited to an extended Trademark Claims Service of indefinite length.

Phase 2 - The second phase will be a limited term registration phase. During this phase, any interested applicant may apply for all second-level domain names not previously registered in the sunrise period. Trademarked terms will be subject to the Rights Protection Mechanisms set forth in Response 29. At the

end of the second phase, if multiple parties have expressed an interest in registering the same second-level domain name, Charleston Road Registry will award the domain name through an auction or other predetermined process that will be published prior to the commencement of this phase.

Phase 3 - The third phase will be a steady state phase for the duration of registry operation. During this phase, any interested applicant may apply for all second-level domain names not previously registered in an earlier phase. Trademarked terms will be subject to the Rights Protection Mechanisms set forth in Response 29. If multiple parties express an interest in registering the same domain name, Charleston Road Registry will award the domain name on a strictly first come, first served basis.

#### 18.c.ii

While Charleston Road Registry reserves the right to charge different prices for unique second-level domains within the gTLD, once Charleston Road Registry determines the price for a particular second-level domain, Charleston Road Registry will not price discriminate among ICANN-accredited registrars. Charleston Road Registry does not intend but reserves the right to offer introductory discounts and bulk registration discounts. Volume discounts, marketing support and incentive programs may be made available, and if so will be offered to all ICANN-accredited registrars without preference.

#### 18.c.iii

Pursuant to the ICANN-Registry Operator Agreement, Charleston Road Registry will provide written notice a minimum of 30 days prior to any increases in price for initial registrations, as well as written notice 180 days prior to any increase in registration renewals. Further, Charleston Road Registry will offer uniform pricing for renewals as specified in the ICANN-Registry Operator Agreement.

Charleston Road Registry does not currently intend to make contractual commitments to registrants regarding the magnitude of price escalation. Charleston Road Registry does, however, intend to keep its practices competitive and aligned to activity in the marketplace.

## 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.**

As specified throughout this application, Charleston Road Registry (CRR) plans to implement comprehensive anti-abuse mechanisms. CRR will protect against the abusive registration of geographic names at the second and other levels in the applied-for gTLD by reserving to the registry protected geographic names in order to prevent registration of such strings.

In that regard, CRR has thoroughly reviewed Specification 5 of the Registry Agreement, the Government Advisory Committee's (GAC) "Principles Regarding New gTLDs", and the .info methodology for reservation and release of country names. Accordingly, CRR will, in connection with its registry services operator and registrar, initially reserve from registration by any party names with national or geographic significance within the TLD during the TLD's Sunrise Period and Trademark Claims Period.

The names with national or geographic significance (hereto referred to as "geographic names") that will be initially blocked are those specified in Specification 5 of the New gTLD Registry Agreement, namely:

- (1) The short form (in English) of all country and territory names contained on the ISO 3166-1 list, as updated from time to time, including the European Union, which is exceptionally reserved on the ISO 3166-1 list, and its scope extended in August 1999 to any application needing to represent the name European Union;
- (2) The United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World; and
- (3) The list of United Nations member states in 6 official United Nations languages prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names.

As noted above, the top-level domain shall not permit the public to register domain names with national or geographic significant at the second-level. The names will be set aside by use of the Reserved state making them inaccessible (See response to Question 27 for details). Google, as the registry services provider, has arranged for such reservation to occur prior to the launch of the TLD.

In the event there is a compelling use of a two-character geographic name, the two-character label string may be released to the extent that CRR reaches agreement with the government and country-code manager and consults with the GAC and ICANN. The Registry may also propose the future release of these reserved names based on the implementation by the prospective registrant of measures to avoid confusion with the corresponding country codes.

As with the .info TLD, only if a potential second-level domain registrant makes a proper showing of governmental support for country or territorial names will CRR relay this request to ICANN. CRR also plans to consult with the GAC and of ICANN before proceeding to delegate the domain at issue.

## Registry Services

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

Charleston Road Registry (CRR) will outsource the entirety of its technical operations to Google. In addition to running the technical platform, Google will provide CRR with staffing and support to ensure that all registry services meet both the requirements laid out by ICANN in the new generic top-level domain (gTLD) Applicant Guidebook as well as in the gTLD registry agreement. Additional details of Google's provision of services to CRR are set forth in Question 31, Section 31.1.

By making use of Google's Registry platform, CRR will provide the following registry services:

- Receipt of data from registrars concerning registration of domain names and name servers
- Dissemination of top-level domain (TLD) zone files
- Dissemination of contact or other information concerning domain name registrations (WHOIS service)

- Internationalized Domain Names (IDN) Support for all domain names
- Domain Name System Security Extensions (DNSSEC) support
- IPv6 Support
- Data escrow
- Redemption grace period for domain names
- Registrar and developer account creation

"Q23\_Registry Services Diagram" shows major services being exposed by high-level systems. Note that this diagram shows only data flow and does not specify the physical deployment characteristics of these services.

Details on these services are discussed below.

### 23.1. Receipt of Registration Data

Google will receive registration data from users in a manner consistent with standard registry operations. This will be handled via the extensible provisioning protocol (EPP) interface through ICANN-accredited third-party registrars. Google will operate a robust Shared Registration Service (SRS) that allows registrars to add, modify, and delete domain registrations and provides full support for the domain registration lifecycle.

Google's shared registration system (SRS) infrastructure consists of three major components: an extensible provisioning protocol (EPP) server that provides an EPP interface to registrars; the Google SRS Frontend, which provides web-based access to the state of the Google Registry, the registrar's profile and access to registration reports for the registrar; and the Google SRS Backend, which implements most business logic, interacts with the data store, and pushes updates to DNS and WHOIS servers in order to disseminate TLD Zone files as well as registrant contact information.

Details of the SRS are described in Question 24, EPP support in Question 25, and the registration lifecycle in Question 27.

### 23.2. Dissemination of TLD Zone Files

TLD zone data will be propagated in near real time to Google's Authoritative DNS infrastructure, which will serve as the primary means of publication of the TLD zone files. This DNS infrastructure is based on Google's existing Public DNS product, which handles over 70 billion queries per day. This DNS implementation will be fully compliant with RFCs 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 3901, 4343, 4472, 4972, and 5966 as well as ICANN's Specification 10. A full description of Google's Authoritative DNS infrastructure is described in Question 35.

In addition to real-time publication via port 53, the Google Registry will also support publication of the entire zone, as described below:

The master zone file will be internally generated and cached in the Google Shared Registration System (GSRS) as modifications to GSRS's persistent store are made. The zone data will be signed by the Authoritative DNS infrastructure; a copy of the signed data is also returned to the GSRS. The entire master zone file will then be available to authorized parties at an HTTP URL shared with them over the web.

The master zone file at this location will be guaranteed to be no more than one hour old.

When retrieving the zone file, the client will pass a single HTTP request parameter ("key"), in order to identify individually the qualified client requesting access. This parameter will be the API key given to the registrar during account signup.

The mimetype "text/dns" will be set on the HTTP response and the content



encoding will be gzip.

The master zone file will follow the format specified by RFC 1035, with the additional restrictions as specified in Specification 4, Section 2.1.4 of the gTLD Applicant Guidebook. DNSSEC resource records will also be present.

In addition, the master zone file will be made available through the Centralized Zone Data Access Provider as specified in Specification 4, Section 2.1.4 of the gTLD Applicant Guidebook.

### 23.3. Dissemination of Contact Information (WHOIS)

Google will create an implementation of the WHOIS protocol (as defined by RFC 3912) that will listen on port 43 for WHOIS requests. Google's WHOIS service will communicate to the name registry through a private API end-point in order to retrieve the necessary information for WHOIS responses. In addition, Google will operate a public WHOIS, web-based Directory Service at <WHOIS.nic.web> providing free, public query-based access. Both traditional WHOIS and web-based WHOIS will be made available over both IPv4 and IPv6.

As required by Specification 4 in the gTLD Applicant Guidebook, Google's WHOIS service will perform in the following manner:

- Semi-free text format followed by a blank line and disclaimer specifying the rights of the Registry Operator, and user querying the database.
- Each data object shall be represented as a set of key/value pairs, with lines beginning with keys, followed by a colon and a space as delimiters, followed by the value.
- For fields where more than one value exists, multiple key/value pairs with the same key shall be allowed.
- The first key/value pair after a new-line starts a new record, and is used to identify the record itself.
- The format of fields governed by EPP RFCs 5730-5734 (domain status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers, email addresses, date and times) will be formatted as specified by those RFCs.

Updates to WHOIS data will be made in near real-time, with the registry's service level agreement (SLA) committing to 95% of the updates reaching the serving infrastructure within 15 minutes. Details of WHOIS support are included in Question 26.

### 23.4. Internationalized Domain Names

IDNs allow registrars to register domain names with unicode code points representing non-ASCII-based character sets. IDNs constrained by the IDN Tables for this TLD will be supported by the Google Registry. Google's IDN implementation will make use of the IDNA standard and be fully compliant with both RFCs 5890-5893 and ICANN's IDN implementation guidelines. For more information on the IDN implementation for the TLD, see Question 44.

### 23.5. DNS Security Extensions

The Google Registry will support DNSSEC. In particular, registrants will be able to specify a DS record as part of normal domain name registration with their registrars, which will be transmitted to the Google Registry via its EPP interface. The Google Registry will then sign the DS record, along with all other DNS resource records in the TLD Zone, forming a chain of trust between the Google Registry and second-level domain name. The Google Registry itself will publish its own DS record with the root. Google's DNSSEC implementation will be fully compliant with RFCs 4033, 4034, 4035, 5910, 4509, 4641, and 5155. More information on this topic, including the DNSSEC Policy statement for the TLD is contained in Question 43.

### 23.6. IPv6 Support

The Google Registry operates on Google's production network, which supports IPv6. Specifically, the Google Registry will specifically support IPv6 access to all registry service endpoints (WHOIS, EPP, DNS, etc.). All services are provided through dual-stack, which is considered the industry-standard best practice for supporting IPv6. In addition, domain name registrants will be able to create IPv6 AAAA glue records for nameservers in the TLD zone. Further detail about Google's IPv6 implementation is available in Question 36.

#### 23.7. Data Escrow

Google will escrow relevant registration data, as required by ICANN's registry agreement. Google will ensure that its data escrow will be fully ICANN compliant and performed in accordance to industry best practices. In addition to Google's practice of hosting critical data on redundant and geographically disparate datacenters, data escrow will provide further assurance against data loss and ensure that all Google Registry data can be retrieved in a timely manner. For more information on Data Escrow, see Question 38.

#### 23.8. Redemption Grace Period for Domain Names

After a domain name has been deleted by a registrar, the domain name shall move into a Redemption Grace Period. The status of the domain will be listed as PENDING DELETE RESTORABLE. When a domain is in this state, it is deleted from the zone for the TLD. This is a strong indicator to the registrant that it must act take action in order to restore the domain to its previous state. For details, see Question 27.

#### 23.9. Creation of Registrar and Developer Accounts

Google's Registry will use Google Accounts to manage registrars.

To create a Google Account, all parties will be directed to the following URL:

<http://www.google.com/accounts>

Once a prospective registrar or developer has created an account in Google, the registrar or developer can upgrade from a standard Google account to a registrar and/or developer, if certain requirements are met.

To obtain a set of credentials used to interact with the Google Registry, a registrar will proceed through the following workflow:

- A. The Google registrar logs in with Google account credentials.
- B. The Google registrar submits an application identifying that it is an accredited ICANN registrar, and that it wishes to interact with the Google Registry.
- C. The Google registrar requests and resets initial EPP credentials, which are separate from a Google account.

Once a Registrar has been certified and authorized for billing, they will be ready to interact with Google through Google EPP. At this point, the registrar can also view reports on domains registered, EPP transactions, remaining account balance, and other TLD registry statistics.

"Q23\_Registrar Registration Process Diagram" shows the registration process for registrars.

In addition to registrars, Google will also provide accounts to developers and other authorized users, who will obtain credentials through the following workflow:

- A. The developer logs in the previously created Google account.
- B. The developer requests an API key to be used for all public API calls.
- C. The developer reviews access restrictions, quota, and service-level agreements and agrees to appropriate terms.

D. Google Registry grants access to zone data exported by the domain.

"Q23\_Developer Registration Process Diagram" shows the registration process for developers.

## Demonstration of Technical & Operational Capability

### 24. Shared Registration System (SRS) Performance

All Shared Registration System (SRS) services described in Question 23 will run on Google's robust, high-performance platform. Google's production platform is an extremely high-capacity, high-availability, scalable platform designed to support some of the most resource-intensive and often-used applications on the Internet, including Google Search, Gmail, and YouTube. Google builds large clusters out of thousands of individual servers. Google uses a common set of tools to allocate resources, provide access to basic services such as storage and locking, and to simplify programmers' ability to build distributed systems using the cluster's hardware. Rather than relying on expensive hardware to provide reliability, Google uses a more cost effective approach based on commodity components, and builds fault tolerance into its software. Google simultaneously increases performance, reliability, and scalability of our production systems by splitting work into shards and running multiple replicas of the same process.

The numbered sections below discuss details of our SRS implementation and capacity plans.

#### 24.1. Google SRS (GSRS)

The Google Shared Registration System (GSRS) will provide all standard registry services:

- Receipt of data from registrars concerning registration of domain names and name servers
- Dissemination of top-level domain (TLD) zone files
- Dissemination of contact or other information concerning domain name registrations (WHOIS service)
- Internationalized Domain Names Support for all domain names
- Domain Name System Security Extensions (DNSSEC) support
- IPv6 Support
- Data Escrow

For descriptions and details of all SRS functions, see Question 23.

#### 24.2. Google SRS Components

GSRS will be a multi-tier application that consists of the following components.

- Google SRS Front End (GSRS-FE): Presentation. A web application which provides an interface between registrars, developers, and other parties that need access to Google Registry information through a web interface. GSRS-FE will also include a web-based WHOIS interface.
- Google SRS Back End (GSRS-BE): Business Logic. A representational state transfer (RESTful) service that exposes and controls all registry data. Most business logic related to registry data storage and persistence will be implemented in GSRS-BE.
- Google EPP (GEPP): API Proxy. A public end-point for EPP (Extensible

Provisioning Protocol) for the top-level domain. GEPP will translate all EPP requests and responses to interface with GSRS-BE. For more information on EPP support, see Question 25.

- Google WHOIS (GWHO): A public end-point for WHOIS queries for the top-level domain. GWHO will translate all WHOIS requests and responses to interface with the GSRS-BE. For more information on WHOIS support, see Question 26.

In addition, GSRS will integrate with the following internal systems. These internal systems are designed for extremely high performance and robustness, and use the same technologies used for other high-capacity services currently in production.

- Google Persistence Service (Persistence): A multi-master persistence solution which will run on top of Google's proprietary database, BigTable. The Google Persistence Service coordinates between masters using an algorithm for fault-tolerant distributed systems, such as Paxos. BigTable is Google's internal implementation of a distributed hash table used for the majority of our persistence needs.

- Google Accounts (Authentication): An existing platform for creation and authentication of user accounts. Google Accounts provides a standard login page for all Google products, as well as programmatic access for internal applications to retrieve credentials for the logged-in user.

- Google Monetization (Billing, as needed for the TLD): A monetization and billing system. Enables Google products to create accounts, create invoices, and perform financial transactions for Google customers.

- Google Authoritative DNS (Master Zone File): A robust public DNS server. Google Authoritative DNS will receive master zone file information from the GSRS-BE and distribute DNS information to clients.

"Q24\_SRS Services Diagram" shows the interactions with these systems as requests come into a Google datacenter and are handled appropriately. Note that, as shown in "Q24\_SRS Services Diagram", all SRS requests are passed to the GSRS-BE, which contains all business logic for Google Registry. Integrated services are then used as needed. Google plans to provision these services to handle significantly greater load than our most aggressive expectations -- see below for details.

### 24.3. Google SRS Deployment Parameters

Google plans to deploy GSRS in five geographically-distributed datacenters throughout North America. Traffic to these datacenters is dynamically adjusted according to load, and the system will be provisioned to allow two simultaneous datacenter outages without substantial performance impact.

Each datacenter will include several replicas to handle specific machine failures for any GSRS service. Google's production servers include the ability to expand to add new servers dynamically according to need. If SRS performance suddenly requires additional throughput capacity -- for instance, during a Distributed Denial of Service (DDoS) attack -- Google will be able to enable up to 100 additional replica servers in any datacenter dynamically. The limit of 100 additional replica machines is a self-imposed limit and may be revised upward based on ongoing operational considerations.

Each machine will be able to support a minimum of 250 queries per second (read or write), where one query contains one record. For architectural simplicity, our initial implementation will read data without any additional SRS-level caches.

### 24.4. GSRS Performance Scaling

Google plans to deploy sufficient capacity to handle SRS request load on the same scale as the largest top-level domains on the Internet. These computations are detailed in "Q24\_GSRS Performance and Scaling".

The key factor for scaling GSRS performance capacity will be the GSRS-BE component. Other components for GSRS (both GSRS-FE and GEPP) will receive user requests and then transform them into Remote Procedure Call (RPC) calls to GSRS-BE. GSRS-FE and GEPP will not perform any CPU-, disk-, or memory-intensive computations themselves. The performance capacity estimations below will therefore discuss only GSRS-BE capacity.

Based on existing domains and calculations for inbound traffic, Google estimates that there will be about 2300 queries per second for EPP operations, consisting mostly of checks for existing domains, and 3600 queries per second for WHOIS operations. In total, Google estimates that GEPP-BE must handle roughly 5900 queries per second for a scale of 100 million domains. Other operations, such as zone file operations and developer API calls, will create a relatively negligible level of load.

Google will meet the SRS throughput requirement, with a 50% utilization rate, with 48 machines allocated across the five datacenters. At this level of utilization, our active capacity will be double the expected throughput requirement. If a datacenter is lost through a production outage or change request, then additional machines will be enabled immediately to take upon the additional load with no manual intervention required. Google production systems have the standard capability to enable new machines to handle increased capacity needs immediately.

These estimations do not include any smart caching anywhere in the architecture. If the Google Registry reaches a very large number of domains and additional capacity measures are required, Google will consider a design for an appropriate WHOIS and EPP check result caching plan to relieve load and to improve latency characteristics.

These estimates use a very aggressive set of assumptions for scaling, which should be sufficient for a large open domain.

#### 24.5. GSRS Network Scaling

Google expects that our SRS network bandwidth requirements will be greatly below Google's existing per-datacenter network capacity, even for its lowest-capacity datacenters in production. Details of its computations are included below.

Google assumes that 99% of RPC calls across both EPP and WHOIS will be less than 5 kB. EPP and WHOIS queries return more of a fixed number of records, and most queries will return only one record. 5 kB is derived as an estimate from taking the sample WHOIS output in the applicant guidebook, and multiplying it by three to account for XML inflation as if the same information passed through an EPP interface. Considering that most EPP commands are expected to be `<check>` commands, this is a very conservative estimate.

Google then uses 5 kB as the assumed size to calculate the estimates for bandwidth per machine and per datacenter at maximum load.

Network Bandwidth Requirements per Machine = Queries per Second \* Size of RPC Calls

With 250 qps and 5 kB per query, Google expect a maximum of about 12.5 MB/s of bandwidth requirement. This is about one-eighth of our current absolute minimum commodity standard of 1 Gb Ethernet. Our backbone routers connect many metro networks around the globe at 10Gb or greater.

Network Bandwidth Requirement per datacenter = Requirements per Machine \* Number of Machines

With 12.5 MB/s of bandwidth per machine, and 100 machines maximum per datacenter, Google expects a maximum of about 1.25 GB/s data requirements

during a major event that requires increased load demand. All Google datacenters' connections to its production network have a multiple 10 GB/s links, and many exceed this by far.

Based on these computations, Google believes that the network bandwidth required by the SRS system for as many as 100 million second-level domains will never exceed the capacity that even our smallest datacenter can provide.

#### 24.6. Multi-Master Design

GSRS will use a multi-master architecture. This architecture is detailed further in Question 32. Machines across multiple datacenters will serve active traffic, with no machines on cold or hot standby. All instances of the data store update in real-time, and updates to registry data are committed across a quorum of replicas before the write is confirmed. When GSRS or a dependent service goes down or is drained by an outage, Google's network architecture will redirect all affected traffic to another datacenter. Google will design most services as stateless, so service instances will not require any coordination mechanisms.

#### 24.7 Google SRS Adherence to Specification 6

The Google Registry, and in particular the SRS will be compliant with all RFCs outlined in Specification 6. Any RFCs mentioned below and their successors will be complied with.

##### 24.7.1 - Standards Compliance

###### 24.7.1.1 DNS

Google's domain name system (DNS) implementation will comply with RFCs 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 4343, and 5966. See Question 35 for more details on DNS RFC implementation compliance.

###### 24.7.1.2 EPP

Google's EPP implementation will comply with RFCs 5910, 5730, 5731, 5732, 5733, 5734, 3915, and 3735 for any extensions developed. Please see Question 25 for more details on EPP RFC implementation compliance.

###### 24.7.1.3 DNSSEC

Google's DNSSEC implementation will comply with RFCs 4033, 4034, 4035, 4509, 5155, and the best practices indicated in RFC 4641. A DPS statement will be published for each TLD supported by the Google Registry. Please see Question 43 for more details on DNSSEC implementation compliance.

###### 24.7.1.4 IDN

Google's implementation of internationalized domain names (IDN) will comply with RFCs 5890, 5891, 5892, 5893 and ICANN's published IDN Guidelines. Please see Question 44 for more details on IDN RFC implementation compliance.

###### 24.7.1.5 IPv6

Google's implementation of IPv6 will follow BCP 91 and RFCs 4472. All Registry services will be offered over IPv6. Please see Question 36 for more details on Google's IPv6 implementation.

##### 24.7.2 Registry Services and Wildcard Prohibition

Google understands the definition of "registry services" as defined in section 2.1 of Specification 6. Google will not support wildcard matching or resolution in the TLD zone as required by Section 2.2 of Specification 6.

### 24.7.3 Registry Continuity

Google will ensure registry continuity as specified in Section 3 of Specification 6. High availability, extraordinary event handling, and business continuity will be provided with respect to the TLD. See Question 39 for more details on Google's Registry continuity plan.

### 24.7.4 Abuse Mitigation

Google will implement the abuse mitigation requirements as specified in Section 4 of Specification 6. An abuse contact will be made available. See Question 28 for more details on Google's abuse handling. Google will also take action to remove malicious use of orphan glue records when provided evidence in written form that such records are present in connection with malicious content.

### 24.7.5 Supported Initial and Renewal Registration Periods

Google will implement the supported initial and renewal registration periods as specified in Section 5 of Specification 6. The Google Registry will support domain name registration with validity periods of between one to 10 years in increments of one year. Renewal registration may extend registration to a maximum of 10 years from renewal date in increments of one year.

### 24.8. Google SRS SLA and Adherence to Specification 10

The Google SRS will significantly exceed the requirements of the Service Level Requirement Matrix defined in Specification 10 in the gTLD Applicant Guidebook. All EPP and WHOIS/RDDS calls supported by the Google SRS system will have a 99.9% monthly uptime.

For the purpose of measuring this commitment, Google uses the following definitions:

RPC: A series of TCP/IP packets forming a distinct request, and the corresponding TCP/IP packets forming the response.  
Error RPC: An RPC which does not return with 3x 95th percentile latency, or which fails because of internal transient errors.  
Error Minute: Any minute during which 10% of RPC requests are error RPCs.  
Monthly Uptime: The total number of minutes in a month minus the number of error minutes divided over the total number of minutes in the month, rounded to the nearest .01%.

When calculating monthly uptime percentage, Google does not distinguish between scheduled and unscheduled downtime.

Google will meet or exceed all service level agreements (SLA) described in the ICANN Applicant Guidebook. Specifically, Google will meet the commitments as specified in attachment "Q24\_SLAs". Note that the values represent a commitment to exceed SLA Requirements in Specification 10.

#### DNS

- DNS Availability: 0 minutes of downtime.
- DNS Name Server Availability: Less than 31 minutes of downtime per month (At least 99.93% availability)
- TCP DNS resolution RTT: 300ms for at least 95% of the queries
- UDP DNS resolution RTT: 300ms for at least 95% of the queries
- DNS update time: 15 min, for at least 95% of the probes

#### RDDS (WHOIS)

- RDDS Availability: Less than 43 minutes of downtime per month. (At least 99.9% availability)
- RDDS Query RTT: Less than 400 ms.
- RDDS Update Time: Less than 15 minutes for 95% of probes.

## EPP

- EPP Service Availability: Less than 43 minutes of downtime per month. (At least 99.9% availability)
- EPP Session-Command RTT: Less than 1000 ms for at least 95% of commands.
- EPP Query-Command RTT: Less than 400 ms for at least 95% of commands.
- EPP Transform-Command RTT: Less than 800 ms for at least 95% of commands.

Downtime values are on a monthly basis.

Google has the track record to deliver SRS to 99.9% availability. Google is confident in its ability to meet these SLAs for SRS because of its experience with engineering highly-available platforms. As discussed by Urs Hoelzle, Senior Vice President of Technical Architecture, Google has designed its major services to obtain 99.99% reliability [1].

#### 24.9. SRS Technical Support

Charleston Road Registry will provide registrars with access to telephone, email, and web chat support, and will escalate issues to the Google technical team as technical faults are identified. For a further elaboration of the escalation process, see Question 42.

Google will notify ICANN and registrars, at least 24 hours beforehand, of maintenance for all planned outages and maintenance which will directly, significantly, and visibly affect users of the SRS.

#### 24.10. Resourcing Plans

Google will implement these technical requirements using the teams and resources discussed below.

The cost of these services will generally be set at reasonable market rates per agreement between Charleston Road Registry and Google. The expected costs are discussed in Questions 46 and 47.

All services that GSRS will depend on are already well-provisioned and ready to assume the additional load of the Google SRS, including up to 100 million second-level domains, which is well in excess of expected need. The load that GSRS will generate for existing systems will be significantly less than the capacity already designated as part of normal growth for Google and the company's need for high-performance hardware and support personnel resources.

##### 24.10.1. Registry Team

The Google Registry Team will be responsible for designing and implementing our SRS, EPP, and WHOIS systems, including IDNs. They will also be responsible for creating tests and monitoring for these systems.

During initial implementation, this team will consist of at least four to seven software engineers responsible for implementing the project. Additionally, Google plans to staff one software engineer who is responsible for engineering testing and monitoring for the Google Registry, and one software engineer who is responsible for backup, restoration and escrow. In total, Google plans to implement the Google Registry with a team of six to nine software engineers.

After the Google Registry is complete, Google expects to staff a team to support the ongoing operation of the registry. This team will consist of at least four engineers who will participate in on-call rotation, respond to alerts, provide support to ICANN and registrars for emergency escalations, and maintain responsibility for bug fixes and improvements. This team will continue maintenance throughout the life of the registry.

This team's responsibilities will generally be limited to registry-specific components. The Google Registry Team will work closely with other relevant



teams, including the Authoritative DNS support team, Storage Site Reliability Engineering team, network engineering and operations, and customer support teams. These other teams are described in more detail in Question 31 (Section 31.16) as well as the relevant sections throughout this application.

#### 24.11. Summary and Key Insights

Google has an existing production infrastructure that can exceed the performance requirements of the SRS platform:

- Google has a global network of datacenters to provide the scalability to meet the performance requirements of SRS.
- Google has a multi-master high availability strategy to meet the reliability requirements of SRS.
- Google has the proven operational processes and personnel to support the requirements going forward.
- The use of Google's platform allows Charleston Road Registry to commit to service levels that substantially exceed the ICANN requirements in Specification 10.

#### 24.12. Footnotes

[1] New York Times, "99.999% Reliable? Don't Hold Your Breath".  
<http://www.nytimes.com/2011/01/09/business/09digi.html>

## 25. Extensible Provisioning Protocol (EPP)

The primary purpose of Google EPP will be to provide for a provisioning interface to the Google Registry using the standardized EPP protocol.

Google has no initial plans to provide a software development kit, since there already are a variety of open- and closed-source EPP client implementations available on the web today.

Google's EPP service will act as a connector between EPP clients and Google's backend systems, which will handle business logic for registry operations.

### 25.1. RFC Compliance

Google's EPP interface will handle the follow tasks:

- Listen for EPP connections over port 700.
- Support and maintain the EPP session through the life of the connection.
- Translate EPP requests and responses between equivalent requests and responses exposed by the Google SRS Backend private API.
- Terminate the Transport Security Layer (TLS) connection as defined by RFC 5734. TLS client certificates will be self-certified and transmitted to Google via the registrar application process. The credentials in the certificate will be matched against the account identified by the EPP username and password.

Google EPP will support a well defined set of EPP RFCs with a small set of additional, well-defined EPP extensions.

#### 25.1.1. Core Protocol - RFC 5730 (<http://tools.ietf.org/html/rfc5730>)

RFC 5730 defines EPP, a simple object provisioning XML protocol. The base protocol itself is agnostic to the type of objects being provisioned and allows for extensions to the protocol.

Upon connection, a session is established with a <greeting> message from the server as defined by the RFC. From there, the client will login with a <login> command, then entertain a series of request and response cycles, and

then finally ends the session with a `<logout>` command.

All EPP commands will be supported according to the RFC in their standard command and response formats.

As part of the `<greeting>`, a `<dcg>` element is presented indicating Google's data-collection-policy for the Registry. In general, the `<dcg>` element will attempt to mirror (as far as the protocol can mirror) Google's Privacy Policy as stated in <http://www.google.com/policies/privacy/>. A copy of our full Privacy Policy as of March 1, 2012, is also included in Question 31 as an attachment.

For all commands, only objects defined by RFCs 5731 (domains), 5732 (hosts), and 5733 (contacts) will be supported. No other extensions will be used.

For the `<login>` command, the following policy specifics will be implemented:

- A maximum of three failed login attempts per connection
- On the 12th failed login attempt, the account will be locked out and require support to reactivate.
- Changing the EPP password with the optional `<newPW>` element will not be supported. Password changes will instead be handled through the password change interface on the Google SRS Front End. Error code 2501, "Authentication error; server closing connection" will always be returned if this command is used.
- The `<version>` element must be set to 1.0.
- The `<lang>` element must be set to "en".

For all other EPP commands there will be no implementation policy specifics.

Standard behavior as defined by the RFC for each command is expected:

- `<check>` : Determine if an object can be provisioned within the registry
- `<info>` : Retrieve information associated with a given object
- `<poll>` : Discover and retrieve service messages by a server for individual clients
- `<create>` : Create an instance of an object
- `<delete>` : Remove an instance of an existing object
- `<renew>` : Extend the validity of an existing object
- `<transfer>` : Determine real-time status of pending and completed transfer requests
- `<transfer op="request">` : Request that an object be transferred
- `<transfer op="approve">` : Approve a transfer request
- `<transfer op="reject">` : Reject a transfer request
- `<transfer op="cancel">` : Cancel a transfer request
- `<update>` : Update the information in an existing object

#### 25.1.2. Domain Objects - RFC 5731 (<http://tools.ietf.org/html/rfc5731>)

RFC 5731 defines support for domain objects over the EPP protocol.

Since RFC 5732 will be supported as well, domain objects will not be able to specify attributes to describe a name server host machine, but rather must reference the relevant host with `<domain:hostObj>` references.

When `<domain:authInfo>` is used, a `<domain:pw>` must be passed within to denote the password for the domain (or registrant using the "roid" attribute to denote this), or a `<domain:null>` to null it out.

For EPP commands dealing with domain object validity, domains will be by default valid indefinitely unless otherwise specified.

A 2305 error response code will be issued if there are dependent children subordinate to the domain, which still exist in the repository if a `<delete>` command is issued.

For all domains which require additional vetting of the registrant because of

gTLD registration policy reasons, offline review of the domain may occur for transformation EPP commands. Otherwise, no offline review will occur in general.

#### 25.1.3. Host Objects - RFC 5732 (<http://tools.ietf.org/html/rfc5732>)

RFC 5732 provides EPP mappings for host objects. This RFC will be supported in its entirety. There are no special considerations needed for the Google Registry.

There will be no offline review before provisioning of any host.

#### 25.1.4. Contact Objects - RFC 5733 (<http://tools.ietf.org/html/rfc5733>)

This RFC provides EPP mapping for contact objects. This RFC will be supported in its entirety.

As specified by the RFC, unless prohibited by the server's stated data collection policy, per-field disclosure policies will be supported via the `<contact:disclose>` element when provisioning contacts.

There will be no offline review before provisioning of any contact.

#### 25.1.5. EPP Transport over TCP - RFC 5734 (<http://tools.ietf.org/html/rfc5734>)

RFC 5734 defines connection handling procedures regarding the EPP mechanism.

The following policy is adopted from suggestions from this RFC:

- There will be no more than ten concurrent TCP connections from a single source destination IP without first contacting Google to establish an alternate upper limit.
- If a well-formed EPP request is not received at least every 30 seconds, the TCP/IP connection may be severed.
- TLS is mandatory to connect to Google EPP.
- A single TLS client certificate will be required for each EPP user and password pair. Multiple user/password pairs will not be permitted for a single TLS client certificate.
- A Certificate Name (CN) and subject AltName:dnsName will be set to the hostname of GEPP to be validated against by the client.

#### 25.1.6. DS records - RFC 5910 (<http://tools.ietf.org/html/rfc5910>)

RFC 5910 governs the additions to the EPP domain mapping RFC for provisioning DS records for a particular domain. Of the two possible supported mechanisms by the RFC, Google EPP will support the "DS Data Interface", where the client is responsible for the creation of the DS information and is required to pass DS information when performing adds and removes.

Other particular implementation specifics include:

- The optional `<secDNS:maxSigLife>` element will not be initially supported, and a 2102 error code will be returned.
- `<secDNS:update>` with an attribute of `urgent` will not be initially supported, and a 2102 error code will be returned if present.

#### 25.1.7. Grace periods - RFC 3915 (<http://tools.ietf.org/html/rfc3915>)

RFC 3915 extends the EPP RFCs to account for grace period functionality. Grace periods allow for actions to be reversed or revoked within a specified period of time. In particular, this RFC governs four grace periods: add grace period, auto renew grace period, renew grace period and transfer grace period. Google will comply with this RFC in its entirety.

#### 25.1.8. IDN RFCs

In addition to RFCs directly related to EPP, RFCs defining internationalized domain names (IDN) (5890, 5891, 5892, and 5893) and how they are specified will be implemented for Google EPP. In particular, IDNs will be specified using punycode and in the subset of unicode character code points dictated by the IDN tables attached to this gTLD application.

## 25.2. EPP Extensions

A small set of well-defined EPP extensions will also be supported.

### 25.2.1. Launch Phase Mapping for EPP

This draft RFC is currently found here:

<http://tools.ietf.org/html/draft-tan-epp-launchphase>

It defines mappings to create domains and application for domains during "launch" phases. It will be supported in its entirety.

The following launch phases will be used by CRR:

- Sunrise
- Landrush
- Claims

Only encoded signed marks will be accepted in order to minimize signature validation issues.

### 25.2.2. Mark and Signed Mark Objects Mappings

This draft RFC is currently found here:

<http://tools.ietf.org/html/draft-lozano-tmch-smd>

It defines mappings for Mark and Signed Mark objects onto XML. It will be supported in its entirety, as necessitated by 25.2.1.

### 25.2.3. Premium Domain Names Pricing Extension

This extension is currently found here:

<http://ausregistry.github.io/doc/price-1.0/price-1.0.html>

It defines an EPP extension to request and return pricing information on premium domains. It also provides a mechanism for registrars to acknowledge and verify the pricing information on a premium domain before registering it. The extension will be supported in its entirety.

### 25.2.4 Namestore Extension

This extension is currently found here:

<http://www.verisigninc.com/assets/namestore-extension.pdf>

It defines a mechanism for registrars to specify which TLD their EPP command is addressed against. It will be used to multiplex many different TLDs in a single EPP endpoint. It will be supported in its entirety.

## 25.3. Google EPP Testing

Google will develop Google EPP using a software methodology, which ensures correct functionality by concurrently developing unit and large functional tests alongside the production code itself. Standard XML parsing libraries will be used depending on the implementation language. Implementation will also include monitoring rules that test EPP workflows in production on an ongoing basis. Before deploying to production, Google will create staging environments during development for internal manual and automated testing.

## 25.4. Operational Testing and Evaluation for Registrars

All ICANN-accredited registrars must first complete operational testing and

evaluation (OT&E) before submitting EPP commands through the production Google EPP environment. The aim of this testing is to ensure that registrars are functioning properly.

OT&E instructions will be presented to the registrar after it has created a registrar account with the Google Registry. In general, these instructions will include a series of ordered EPP commands the registrar must perform along with test account credentials.

The registrar, once the registrar is ready for certification, it will request a Google Registry Front End evaluation. The test environment will reset to a nominal state, and at this point, the registrar must execute the series of ordered EPP commands within a specified amount of time. If registrar fails OT&E, the registrar will be notified of the failure, and can try again at a later date. If the registrar passes OT&E, the registrar will be notified, and be given production EPP credentials.

#### 25.5. Resourcing Plans

Google Inc. will implement these technical requirements using the teams and resources discussed below.

The cost of these services will generally be set at reasonable market rates per agreement between Charleston Road Registry and Google. The expected costs are discussed in Questions 46 and 47.

##### 25.5.1. Registry Team

The Registry Team will be responsible for designing and implementing the shared registration system (SRS), EPP, and WHOIS systems, including IDNs. They will also be responsible for creating tests and monitoring for these systems.

During initial implementation, this team will consist of at least four to seven software engineers responsible for implementing the project. Additionally, Google plans to staff one software engineer who is responsible for engineering testing and monitoring for the registry, and one software engineer who is responsible for backup, restoration and escrow. In total, Google plans to implement the registry with a team of six to nine software engineers.

After the registry is complete, Google expects to staff a team to support the ongoing operation of the registry. This team will consist of at least four engineers who will participate in on-call rotation, respond to alerts, provide support to ICANN and registrars for emergency escalations, and maintain responsibility for bug fixes and improvements. This team will continue maintenance throughout the life of the registry.

This team's responsibilities will generally be limited to registry-specific components. The Registry Team will work closely with other relevant teams, including the Authoritative DNS support team, Storage Site Reliability Engineering team, network engineering and operations, and customer support teams. These other teams are described in more detail in Question 31 (Section 31.16), as well as the relevant sections throughout this application.

#### 25.6. Summary and Key Insights

Google can design, build and run EPP interface that meets the requirements of a gTLD registry because of:

- A thorough understanding of the requirements for the systems.
- A reuse of existing industry, standard EPP XML schemas to de-risk system implementation.
- A proven software development methodology that will verify implementation against requirements.
- Operational procedures that facilitate the ongoing maintenance of the platform and the support of onboarding of new registrars.

## 26. Whois

Google will implement and maintain a "thick" data model WHOIS service, in which the registry will store and serve contact information related to each domain name -- as opposed to a "thin" model, which provides a query referral to a registrar.

Google will operate a public WHOIS service available via port 43 in accordance with RFC 3912, and a web-based Directory Service at <WHOIS.nic.web> providing free, public query-based access. Both of these services will be made available over both IPv4 and IPv6.

Google's WHOIS service on port 43 will comply with the WHOIS protocol as described in RFC 3912 by accepting an ASCII request (terminated with a <CR> <LF> ) and replying with an ASCII response, terminating the TCP connection once the output is finished. RFC 3912 does not contain further detail on the format of the response payload itself; the format will be as described in "SPECIFICATION 4: SPECIFICATION FOR REGISTRATION DATA PUBLICATION SERVICES", Section 1, and relevant Best Practices.

If ICANN specifies alternative formats and protocols, Google will implement these as soon as reasonably practical and will implement IDN related WHOIS requirements as they evolve. As a matter of policy, Google WHOIS will not return IDN variants for WHOIS queries. Queries for specific domains must be made.

### 26.1 High-level overview of the WHOIS service.

The attachment "Q26\_WHOIS Services Diagram" shows an overview diagram of WHOIS services, and other relevant aspects of Google's network.

#### Step 1: Request.

When a request is received (via the web or "traditional" interface), the appropriate service will extract the query from the request and perform checks to combat abusive behavior (such as Denial of Service and "WHOIS scraping"). Google has extensive infrastructure that profiles requests and applies heuristics to determine if requests are legitimate or "scraping", and we plan to use this infrastructure to limit abuse of the WHOIS service. This functionality is described in Question 30, Section 30.b.3.2.

The request will also increment a counter to allow for reporting of statistics.

#### Step 2: Lookup.

The service will then query the registry database service, using the GSRS backend API. As the WHOIS service will query the database for the response, Google will provide fresh answers, instead of extracting all of the data from the database and synchronizing the data between servers. In order to provide fast, accurate responses, and to act as the first line of defense against DoS attacks, the WHOIS service may cache the result and reply from cache on subsequent queries for a maximum of 15 minutes.

#### Step 3: Reply

Once a result, or an indication that the requested information does not exist, is received from the database it will be converted into the appropriate response format: HTML for web-based requests, or RFC 3912 style responses for port 43 requests.

#### Step 4: Response.

The result of the lookup will then be returned to the requester.

## 26.2. WHOIS Infrastructure

Google operates a fast, reliable, and redundant network, and has developed frameworks for encoding and making remote procedure calls (RPCs). This infrastructure can be leveraged to provide communication and connectivity with other registry systems.

Google has significant experience developing secure, stable, resilient, and high-performance applications that perform lookups against a datastore, and has built substantial infrastructure for running such applications and scaling them to meet demand.

As described in detail in the responses to Questions 31 and 32, the WHOIS service will be designed as a simple, stateless server that accepts user queries and transforms them into RPCs that will be serviced by the SRS backend server. This model allows additional capacity to be scaled in accordance with need simply by adding additional replicas of the WHOIS server, and means that the resource requirements to operate this layer of the service should be minimal. Google continuously monitors the load on production servers and systems and proactively upgrades and supplements systems before there is any degradation in service. The registry will be initially provisioned to support at least 100 million domain names, which substantially exceeds the expected load, but Google's overall scale would allow the scope of the service to be increased substantially if required.

We estimate that each second-level domain will generate slightly more than 3 WHOIS queries per day. Based on our projections, this will result in an expected load of 3600 qps (queries per second) from WHOIS requests. Since each machine can handle 250 qps, and we plan for a 50% utilization rate, we expect to provision about 30 machines. For more details of our expected WHOIS load and performance capacity, see Question 24.

This infrastructure will also help Google meet and exceed the specified Service Level Agreements, including those in Section 10 of the Registry Agreement, as discussed in the response to Question 24. We plan to serve WHOIS queries with at least 99.9% availability, with less than 500 ms latency, and an update time of less than 15 minutes for 95% of updates.

## 26.3 WHOIS Synchronization

As mentioned in previous sections, all incoming RPCs to equivalent calls to the Google SRS Backend. This means that there is no synchronization between Google WHOIS and the SRS since Google WHOIS maintains no persistent state. However, as also previously mentioned, Google may deploy a cache in the WHOIS service to reduce load on the GSRS BE and database while reducing latency, creating a freshness delay of up to 15 minutes.

## 26.4. WHOIS Data and Request/Response Example

Google WHOIS will follow data formats specified in Specification 4 in the application guidebook. Here is an example WHOIS domain query and response.

Query::

EXAMPLE.web

Response:

Domain Name: EXAMPLE.web

Domain ID: D424242-web

WHOIS Server: WHOIS.nic.web

Updated Date: 2012-08-13T20:13:00Z

Creation Date: 2012-02-14T00:45:00Z

Registry Expiry Date: 2014-10-08T00:44:59Z

Sponsoring Registrar: EXAMPLE REGISTRAR LLC

Sponsoring Registrar IANA ID: 314159265

Domain Status: clientDeleteProhibited  
Domain Status: clientRenewProhibited  
Domain Status: clientTransferProhibited  
Domain Status: serverUpdateProhibited  
Registrant ID: 5372808-ERL  
Registrant Name: EXAMPLE REGISTRANT  
Registrant Organization: EXAMPLE ORGANIZATION  
Registrant Street: 123 EXAMPLE STREET  
Registrant City: ANYTOWN  
Registrant State/Province: AP  
Registrant Postal Code: A1A1A1  
Registrant Country: EX  
Registrant Phone: +1.5555551212  
Registrant Phone Ext: 1234  
Registrant Fax: +1.5555551213  
Registrant Fax Ext: 4321  
Registrant Email: EMAIL@EXAMPLE.web  
Admin ID: 5372809-ERL  
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE  
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION  
Admin Street: 123 EXAMPLE STREET  
Admin City: ANYTOWN  
Admin State/Province: AP  
Admin Postal Code: A1A1A1  
Admin Country: EX  
Admin Phone: +1.5555551212  
Admin Phone Ext: 1234  
Admin Fax: +1.5555551213  
Admin Fax Ext:  
Admin Email: EMAIL@EXAMPLE.web  
Tech ID: 5372811-ERL  
Tech Name: EXAMPLE REGISTRAR TECHNICAL  
Tech Organization: EXAMPLE REGISTRAR LLC  
Tech Street: 123 EXAMPLE STREET  
Tech City: ANYTOWN  
Tech State/Province: AP  
Tech Postal Code: A1A1A1  
Tech Country: EX  
Tech Phone: +1.1235551234  
Tech Phone Ext: 1234  
Tech Fax: +1.5555551213  
Tech Fax Ext: 93  
Tech Email: EMAIL@EXAMPLE.web  
Name Server: NS01.EXAMPLEREGISTRAR.web  
Name Server: NS02.EXAMPLEREGISTRAR.web  
DNSSEC: signedDelegation  
DNSSEC: unsigned  
) ) ) Last update of WHOIS database: 2012-08-13T20:15:00Z < < <

## 26.5 Bulk Registration Data Access to ICANN

The Google Registry will comply with Section 3 of Specification 4 in the application guidebook to provide ICANN bulk registration data access.

Data will be provided on a weekly basis. Data will include data committed as of 00:00:00 UTC on the day previous to the one designated for retrieval by ICANN.

The Google Registry will provide at a minimum all content requested in the specification: domain name, domain name repository, object id, registrar id, statuses, last updated date, creation date, expiration date, and name server names. For sponsoring registrars, the registry will provide: registrar name, registrar repository object id, hostname of registrar Whois server, and URL of registrar.



The format of the data will be provided as specified in Specification 2 for Data Escrow.

The Google Registry will have the file ready for download as of 00:00:00 UTC on the day designated for retrieval by ICANN. The file will be made available for download by SFTP with a hostname, username, and password provided to ICANN.

#### 26.6. Resourcing

Google Inc. will implement these technical requirements using the teams and resources discussed below.

The cost of these services will generally be set at reasonable market rates per agreement between Charleston Road Registry and Google. The expected costs are discussed in Questions 46 and 47.

##### 26.6.1. Registry Team

Our Registry Team will be responsible for designing and implementing our SRS, EPP, and WHOIS systems, including IDNs. They will also be responsible for creating tests and monitoring for these systems.

During initial implementation, this team will consist of at least 4-7 software engineers responsible for implementing the project. Additionally, we plan to staff one software engineer who is responsible for engineering testing and monitoring for the registry, and one software engineer who is responsible for backup, restoration and escrow. In total, we plan to implement the registry with a team of 6-9 software engineers.

After the registry is complete, we expect to staff a team to support the ongoing operation of the registry. This team will consist of at least four engineers who will participate in on-call rotation, respond to alerts, provide support to ICANN and registrars for emergency escalations, and maintain responsibility for bug fixes and improvements. This team will continue maintenance throughout the life of the registry.

This team's responsibilities will generally be limited to registry-specific components. The Registry Team will work closely with other relevant teams, including the Authoritative DNS support team, Storage Site Reliability Engineering team, network engineering and operations, and customer support teams. These other teams are described in more detail in Question 31 (Section 31.16), as well as the relevant sections throughout this application.

#### 26.7. Summary and Key Insights

- Google will operate a thick WHOIS service with an interface on port 43 complying with RFC 3912 as well as a web-based query interface. These services will display data in accordance with Specification 4 of the registry agreement.
- Google's WHOIS service offers a simple, stateless, scalable front end to the registry's SRS-BE servers. The capacity of the service can be expanded simply by adding additional replica WHOIS servers. Google will initially scale the service to support a registry with 100 million domain names.

## 27. Registration Life Cycle

Charleston Road Registry (CRR) sets forth below a description of the various stages and states of a second-level domain (SLD) in its proposed registry system. Please see "Q27\_Registry Life Cycle Diagram" for a graphical depiction of the domain registration lifecycle.

### 27.1. Life Cycle States

The following registration life cycle states are described in the sections below:

- Reserved
- Available
- Add Grace Period
- Registered
- Renew Grace Period
- Auto-Renew Grace Period
- Pending Restore
- Redemption Grace Period
- Pending Delete
- Pending Transfer
- Transfer Grace Period

State changes provide specific use cases to the DNS (Domain Name System) architecture explained in responses for Question 31 (Technical Overview), Question 32 (Architecture) and Question 35 (DNS Service). Note that this response makes references to EPP (Extensible Provisioning Protocol) functionality which is fully described in Question 25. Additionally, state changes may change the information retrievable via Registration Data Directory Services (RDDS, a combination of WHOIS and Web-based WHOIS) as described in Question 26.

#### 27.2. Reserved

Reserved domains are not generally available to register. For example, such restrictions may result from agreements with ICANN/IANA for operational/technical reasons or with governments for geographic names. See response to Question 22 (Protection of Geographic Names) for further details. The registry will maintain a schedule of reserved words as per Specification 5 of the Registry Agreement. For a reserved domain, an EPP <check> query would return a value of avail="0", and there would be no entry in the zone file or RDDS associated with the domain name. EPP <create> requests will result in a rejection, except those that have prior approval from CRR. The registry foresees two cases as envisioned by Specification 5 of the New gTLD Agreement, particularly applicable to geographic names: 1) CRR releases an SLD for use by the applicable government or country-code manager. In this case, at the end of the registration, the SLD would return to the Reserved state. 2) CRR works with the affected government(s) or country-code manager(s) to permanently make available SLD(s). In this case, at the end of a reservation the string would revert to the Available state.

In addition to an explicit Reserved state, CRR will also support a functional equivalent to reserving through registration. This approach follows the practices of the .info registry. That is, CRR will reserve certain names by registering them for the registry, pursuant to Section 2.6 of the gTLD registry agreement. Names reserved using this approach follow the life cycle described below. Generally, CRR will use the state machine to control reservations but leaves open the possibility of using reservation by registration when more appropriate.

#### 27.3. Available

If a second level domain (SLD) is not reserved, it is considered available if either of the following holds true:

- The SLD has not existed previously.
- The SLD has passed through the Pending Delete state.

Domains that are available do not exist in the zone file or RDDS. The Shared Registry System - Back End (SRS-BE) would return a value of avail="1" when responding to the EPP <check> query for domain in the Available state.

All other states would return a value of avail="0".

#### 27.4. Add Grace Period (AGP)

Names that are selected for registration are entered into the zone file at the start of this five-day add-grace period ( `<addPeriod>` ). Registrars are charged for submitting `<create>` requests to the registry.

The Google SRS-Backend (GSRS-BE) manages the 5-day grace period countdown, including the transition of the state to Registered. During the Add Grace Period, registrars can cancel the registration and receive a credit for the cost of the original registration (with domain names becoming immediately Available or Reserved, as appropriate), subject to ICANN's AGP Limits Policy. GSRS-BE will set the status of the Domain Name to `<addPeriod>` while making the zone file and RDDS updates, and then reset it when grace period ends.

#### 27.5. Registered

Owners of domain names can register them for a period of one to ten years. The registrar may renew the SLD for no less than one and no more than ten years from the current day using the EPP `<renew>` command. GSRS-BE will manage state changes based on expiration date of domains, including updates to the zone file and RDDS. By default, status of the object is "ok". Subsequent EPP `<transform>` commands or actions by SRS-BE may change that value to indicate restrictions present or transformations pending.

#### 27.6 Renew Grace Period (RGP)

Upon receipt of a `<renew>` EPP command, SRS-BE will transition the domain name to the state of Renew Grace Period ( `<renewPeriod>` ). The renew grace period allows registrars to correct the mistaken renewal of an SLD. The Renew Grace Period lasts for five (5) days during which the receipt of a `<delete>` EPP command will result in the crediting back to the registrar the cost of the renewal. After this grace period ends, the domain name will revert to the Registered state. Domains in the RGP may transition to the following states: Redemption Grace Period (by meaning of a delete) or Pending Transfer (by means of a transfer) as described in sections 27.8 and 27.11, respectively.

#### 27.7. Auto-Renew Grace Period (ARGP)

GSRS-BE will automatically renew a registration once it has expired and charge the registrar the current renewal fee. By default, CRR will extend the registration for one year. The ARGP is intended to allow registrars to delete a registration which has been auto-renewed and to receive a refund for the renewal fee. For a predetermined number of days after an automatic renewal, the domain is in state of the Auto-Renew Grace Period ( `<autoRenewPeriod>` ). During this grace period, GSRS-BE will accept requests from the EPP for the existing owner to update, renew, transfer and delete the registration provided there is not a corresponding status that prohibits the transformation. The registrar will then be charged the cost of this new transaction. If the registry happens to receive a `<delete>` EPP command during the ARGP, CRR will credit the cost of a renewal to the registrar. Without intervention, SRS-BE will then update the domain's state to Registered.

#### 27.8. Redemption Grace Period (RdGP)

SLDs that are deleted, such as when a registrar uses the `<delete>` EPP command, then enter the Redemption Grace Period (RdGP) ( `<redemptionPeriod>` ), with the exception of those deleted during the Add Grace Period (see above). The RdGP permits registrars to restore domains that were mistakenly deleted. The RdGP lasts for thirty (30) days. SRS-BE will first check for a `clientDeleteProhibited` or a `serverDeleteProhibited` prohibition before making the transition, and will not make the transition if those prohibitions exist.

Domains which enter this state become non-operational and are removed from the zone file and RDDS. The SRS-BE will accomplish this change by updating the DNS service. GSRS-BE will also set the status to "pendingDelete".

During the RdGP, the SRS-BE will reject all EPP requests other than `<restore>`. Registrars have 30 days to submit a `<restore>` request in order for the transaction to be accepted and the transaction cost credited back to the registrar. Registrars must provide a `<report>` that provides, among other things, a reason (`<resReason>`) and supporting information (`<statement>`) within 5 days (during which time the status will be Pending Restore or `<pendingRestore>`). CRR will not process a `<restore>` without a `<report>`. If a `<restore>` request is not received or if a `<report>` is not received on time, GSRS-BE transitions the domain name to the Pending Delete state. Should a registrar reactivate the domain, SRS-BE will update the DNS zone file and RDDS. When complete, SRS-BE will update the state to Registered.

#### 27.9. Pending Delete

This state is the final stage of the lifecycle prior to the domain again being made available. It lasts for 5 days. During this period, registrars shall not have the ability to reactivate the domain, but would have to wait to make a new request once the domain becomes available. During the Pending Delete phase, the SRS-BE will reject all requests to transform a domain name received through the EPP interface. The status of the domain name will be `<pendingDelete>`. After this stage, the domain shall be removed from the registry's database and once again made available for registration.

#### 27.10. Released/Available

As noted above, at the conclusion of the Pending Delete state, GSRS-BE removes the domain name entirely from its database. It is now available for registrars. See 27.3 above for further details of "Available" state. The exception would be those domain names on the reserved list, which will instead return to the Reserved state after they are released.

#### 27.11. Transfers

CRR and Google will adhere to the 15 March 2009 ICANN Policy on Transfer of Registrations (as well as its successor scheduled to take effect on 1 June 2012). Therefore, registrars are allowed to transfer domains between each other, provided that the states and status allow for it.

Transfer requires the following conditions:

- The domain must be in one of the following states: Add Grace Period, Registered, Renew Grace Period, Transfer Grace Period, or Auto Renew Grace Period.
- Neither a `clientTransferProhibited` nor a `serverTransferProhibited` status must be present.

Provided those two conditions are met, GSRS-BE will set the status to `<pendingTransfer>` while it performs its activities (during this period, the domain is considered to be in the Pending Transfer state). First, the registry will notify both registrars of the pending transfer. The registry will complete the transfer if it receives an `<ACK>` response from the Registrar of Record if received within the first five (5) days. If after five (5) days and the registry has not received any message, the transfer will be automatically completed. If a `<NACK>` response is received from the Registrar of Record, the transfer will be rejected. A rejected transfer would result in the SRS-BE setting the state back to its previous value.

Upon completion of the transfer, CRR will update the zone file and RDDS and send another notification to both registrars. When a transfer is complete, the registration period for the SLD is extended by a year (but not to exceed ten (10) years from the date of the transfer) and the gaining registrar will be

charged for submitting a <transfer> EPP request.

#### 27.11.1. Transfer Grace Period (TGP)

The registry places the domain name into the Transfer Grace Period ( <transferPeriod> ) for the first 5 days after the completion of the <transfer> request. During this time, the Gaining registrar will receive a credit for the cost of the transfer if a <delete> EPP transaction is received. Provided the domain is not deleted, at the end of the 5 day period the domain will return to the Registered state. A transfer received during TGP would result in the domain moving to <pendingTransfer> as described above.

#### 27.12. Resourcing

Google Inc. will implement these technical requirements using the teams and resources discussed below.

The cost of these services will generally be set at reasonable market rates per agreement between Charleston Road Registry and Google. The expected costs are discussed in Questions 46 and 47.

##### 27.12.1. Registry Team

The Registry Team will be responsible for designing and implementing the SRS, EPP, and WHOIS systems, including details related to domain name lifecycle. They will also be responsible for creating tests and monitoring for these systems.

During initial implementation, this team will consist of at least 4-7 software engineers responsible for implementing the project. Additionally, Google plans to staff one software engineer who is responsible for engineering testing and monitoring for the registry, and one software engineer who is responsible for backup, restoration and escrow. In total, Google plans to implement the registry with a team of 6-9 software engineers.

After the registry is complete, Google expects to staff a team to support the ongoing operation of the registry. This team will consist of at least four engineers who will participate in on-call rotation, respond to alerts, provide support to ICANN and registrars for emergency escalations, and maintain responsibility for bug fixes and improvements. This team will continue maintenance throughout the life of the registry.

This team's responsibilities will generally be limited to registry-specific components. The Registry Team will work closely with other relevant teams, including the Authoritative DNS support team, Storage Site Reliability Engineering team, network engineering and operations, and customer support teams. These other teams are described in more detail in Question 31 (Section 31.16), as well as the relevant sections throughout this application.

##### 27.12.2. Customer Services Team

The Google Customer Services Team will be responsible for supporting customers and partners, including life cycle requests. Google has a very large existing customer service team of both internal staff as well as staff contracted through third parties, with many hundreds of dedicated staff members already in place. Since these teams and their management are already in place, no standalone implementation resources are needed.

To continue ongoing maintenance of CRR support needs, Google plans to add additional resources for capacity as needed. Google expects to add a total of approximately fifteen additional personnel (including both Google employees and outside vendors) to support all of CRR's customers and partners. The individual staffing allocation to each TLD is described in Question 47.

### 27.13. Summary and Key Insights

- The registry will support a full registration lifecycle consistent with that offered by other major gTLDs. State changes are triggered by registrar commands via the EPP interface or by the SRS-BE, which manages changes triggered by the passage of time.

## 28. Abuse Prevention and Mitigation

Specifically, we will implement in our internal policies and in our Registry/Registrar and Registration Agreements that all registered domain names will be subject to a Domain Name Anti-Abuse Policy ("Abuse Policy"). The Abuse Policy will provide CRR with broad power to suspend, cancel, or transfer domain names that violate the Abuse Policy. We plan to post the Abuse Policy on a publicly facing website at [nic.web/abuse](http://nic.web/abuse), which will provide a reporting mechanism whereby violations of the policy can be reported by those who are impacted; an easy to find place to report policy violations; "plain language" definitions of what constitutes a "reportable" problem; and compliance processes to provide due process, and sanctions that will be applied, in the case of policy violations. The [nic.web/abuse](http://nic.web/abuse) website will list CRR's Abuse Point of Contact. The Abuse Point of Contact shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of abuse complaints. CRR will ensure that this information is kept accurate and up to date and will be provided to ICANN if and when changes are made. The Abuse Point of Contact will review complaints regarding an alleged violation of the Abuse Policy.

### 28.1. Abuse Tracking

CRR also plans to catalog all abuse communications in Google's customer relationship management (CRM) software using a ticketing system and to maintain records of all abuse complaints for an appropriate amount of time. We shall only provide access to these records to third parties under limited circumstances, such as in response to a subpoena or other such court order or demonstrated official need by law enforcement.

The Abuse Policy will define abuse as an action that:

- a. Causes actual and substantial harm, or is a material predicate of such harm; and
- b. Is illegal or illegitimate, or is otherwise considered contrary to the intention and design of a stated legitimate purpose, if such purpose is disclosed.

### 28.2. Abuse Definitions

The Abuse Policy will also name and provide basic definitions as to what constitutes the abusive registration and/or use of domain names within the TLD. These will include, but not be limited to, the following activities:

1. Unqualified Applicant - not authorized to register domain name;
2. Child Pornography - Web sites that contain content that exploits children, such as child pornography (including cartoon child porn) or content that presents children in a sexual manner;
3. Fake renewal notices - Fake renewal notices are misleading correspondence sent to registrants from an individual or organization claiming to be or to represent the current registrar. These are sent for a variety of deceptive purposes, such as obtaining an unnecessary fee (fraud); getting a registrant to switch registrars unnecessarily ("slamming", or illegitimate market-based switching); or to obtain registrant credentials or authorization codes to facilitate theft of the domain;
4. Cross-TLD Registration Scam - a deceptive sales practice where an existing registrant is sent a notice that another party is interested in or is attempting to register the registrant's domain string in another TLD;

5. Domain kiting/tasting - Registrants may abuse an Add Grace Period through continual registration and deletion of domain names to test their monetization ("tasting"), and re-registration of the same names in order to avoid paying the registration fees ("kiting");
6. Phishing - a Web site fraudulently presenting itself as a trusted site (often a bank) in order to deceive Internet users into divulging sensitive information (e.g. online banking credentials, email passwords);
7. Spam - use of electronic messaging systems from email addresses from domains in the TLD to send unsolicited bulk e-mail;
8. Malware / Botnet Command-and-Control - Malware authors sometimes use domain names as a way to control and update botnets. Botnets are composed of thousands to millions of infected computers under the common control of a criminal. Botnets can be used to perpetrate many kinds of malicious activity, including distributed denial-of-service attacks (DDoS), spam, and fast-flux hosting of phishing sites;
9. Use of Stolen Credentials -such as stolen credit card numbers, to register domain names for malicious purposes;
10. Pharming - redirecting of unknowing users to fraudulent Web sites or services, typically through domain name system (DNS) hijacking or poisoning;
11. Fast flux hosting - use of fast-flux techniques to disguise the location of Web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. Fast flux hosting may be used only with prior permission of CRR;

### 28.3. Abuse Policy Rights Reserved

The Abuse Policy will state, at a minimum, that CRR 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 CRR, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement or any agreement CRR has with any party; (5) to correct mistakes made by CRR, its registry services provider, or any registrar in connection with a domain name registration; (6) during resolution of any dispute regarding the domain; and (7) to remedy the abusive registration or use of any domain name.

### 28.4. Orphan Glue

We will remove orphan glue records for names removed from the zone when provided with evidence in written form to the Abuse Point of Contact that the glue is present in connection with malicious conduct according to Specification 6 of the New gTLD Registry Agreement. Google's back-end systems will also periodically search for orphaned glue. We will inform its registrants that it removes glue if the covering zone is removed, and thus registrants should not reference it from outside the domain.

### 28.5. Resourcing

CRR and its affiliates will commit ample resources for the purpose of implementing its internal policies and its Registry-Registrar and Registration Agreements. As described herein, we will create an Internal Abuse Team, including an Abuse Point of Contact, whose responsibilities will include reviewing, responding, cataloging, and, if applicable, remedying complaints regarding alleged violations of the Abuse Policy. This team will be dedicated to manually reviewing abuse complaints. The roles and responsibilities of the team members are anticipated to include, but are not limited to, the following:

- Reviewing, responding, and if applicable, resolving complaints regarding alleged violations of the Abuse Policy

- Enforcing the Abuse Policy
- Monitoring productivity and efficiency of the manual review process
- Addressing high priority escalations from Law Enforcement quickly
- Collaborating with internal and external partners to drive issues to resolution
- Interface with the technical team to improve workflow, prioritize escalations, create tools for the manual review process

#### 28.6. Anti-abuse Notice and Takedown Procedure

In order to reduce abusive registrations that affect the security of the TLD and its users, CRR plans to provide a domain anti-abuse notice and takedown procedure. Specifically, we will operate an anti-abuse website at the URI address `nic.web/abuse` that will provide the contact information for the Abuse Point of Contact. The `nic.web/abuse` website will prominently display CRR's Abuse Policy and a fill-in section wherein the user will then be asked to fill in several fields, including the user's identity and contact information, and the identity and relevant information of the individual or organization that is making an abusive registration or use of a domain name within the TLD, and specific details on how, why, and when the complainant believes the registration or use of the domain name is abusive. The user will be asked to read the Abuse Policy before it submits a complaint and then click on a check box to indicate that the user has read and understands the Abuse Policy.

#### 28.7. Abuse Response

CRR will then provide a targeted response time as to the decision regarding the complaint. We will review with the Internal Abuse Team and render a decision regarding the alleged abuse, and decide whether to deny, cancel, or transfer any registration or transaction, or place any domain(s) on registry lock, hold, or similar status that violates the Abuse Policy, if applicable. In accordance with the applicable terms of service, CRR reserves the right to terminate the accounts or domains of repeat abusers.

Specifically, the process is anticipated to occur as follows: an email containing the information relayed in the complaint will be sent to the Abuse Point of Contact. The Abuse Point of Contact will send an email to the complainant within twenty-four hours of receiving the complaint confirming receipt of the email. The Abuse Point of Contact will preliminarily review to determine whether the complaint reasonably falls within an abusive use as defined by the Abuse Policy. If the complaint does not, the Abuse Point of Contact will email the complainant within forty-eight business hours of the confirmation email to indicate that the subject of the complaint does not fall within the abusive uses as defined by the Abuse Policy, and that CRR considers the matter closed.

If the preliminary review does not resolve the matter, the Abuse Point of Contact will relay the complaint to CRR's Abuse Team.

All requests from law enforcement will be flagged for prompt review by the Internal Abuse Team. With the resources of Google's registry services team, CRR can meet its obligations under Section 2.8 of the Registry Agreement where required to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its TLD.

In high-priority cases the Internal Abuse Team will seek to determine within forty-eight business hours whether the registration or use of the domain within the TLD is abusive as defined by the Abuse Policy. In all cases, the Internal Abuse Team will determine whether a domain is abusive within seven business days or sooner of receipt of the Complaint. If an abusive use is determined, the Internal Abuse Team may alert the registry services team to immediately suspend resolution of the domain name, as appropriate. Thereafter, if we decide to suspend resolution of the domain name at issue, the Abuse Point of Contact



will immediately notify the abusive domain name registrant of such action, the nature of the complaint, and provide the registrant with the option to respond within ten days. All such actions will be ticketed in Google's CRM software to maintain accurate complaint processing records.

If the registrant responds within ten business days, the Internal Abuse Team will review the response to determine if the registration or use is not abusive. If the Internal Abuse Team is satisfied by the registrant's response, the Abuse Point of Contact will submit a request to the registry services team to reactivate the domain name. If the registrant does not respond within ten business days or the Internal Abuse Team is not satisfied by the registrant's response, the Abuse Point of Contact will notify the registry services team to continue the suspension, transfer or cancel the abusive domain name, as appropriate.

The anti-abuse procedure will not prejudice either party's election to pursue another dispute mechanism, such as the Uniform Rapid Suspension System (URS) or Uniform Domain-Name Dispute-Resolution Policy (UDRP). If CRR's registrar receives notice of a URS or UDRP complaint pertaining to a domain name within the TLD, the registrar will ensure that the domain name is locked within twenty-four hours of receipt of the complaint. The registrar will also notify CRR's Abuse Point of Contact and the registrant.

#### 28.8. Abuse Prevention

In order to further minimize abusive domain name registrations and other activities that have a negative impact on Internet users, CRR will promote the ability to contact a domain registrant using information in WHOIS by providing accessibility in a reliable, consistent, and predictable fashion. CRR will adhere to port 43 WHOIS Service Level Agreements (SLA), which require that port 43 WHOIS service be highly accessible and fast.

CRR will either verify the email address or telephone number provided by the registrant or will require that the registrar do so as a part of registration.

CRR plans to establish policies and procedures to address domain names with inaccurate or incomplete WHOIS data.

As required by Specification 4 of the new gTLD Registry Agreement, CRR will offer thick WHOIS services, in which all authoritative WHOIS data is maintained at the registry. Through CRR's registrar and registry services team, we will maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information, identity of the registrar, domain name's expiration date, nameservers associated with the domain, and specified fields of data for the Registrant Contact, Administrative Contact, and Technical Contact.

CRR will employ query rate limiting and CAPTCHA procedures for its WHOIS database to minimize abuse of its features.

#### 28.9. Summary and Key Insights

Abusive activity on the Internet has been a growing problem, creating security and stability issues for registrants, registrars and users of the Internet in general. CRR intends to address this issue across its TLDs by dedicating ample resources for the purpose of implementing its strict abuse policies and procedures.

## 29. Rights Protection Mechanisms

Abusive registrations and uses of domain names in the global top-level domain (gTLD) will not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet in general. As set forth in prior responses, Charleston Road Registry (CRR) will employ a stringent verification process to establish that every prospective registrant meets the registration criteria. In addition to this verification process, the registry promises to incorporate the following Rights Protection Mechanisms.

### 29.1. Rights Protection Mechanisms - Sunrise Period

Subject to the Sunrise Eligibility Requirements (SERs) outlined herein, Charleston Road Registry (CRR) will offer a Sunrise Period of 60 days for owners of trademarks listed in the Trademark Clearinghouse to register domain names that contain a second level consisting of an identical match to their listed trademarks. In addition, CRR plans to implement a pricing structure to make it easy for brand owners to secure their trademarks and brand names within the gTLD. CRR's registrar will confirm all Sunrise and Registration eligibility. As an added measure of security for brand owners, CRR will staff an internal sunrise team (the "Sunrise Contact") which will review all Sunrise registrations to ensure Sunrise and registration eligibility.

The SERs, which will be verified by Clearinghouse data, will include the following: (i) proof of membership in eligible registrant class, (ii) ownership of a mark that is (a) nationally or regionally registered and for which proof of use, such as a declaration and a single specimen of current use - was submitted to, and validated by, the Trademark Clearinghouse; or (b) that have been court-validated; or (c) that are specifically protected by a statute or treaty currently in effect and that was in effect on or before 26 June 2008; (iii) representation that all provided information is true and correct; and (iv) provision of data sufficient to document rights in the trademark.

Upon submission of all of the required information and documentation, the registrar will review the submissions and verify the trademark and eligibility information and all contact information provided for registration. The registrar shall then send confirmation messages, listing any deficiencies regarding the trademark information provided with the application. If a registrant does not cure any eligibility deficiencies and/or respond by the means listed within one week, the registrar will release the name.

CRR will incorporate a Sunrise Dispute Resolution Policy (SDRP). The SDRP will allow challenges to Sunrise Registrations by third parties for a ten-day period after acceptance of the registration based on the following four grounds: (i) at the time the challenged domain name was registered, the registrant did not hold a trademark registration of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; (ii) the domain name is not identical to the mark on which the registrant based its Sunrise registration; (iii) the trademark registration on which the registrant based its Sunrise registration is not of national or regional effect or the trademark had not been court-validated or protected by statute or treaty; or (iv) the trademark registration on which the domain name registrant based its Sunrise registration did not issue on or before the effective date of the Registry Agreement and was not applied for on or before ICANN announced the applications received.

After receiving a Sunrise Complaint, the Sunrise Contact will review the Complaint to see if the Complaint reasonably asserts a legitimate challenge as defined by the SDRP. If the Complaint does not, the Sunrise Contact will email the complainant within 36 hours of the complaint to indicate that the subject of the complaint does not fall within SDRP, and that CRR considers the matter closed.

If the domain name is not found to have adequately met the SERs, the Sunrise Contact may alert the registrar to immediately suspend resolution of the domain name, as appropriate. Thereafter, the Sunrise Contact will immediately notify the registrant of such action, the nature of the complaint, and provide the registrant with the option to respond within ten days to cure the SER deficiencies or the domain will be canceled. All such actions will be ticketed in Google's customer relationship management (CRM) software to maintain accurate SDRP processing records.

If the registrant responds within ten business days, its response will be reviewed by the Sunrise Contact to determine if the SERs are met. If the Sunrise Contact is satisfied by the registrant's response, it will submit a request by the registry services team to reactivate the domain name. The Sunrise Contact will then notify the Complainant that its complaint was ultimately denied and provide the reasons for the denial. If not, both the registrant and the complainant will be notified that the domain name will be released.

## 29.2. Rights Protection Mechanisms - Trademark Claims Service

CRR will offer a Trademark Claims Service during the Sunrise Period and plans to continue to offer the service for an indefinite period of time thereafter during general registration. CRR will staff an internal team that will be considered the Trademark Claims Contact. The registrar will verify whether any domain name requested to be registered in the gTLD is an identical match of a trademark that has been filed with the Trademark Clearinghouse. It is anticipated that a domain name will be considered an identical match when the domain name consists of the complete and identical textual elements of the mark, and includes domain names where (a) spaces contained within a mark that are either replaced by hyphens (and vice versa) or omitted; (b) certain special characters contained within a trademark are spelled out with appropriate words describing it (e.g., @ and &); and (c) punctuation or special characters contained within a mark that are unable to be used in a second-level domain name are either (i) omitted or (ii) replaced by hyphens or underscores.

If the registrar determines that a prospective domain name registration is identical to a mark registered in the Trademark Clearinghouse, the registrar will provide a "Trademark Claims Notice" ("Notice") in English on the registrar's website to the prospective registrant of the domain name. The Notice will provide the prospective registrant with access to the Trademark Clearinghouse Database information referenced in the Trademark Claims Notice to enhance its understanding of the Trademark rights being claimed by the trademark holder via a link. The Notice will be provided in real time without cost to the prospective registrant.

After receiving the Notice, the registrar will require the prospective registrant to click a link that specifically warrants that: (i) the prospective registrant has received notification that the mark(s) is included in the Clearinghouse; (ii) the prospective registrant has received and understood the Notice; and (iii) the registration and use of the requested domain name will not infringe on the rights that are the subject of the Notice.

CRR reserves the right to adopt other procedures and requirements for the Trademark Claims Service. At a minimum, it is anticipated that after the effectuation of a registration that is identical to a mark listed in the Trademark Clearinghouse, the registrar will then provide a clear notice to the trademark owner of the trademark with an email detailing the WHOIS information of the registered domain name. The trademark owner then has the option of filing a Complaint under the Uniform Domain Name Dispute Resolution Policy (UDRP) and/or the Uniform Rapid Suspension System (URS) against the domain name. As discussed in its right protection mechanisms, CRR will require in its domain name registration agreements that its registry operator and registrar providers, as well as all registrants, submit to the Uniform Domain Name Dispute Resolution Policy (UDRP) and the Uniform Rapid Suspension System (URS)

procedures. CRR and its registrar(s) will abide by decisions rendered under the UDRP and URS on a timely and ongoing basis upon notification.

#### 29.3. Rights Protection Mechanisms - URS

CRR will specify in the Registry Agreement, all Registry-Registrar Agreements, and all Registration Agreements used in connection with the gTLD that it will abide by all decisions made by panels in accordance with the Uniform Rapid Suspension System (URS). CRR's registrar will be tasked with receiving all URS Complaints and decisions. After receiving a URS complaint about a domain name within the gTLD, the registrar will ensure that the domain name is locked within twenty-four (24) hours of receipt of a URS complaint from the URS Provider and will notify CRR's Abuse Point of Contact and the registrant. In the event of a determination in favor of the complainant, the registrant will notify the Abuse Point of Contact and the registry services provider to ensure that the registry suspends the domain name in a timely fashion and has the website at that domain name is redirected to an informational web page provided by the URS Provider about the URS throughout the life of its registration. CRR's Abuse Point of Contact will oversee and monitor the status and resolution of all URS complaints and decisions.

#### 29.4. Rights Protection Mechanisms - UDRP

CRR will specify in the Registry Agreement, all Registry-Registrar Agreements, and all Registration Agreements used in connection with the gTLD, that it will abide by all decisions made by panels in accordance with the Uniform Domain-Name Dispute-Resolution Policy (UDRP). CRR's registrar will be tasked with receiving all UDRP complaints and decisions. After receiving a UDRP complaint about a domain name within the gTLD, the registrar will ensure that the domain name is locked within twenty-four (24) hours of receipt of a UDRP complaint from the UDRP Provider and will notify CRR's Abuse Point of Contact and the registrant. In the event of a determination in favor of the complainant, the registrant will notify the Abuse Point of Contact and the registry services provider to ensure that the registry cancels or transfers the domain name in a timely fashion as provided for by the decision. CRR's Abuse Point of Contact will oversee and monitor the status and resolution of all UDRP complaints and decisions.

#### 29.5. Rights Protection Mechanisms - Proven Registrars

CRR will contract with various ICANN-accredited registrars. CRR is committed to reducing abusive registrations, and will ensure that its registrar operates accordingly.

#### 29.6. Rights Protection Mechanisms - Pre-Authorization and Authentication

CRR will either verify the email address or telephone number provided by the registrant or will require that the registrar do so as a part of registration. CRR will ensure proper access to domain functions by requiring multi-factor authentication from registrants to process update, transfer, and deletion requests.

No name will resolve until the registrant has been verified by the internal team as an eligible registrant.

#### 29.7. Rights Protection Mechanisms - Grace Period

See Question 27 for a detailed discussion of CRR's policies with respect to Add Grace Periods.

#### 29.8. Rights Protection Mechanisms - Domain Anti-Abuse Policy

CRR will implement in its internal policies and its Registry-Registrar and Registration agreements that all registered domain names will be subject to a

Domain Name Anti-Abuse Policy ("Policy"). See Question 28 for a detailed discussion of CRR's Anti-Abuse Policy.

#### 29.9. Resourcing

Google will implement these technical requirements using the teams and resources discussed below.

The cost of these services will generally be set at reasonable market rates per agreement between CRR and Google. The expected costs are discussed in Questions 46 and 47.

##### 29.9.1. Registry Team

The Registry Team will be responsible for designing and implementing the SRS, EPP, and WHOIS systems, including implementation of the rights protection mechanisms. They will also be responsible for creating tests and monitoring for these systems.

During initial implementation, this team will consist of at least 4-7 software engineers responsible for implementing the project. Additionally, Google plans to staff one software engineer who is responsible for engineering testing and monitoring for the registry, and one software engineer who is responsible for backup, restoration and escrow. In total, Google plans to implement the registry with a team of 6-9 software engineers.

After the registry is complete, Google expects to staff a team to support the ongoing operation of the registry. This team will consist of at least four engineers who will participate in on-call rotation, respond to alerts, provide support to ICANN and registrars for emergency escalations, and maintain responsibility for bug fixes and improvements. This team will continue maintenance throughout the life of the registry.

This team's responsibilities will generally be limited to registry-specific components. The Registry Team will work closely with other relevant teams, including the Authoritative DNS support team, Storage Site Reliability Engineering team, network engineering and operations, and customer support teams. These other teams are described in more detail in Question 31 (Section 31.16), as well as the relevant sections throughout this application.

##### 29.9.1. Customer Service Team

The Customer Services Team will be responsible for supporting customers and partners, including responding to abusive registrations. Google has a very large existing customer service team of both internal staff as well as staff contracted through third parties, with many hundreds of dedicated staff members already in place. Since these teams and their management are already in place, no standalone implementation resources are needed.

To continue ongoing maintenance of CRR support needs, Google plans to add additional resources for capacity as needed. Google expects to add a total of approximately fifteen additional personnel (including both Google employees and outside vendors) to support all of CRR's customers and partners. The individual staffing allocation to each gTLD is described in Question 47.

#### 29.10. Summary and Key Insights

CRR is committed to implementing strong and integrated intellectual property rights protection mechanisms. Doing so is critical to Google's goals of model Internet citizenship and fostering Internet development, especially in emerging regions. Accordingly, CRR intends to offer a suite of rights protection measures which builds upon ICANN's required policies while fulfilling our commitment to encouraging innovation, competition, and choice on the Internet.

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

### 30.a. Security Policy

Google plans to use the same common secure infrastructure to support the proposed registry that we use for our other production networks and computing environments. Google currently provides best-in-class security technologies and processes to protect Google's products, services, infrastructure and user data. Google's common secure infrastructure supports some of the web's most widely-used services, such as Google Search YouTube, and Google Apps. These services are used by many millions of consumers, businesses and government customers for their daily operations. Google does not have any plan to support High Security Top Level Domain (HSTLD).

#### 30.a.1. Google Security Policies

Google's security programs are governed through the Google Security Team. The Security Team is led by Google's Vice President of Security, who reports to Google Senior Leadership including the President of Technology and Chief Executive Officer. Google's VP of Security has approved the security policies that underpin Google's information security program.

Our Security Team is committed to:

- Control and maintain the confidentiality, integrity, and availability of information and information systems.
- Limit Google's exposure to the risks arising from loss, corruption or misuse of our information assets.
- Ensuring consistency, which is attained against legal, regulatory, policy and best practice requirements.

Google regularly reviews and updates the security policies that address purpose, scope, responsibilities, management commitment, coordination among organizational entities, and compliance.

To ensure the consistent implementation of security controls across the various layers of infrastructure and services, Google has documented the following security policies.

- Basic Security Policy: States the foundation and principles of Google's Security Policies.
- Physical Security Policy: States how the safety of people and property is protected at Google.
- Accounts Access and Administration Policy: States the kinds of internal accounts Google has and how to access, use, and administer them in a way that reduces risk and provides the ability to audit account activity.
- Data Security Policy: States how data should be handled at Google to help ensure its confidentiality, integrity, and availability.
- Corporate Services Security Policy: Informs Google employees of what to expect regarding access, monitoring, and other security considerations for communications and other data sent, received, or stored using Google's corporate services.
- Network and Computer Security Policy: States how to reduce the likelihood of compromise to Google's data and infrastructure from devices connected to Google networks.
- Applications, Systems, and Services Security Policy: Ensures that adequate attention is paid to security in the design, procurement, development, deployment, and maintenance of Applications, Systems, and Services.
- Change Management Policy: Describes the safeguards that protect Google from accidental or malicious changes to Google's systems.

- Information Security Incident Response Policy: States the minimal requirements for preparing for and responding to information security incidents.
- Datacenter Security Policy: Ensures that adequate attention is given to verifying that each datacenter hosting Google systems maintains security controls that provide protection appropriate to the criticality of those systems.

### 30.a.2. Independent Assessment Reports

Google regularly engages independent assessors to independently assess its information systems, infrastructure and security program and controls for compliance with the following:

- Federal Information Security Management Act (FISMA). Independent assessments conducted every two years. In 2011, Google received FISMA certification for Google Apps Cloud, another service that uses the same production network as the Google registry will use. Grant Thornton LLP performed independent assessment, and United States General Services and Administration (GSA) issued FISMA certification to Google based on this independent assessment.
- Statement on Standards for Attestation Engagements (SSAE16). Independent assessments conducted annually.
- Sarbanes-Oxley (SOX). Independent assessments conducted annually.
- Payment Card Industry (PCI). Independent assessments conducted annually.

Government agencies and Enterprise customers are currently using Google Apps Cloud Services. Google's corporate and production networks were both in scope for FISMA and SSAE16 independent assessments. Google is also currently preparing for ISO 27001 certification of Google Apps Cloud.

### 30.a.3. Commitments made to Registrants

Google will make the following commitments to registrants.

- Google's existing dedicated Security Organization will remain the focal point for ensuring implementation of adequate system security in order to prevent, detect, and recover from security breaches. Various teams in the security organization ensure that Google's infrastructure and services are operated, used, maintained, and disposed of in accordance with internal security policies.
- Google will continue to contemplate threats from internal and external sources, and will exercise our existing incident response capability.
- Google will continue to perform quarterly scanning of our internal and external infrastructure to detect network, database, application, and OS vulnerabilities.
- Google will continue to maintain robust Logging, Monitoring and Auditing capabilities for its systems and networks. These policies are discussed further in Section 30b.
- Google's externally facing network infrastructure will continue to enforce strict access control restrictions to deny all traffic and allow only authorized protocols to enter the Google network.
- Google has established background investigations for all Google employees in accordance with local laws and will continue to do background investigations for any new Google employees.

© Internet Corporation For Assigned Names and Numbers.





# **Annex 6.**



## **New gTLD Application Submitted to ICANN by: Afilias Domains No. 3 Limited,**

**String: WEB**

**Originally Posted: 13 June 2012**

**Application ID: 1-1013-6638**

### **Applicant Information**

#### **1. Full legal name**

Afilias Domains No. 3 Limited,

#### **2. Address of the principal place of business**

Contact Information Redacted

#### **3. Phone number**

Contact Information Redacted

#### **4. Fax number**

Contact Information Redacted

## 5. If applicable, website or URL

<http://www.AfiliasDomains3.info>

## Primary Contact

### 6(a). Name

John Kane

### 6(b). Title

Vice President, Corporate Services

### 6(c). Address

### 6(d). Phone Number

Contact Information Redacted

### 6(e). Fax Number

### 6(f). Email Address

Contact Information Redacted

## Secondary Contact

### 7(a). Name

John Kane

**7(b). Title**

Vice President, Corporate Services

**7(c). Address****7(d). Phone Number**

Contact Information Redacted

**7(e). Fax Number****7(f). Email Address**

Contact Information Redacted

**Proof of Legal Establishment****8(a). Legal form of the Applicant**

limited liability corporation

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

Republic of Ireland

**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.**

Afilias Limited

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

not a joint venture

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

M. Scott Hemphill	Director
Thomas Wade	Director

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

Thomas Wade	CFO
-------------	-----

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

WEB

**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.**

Afilias anticipates the introduction of this TLD without operational or rendering problems. Based on a decade of experience launching and operating new TLDs, Afilias, the back-end provider of registry services for this TLD, is confident the launch and operation of this TLD presents no known challenges. The rationale for this opinion includes:

- The string is not complex and is represented in standard ASCII characters and follows relevant technical, operational and policy standards;
- The string length is within lengths currently supported in the root and by ubiquitous Internet programs such as web browsers and mail applications;
- There are no new standards required for the introduction of this TLD;
- No onerous requirements are being made on registrars, registrants or Internet users, and;
- The existing secure, stable and reliable Afilias SRS, DNS, WHOIS and supporting systems and staff are amply provisioned and prepared to meet the needs of this TLD.

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

## Mission/Purpose

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

Afilias Domains No. 3, the Applicant, is a subsidiary of Afilias Limited, and will be referred to throughout this application as Afilias for simplicity of review by ICANN.

### Mission and purpose

The goal of the .WEB TLD is to help users of the Internet establish meaningful and relevant identities while promoting themselves or their groups, companies or organizations at the same time. This TLD will open up new opportunities for individuals, businesses and organizations to garner a unique piece of the Internet in a space where they can secure the domain name they want but can't have currently.

Businesses and organizations will want to acquire a domain in the .WEB TLD:

- A professional web presence is desired to support merchandising, retailing efforts and business goals.
- Retailers may wish to obtain a .WEB domain to create websites to support or announce planned business offerings and marketing efforts in the "web" arena.
- The web is an indispensable part of virtually every individual's and business' life today.

"As of 2011, more than 2.2 billion people - nearly a third of Earth's population - uses the services of the Internet." (source: Internet World Stats, updated 31 March 2011). Considering that many of this population have

heretofore been unable to get the domain name they desired because it was already taken or reserved in a .com or .net environment, the need for a new TLD with a well-established name in the industry is obvious. And nothing is as synonymous with "Internet" or "net" as the word, "web".

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

The .WEB TLD will be positioned to become one the most-used, professional Internet spaces available.

### **i. General goals**

.WEB will be an open TLD, generally available to all registrants (except in the Sunrise period as described below). The domains can be used for any purpose, including for business use, for personal use and by organizations. There are no content or use restrictions for this TLD.

Afilias will design and position the .WEB TLD to be one of the most popular TLDs on the Internet. The company will market, brand, provide outreach, and offer marketing support to registrars with the goal of gaining public support for the .WEB TLD. This can only be accomplished by creating a user friendly, easy to use, interesting, professionally relevant and entertaining TLD.

### **ii. How .WEB adds to the current space**

On today's Internet, there are hundreds of thousands of companies around the world vying for the attention of potential users and customers. For this precise reason, the .WEB TLD provides an excellent opportunity for companies who elect to participate in the domain to separate themselves from the rest of the .com and .net pack.

The .WEB TLD opens up a tremendous number of options for those companies involved with applications who wish to create a targeted identity on the Internet. In addition, it gives those companies the opportunity to build off the name recognition associated with their brand and name. Any company would be very receptive to being able to associate its own products or services with other quality products and services through the .WEB TLD.

### **iii. User experience goals**

As is the goal of all new gTLDs, this TLD intends to create a space where registrants who desire to participate in the .WEB can create identities where potential users and clients can find the kinds of information they want and need. For example, if you are an organization or company whose business is built around use of the Internet, by belonging to this space you will be able to join forces or share information with other organizations or companies with similar interests and common goals. If an entity or group belongs to the .WEB TLD group, they can be assured they are establishing a presence on the Internet which will:

- a) closely align them with similar brands,
- b) ensure they can keep their own names/brands rather than having to "fit in" to the short list of current TLDs available,
- c) facilitate ease of discovery when searched for by potential customers and users, and
- d) foster confidence of users seeking any information whatsoever regarding applications because this person belongs to the .WEB.

### **iv. Registry policies**

.WEB will be an open TLD, generally available to all registrants except during



the Sunrise period.

.WEB domains will be offered for one to ten years as a general rule with a maximum period of no more than ten years. During the Sunrise period, initial registrations will likely have a minimum requirement for number of years. A requirement may be put in place during Sunrise, for example, that all names must be registered for at least five years.

The roll-out of our TLD is anticipated to feature the following phases:

- Reservation of reserved names and premium names, which will be distributed through special mechanisms (detailed below).
- Sunrise – the required period for trademark owners to secure their domains before availability to the general public. This phase will feature applications for domain strings, verification of trademarks via Trademark Clearinghouse and a trademark verification agent, auctions between qualified parties who wish to secure the same string, and a Trademark Claims Service.
- Land rush – this period provides an opportunity for potential registrations to apply for names prior to the General availability period.
- General Availability period – real-time registrations, made on a first-come first-served basis. Trademark Claims Service will be in use at least for the first 60 days after General Availability applications open.

The registration of domain names in the .WEB TLD will follow the standard practices, procedures and policies Afiliias, the back-end provider of registry services, currently has in place. This includes the following:

- Domain registration policies (for example, grace periods, transfer policies, etc.) are defined in response #27.
- Abuse prevention tools and policies, for example, measures to promote WHOIS accuracy and efforts to reduce phishing and pharming, are discussed in detail in our response #28.
- Rights protection mechanisms and dispute resolution mechanism policies (for example, UDRP, URS) are detailed in #29.

Other detailed policies for this domain include policies for reserved names.

#### Reserved names

##### Registry reserved names

We will reserve the following classes of domain names, which will not be made generally available to registrants via the Sunrise or subsequent periods:

- All of the reserved names required in Specification 5 of the new gTLD Registry Agreement;
- The geographic names required in Specification 5 of the new gTLD Registry Agreement, and may be released to the extent that Registry Operator reaches agreement with the government and country-code manager;
- The registry operator's own name and variations thereof, and registry operations names (such as registry.tld, and www.tld), for internal use;
- Names related to ICANN and Internet standards bodies (iana.tld, ietf.tld, w3c.tld, etc.), and may be released to the extent that Registry Operator reaches agreement with ICANN.

The list of reserved names will be published publicly before the Sunrise period begins, so that registrars and potential registrants will know which names have been set aside.

#### Premium names

The registry will also designate a set of premium domain names, set aside for distribution via special mechanisms. The list of premium names will be

published publicly before the Sunrise period begins, so that registrars and potential registrants will know that these names are not available. Premium names may be distributed via mechanisms such as requests for proposals, contests, direct sales, and auctions.

For the auctioning of premium names, we intend to contract with an established auction provider that has successfully conducted domain auctions. This will ensure that there is a tested, trustworthy technical platform for the auctions, auditable records, and reliable collection mechanisms. With our chosen auction provider, we will create and post policies and procedures that ensure clear, fair, and ethical auctions. As an example of such a policy, all employees of the registry operator and its contractors will be strictly prohibited from bidding in auctions for domains in the TLD. We expect a comprehensive and robust set of auction rules to cover possible scenarios, such as how domains will be awarded if the winning bidder does not make payment.

#### v. Privacy and confidential information protection

As per the New gTLD Registry Agreement, we will make domain contact data (and other fields) freely and publicly available via a Web-based WHOIS server. This default set of fields includes the mandatory publication of registrant data. Our Registry-Registrar Agreement will require that registrants consent to this publication.

We shall notify each of our registrars regarding the purposes for which data about any identified or identifiable natural person ("Personal Data") submitted to the Registry Operator by such registrar is collected and used, and the intended recipients (or categories of recipients) of such Personal Data (the data in question is essentially the registrant and contact data required to be published in the WHOIS). We will require each registrar to obtain the consent of each registrant in the TLD for the collection and use of such Personal Data. The policies will be posted publicly on our TLD web site. As the registry operator, we shall not use or authorize the use of Personal Data in any way that is incompatible with the notice provided to registrars.

Our privacy and data use policies are as follows:

- As registry operator, we do not plan on selling bulk WHOIS data. We will not sell contact data in any way. We will not allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations.
- We may use registration data in the aggregate for marketing purposes.
- DNS query data will never be sold in a way that is personally identifiable.
- We may from time to time use the demographic data collected for statistical analysis, provided that this analysis will not disclose individual Personal Data and provided that such use is compatible with the notice provided to registrars regarding the purpose and procedures for such use.

As the registry operator we shall take significant steps to protect Personal Data collected from registrars from loss, misuse, unauthorized disclosure, alteration, or destruction. In our responses to Question 30 ("Security Policy") and Question 38 ("Escrow") we detail the security policies and procedures we will use to protect the registry system and the data contained therein from unauthorized access and loss.

Please see our response to Question 26 ("WHOIS") regarding "searchable WHOIS" and rate-limiting. That section contains details about how we will limit the mining of WHOIS data by spammers and other parties who abuse access to the WHOIS.

In order to acquire and maintain accreditation for our TLD, we will require registrars to adhere to certain information technology policies designed to help protect registrant data. These will include standards for access to the registry system and password management protocols. Our response to Question 30, "Security Policy" provides details of implementation.

We will allow the use of proxy and privacy services, which can protect the personal data of registrants from spammers and other parties that mine zone files and WHOIS data. We are aware that there are parties who may use privacy services to protect their free speech rights, or to avoid religious or political persecution.

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

Afilias has adopted the above-mentioned and other policies to ensure fair and equitable access and cost structures to the Internet community, including:

- no new burdens placed on the Internet community to resolve name disputes
- utilization of standard registration practices and policies (as detailed in responses to questions #27, #28, #29)
- protection of trademarks at launch and on-going operations (as detailed in the response to question #29)
- fair and reasonable wholesale prices
- fair and equitable treatment of registrars

As per the ICANN Registry Agreement, we will use only ICANN-accredited registrars, and will provide non-discriminatory access to registry services to those registrars.

#### Pricing Policies and Commitments

Pricing for domain names at General Availability will be \$8 per domain year for the first year. Applicant reserves the right to reduce this pricing for promotional purposes in a manner available to all accredited registrars. Registry Operator reserves the right to work with ICANN to initiate an increase in the wholesale price of domains if required. Registry Operator will provide reasonable notice to the registrars of any approved price increase.

## **Community-based Designation**

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

No

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

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

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

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

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

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

Attachments are not displayed on this form.

## Geographic Names

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

No

## Protection of Geographic Names

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

We will protect names with national or geographic significance by reserving the country and territory names at the second level and at all other levels within the TLD, as per the requirements in the New TLD Registry Agreement (Specification 5, paragraph 5).

We will employ a series of rules to translate the geographical names required to be reserved by Specification 5, paragraph 5 to a form consistent with the "host names" format used in domain names.

Considering the Governmental Advisory Committee (GAC) advice "Principles regarding new gTLDs", these domains will be blocked, at no cost to governments, public authorities, or IGOs, before the TLD is introduced (Sunrise), so that no parties may apply for them. We will publish a list of these names before

Sunrise, so our registrars and their prospective applicants can be aware that these names are reserved.

We will define a procedure so that governments can request the above reserved domain(s) if they would like to take possession of them. This procedure will be based on existing methodology developed for the release of country names in the .INFO TLD. For example, we will require a written request from the country's GAC representative, or a written request from the country's relevant Ministry or Department. We will allow the designated beneficiary (the Registrant) to register the name, with an accredited Afiliias Registrar, possibly using an authorization number transmitted directly to the designated beneficiary in the country concerned.

As defined by Specification 5, paragraph 5, such geographic domains may be released to the extent that Registry Operator reaches agreement with the applicable government(s). Registry operator will work with respective GAC representatives of the country's relevant Ministry of Department to obtain their release of the names to the Registry Operator.

If internationalized domains names (IDNs) are introduced in the TLD in the future, we will also reserve the IDN versions of the country names in the relevant script(s) before IDNs become available to the public. If we find it advisable and practical, we will confer with relevant language authorities so that we can reserve the IDN domains properly along with their variants.

Regarding GAC advice regarding second-level domains not specified via Specification 5, paragraph 5: All domains awarded to registrants are subject to the Uniform Domain Name Dispute Resolution Policy (UDRP), and to any properly-situated court proceeding. We will ensure appropriate procedures to allow governments, public authorities or IGO's to challenge abuses of names with national or geographic significance at the second level. In its registry-registrar agreement, and flowing down to registrar-registrant agreements, the registry operator will institute a provision to suspend domains names in the event of a dispute. We may exercise that right in the case of a dispute over a geographic name.

## Registry Services

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

Afiliias Domains No. 3, the Applicant, is a subsidiary of Afiliias Limited, and will be referred to throughout this application as Afiliias for simplicity of review by ICANN.

Afiliias has more experience successfully applying to ICANN and launching new TLDs than any other provider. Afiliias is the ICANN-contracted registry operator of the .INFO and .MOBI TLDs, and Afiliias is the back-end registry services provider for other ICANN TLDs including .ORG, .ASIA, .AERO, and .XXX.

Registry services for this TLD will be performed by Afiliias in the same responsible manner used to support 16 top level domains today. Afiliias supports more ICANN-contracted TLDs (6) than any other provider currently. Afiliias' primary corporate mission is to deliver secure, stable and reliable registry services. This TLD will utilize an existing, proven team and platform for registry services with:

- A stable and secure, state-of-the-art, EPP-based SRS with ample storage capacity, data security provisions and scalability that is proven with

registrars who account for over 95% of all gTLD domain name registration activity (over 375 registrars);

- A reliable, 100% available DNS service (zone file generation, publication and dissemination) tested to withstand severe DDoS attacks and dramatic growth in Internet use;
- A WHOIS service that is flexible and standards compliant, with search capabilities to address both registrar and end-user needs; includes consideration for evolving standards, such as RESTful, or draft-kucherawy-wierds;
- Experience introducing IDNs in the following languages: German (DE), Spanish (ES), Polish (PL), Swedish (SV), Danish (DA), Hungarian (HU), Icelandic (IS), Latvian (LV), Lithuanian (LT), Korean (KO), Simplified and Traditional Chinese (CN), Devanagari (HI-DEVA), Russian (RU), Belarusian (BE), Ukrainian (UK), Bosnian (BS), Serbian (SR), Macedonian (MK) and Bulgarian (BG) across the TLDs it serves;
- A registry platform that is both IPv6 and DNSSEC enabled;
- An experienced, respected team of professionals active in standards development of innovative services such as DNSSEC and IDN support;
- Methods to limit domain abuse, remove outdated and inaccurate data, and ensure the integrity of the SRS, and;
- Customer support and reporting capabilities to meet financial and administrative needs, e.g., 24x7 call center support, integration support, billing, and daily, weekly, and monthly reporting.

Afilias will support this TLD as the registry operator, leveraging a proven registry infrastructure that is fully operational, staffed with professionals, massively provisioned, and immediately ready to launch and maintain this TLD.

The below response includes a description of the registry services to be provided for this TLD, additional services provided to support registry operations, and an overview of Afilias' approach to registry management.

#### Registry services to be provided

To support this TLD, Afilias will offer the following registry services, all in accordance with relevant technical standards and policies:

- Receipt of data from registrars concerning registration for domain names and nameservers, and provision to registrars of status information relating to the EPP-based domain services for registration, queries, updates, transfers, renewals, and other domain management functions. Please see our responses to questions #24, #25, and #27 for full details, which we request be incorporated here by reference.
- Operation of the registry DNS servers: The Afilias DNS system, run and managed by Afilias, is a massively provisioned DNS infrastructure that utilizes among the most sophisticated DNS architecture, hardware, software and redundant design created. Afilias' industry-leading system works in a seamless way to incorporate nameservers from any number of other secondary DNS service vendors. Please see our response to question #35 for full details, which we request be incorporated here by reference.
- Dissemination of TLD zone files: Afilias' distinctive architecture allows for real-time updates and maximum stability for zone file generation, publication and dissemination. Please see our response to question #34 for full details, which we request be incorporated here by reference.
- Dissemination of contact or other information concerning domain registrations: A port 43 WHOIS service with basic and expanded search capabilities with requisite measures to prevent abuse. Please see our response to question #26 for full details, which we request be incorporated here by reference.
- Internationalized Domain Names (IDNs): Ability to support all protocol valid Unicode characters at every level of the TLD, including alphabetic, ideographic and right-to-left scripts, in conformance with the ICANN IDN Guidelines. Please see our response to question #44 for full details, which we request be incorporated here by reference.

- DNS Security Extensions (DNSSEC): A fully DNSSEC-enabled registry, with a stable and efficient means of signing and managing zones. This includes the ability to safeguard keys and manage keys completely. Please see our response to question #43 for full details, which we request be incorporated here by reference.

Each service will meet or exceed the contract service level agreement. All registry services for this TLD will be provided in a standards-compliant manner.

#### Security

Afilias addresses security in every significant aspect—physical, data and network as well as process. Afilias' approach to security permeates every aspect of the registry services provided. A dedicated security function exists within the company to continually identify existing and potential threats, and to put in place comprehensive mitigation plans for each identified threat. In addition, a rapid security response plan exists to respond comprehensively to unknown or unidentified threats. The specific threats and Afilias mitigation plans are defined in our response to question #30(b); please see that response for complete information. In short, Afilias is committed to ensuring the confidentiality, integrity, and availability of all information.

#### New registry services

No new registry services are planned for the launch of this TLD.

#### Additional services to support registry operation

Numerous supporting services and functions facilitate effective management of the TLD. These support services are also supported by Afilias, including:

- Customer support: 24x7 live phone and e-mail support for customers to address any access, update or other issues they may encounter. This includes assisting the customer identification of the problem as well as solving it. Customers include registrars and the registry operator, but not registrants except in unusual circumstances. Customers have access to a web-based portal for a rapid and transparent view of the status of pending issues.
- Financial services: billing and account reconciliation for all registry services according to pricing established in respective agreements.

Reporting is an important component of supporting registry operations. Afilias will provide reporting to the registry operator and registrars, and financial reporting.

#### Reporting provided to registry operator

Afilias reporting provides an extensive suite of reports, including daily, weekly and monthly reports with data at the transaction level that enable us to track and reconcile at whatever level of detail preferred. Afilias provides the exact data required by ICANN in the required format to enable the registry operator to meet its technical reporting requirements to ICANN.

In addition, Afilias offers access to a data warehouse capability that will enable near real-time data to be available 24x7. Afilias' data warehouse capability enables drill-down analytics all the way to the transaction level.

#### Reporting available to registrars

Afilias provides an extensive suite of reporting to registrars and has been doing so in an exemplary manner for more than ten years. Specifically, Afilias provides daily, weekly and monthly reports with detail at the transaction level to enable registrars to track and reconcile at whatever level of detail they prefer.

Reports are provided in standard formats, facilitating import for use by

virtually any registrar analytical tool. Registrar reports are available for download via a secure administrative interface. A given registrar will only have access to its own reports. These include the following:

- Daily Reports: Transaction Report, Billable Transactions Report, and Transfer Reports;
- Weekly: Domain Status and Nameserver Report, Weekly Nameserver Report, Domains Hosted by Nameserver Weekly Report, and;
- Monthly: Billing Report and Monthly Expiring Domains Report.

Weekly registrar reports are maintained for each registrar for four weeks. Weekly reports older than four weeks will be archived for a period of six months, after which they will be deleted.

#### Financial reporting

Registrar account balances are updated real-time when payments and withdrawals are posted to the registrars' accounts. In addition, the registrar account balances are updated as and when they perform billable transactions at the registry level.

Afilias provides Deposit/Withdrawal Reports that are updated periodically to reflect payments received or credits and withdrawals posted to the registrar accounts.

The following reports are also available: a) Daily Billable Transaction Report, containing details of all the billable transactions performed by all the registrars in the SRS, b) daily e-mail reports containing the number of domains in the registry and a summary of the number and types of billable transactions performed by the registrars, and c) registry operator versions of most registrar reports (for example, a daily Transfer Report that details all transfer activity between all of the registrars in the SRS).

#### Afilias approach to registry support

Afilias is dedicated to managing the technical operations and support of this TLD in a secure, stable and reliable manner. Afilias has reviewed specific needs and objectives of this TLD. The resulting comprehensive plans are illustrated in technical responses #24-44. Afilias has provided financial responses for this application which demonstrate cost and technology consistent with the size and objectives of this TLD.

Afilias is the registry services provider for this and several other TLD applications. Over the past 11 years of providing services for gTLD and ccTLDs, Afilias has accumulated experience about resourcing levels necessary to provide high quality services with conformance to strict service requirements. Afilias currently supports over 20 million domain names, spread across 16 TLDs, with over 400 accredited registrars.

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

With over a decade of registry experience, Afilias has the depth and breadth of experience that ensure existing and new needs are addressed, all while meeting or exceeding service level requirements and customer expectations. This is evident in Afilias' participation in business, policy and technical organizations supporting registry and Internet technology within ICANN and



related organizations. This allows Afiliias to be at the forefront of security initiatives such as: DNSSEC, wherein Afiliias worked with Public Interest Registry (PIR) to make the .ORG registry the first DNSSEC enabled gTLD and the largest TLD enabled at the time; in enhancing the Internet experience for users across the globe by leading development of IDNs; in pioneering the use of open-source technologies by its usage of PostgreSQL, and; being the first to offer near-real-time dissemination of DNS zone data.

The ability to observe tightening resources for critical functions and the capacity to add extra resources ahead of a threshold event are factors that Afiliias is well versed in. Afiliias' human resources team, along with well-established relationships with external organizations, enables it to fill both long-term and short-term resource needs expediently.

Afiliias' growth from a few domains to serving 20 million domain names across 16 TLDs and 400 accredited registrars indicates that the relationship between the number of people required and the volume of domains supported is not linear. In other words, servicing 100 TLDs does not automatically require 6 times more staff than servicing 16 TLDs. Similarly, an increase in the number of domains under management does not require in a linear increase in resources. Afiliias carefully tracks the relationship between resources deployed and domains to be serviced, and pro-actively reviews this metric in order to retain a safe margin of error. This enables Afiliias to add, train and prepare new staff well in advance of the need, allowing consistent delivery of high quality services.

## Demonstration of Technical & Operational Capability

### 24. Shared Registration System (SRS) Performance

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE " <" and "> " CHARACTERS), WHICH ICANN INFORMS AFILIAS (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE.

Afiliias operates a state-of-the-art EPP-based Shared Registration System (SRS) that is secure, stable and reliable. The SRS is a critical component of registry operations that must balance the business requirements for the registry and its customers, such as numerous domain acquisition and management functions. The SRS meets or exceeds all ICANN requirements given that Afiliias:

- Operates a secure, stable and reliable SRS which updates in real-time and in full compliance with Specification 6 of the new gTLD Registry Agreement;
- Is committed to continuously enhancing our SRS to meet existing and future needs;
- Currently exceeds contractual requirements and will perform in compliance with Specification 10 of the new gTLD Registry Agreement;
- Provides SRS functionality and staff, financial, and other resources to more than adequately meet the technical needs of this TLD, and;
- Manages the SRS with a team of experienced technical professionals who can seamlessly integrate this TLD into the Afiliias registry platform and support the TLD in a secure, stable and reliable manner.

Description of operation of the SRS, including diagrams

Afiliias' SRS provides the same advanced functionality as that used in the .INFO and .ORG registries, as well as the fourteen other TLDs currently supported by Afiliias. The Afiliias registry system is standards-compliant and utilizes proven technology, ensuring global familiarity for registrars, and it is protected by

our massively provisioned infrastructure that mitigates the risk of disaster.

EPP functionality is described fully in our response to question #25; please consider those answers incorporated here by reference. An abbreviated list of Afiliias SRS functionality includes:

- Domain registration: Afiliias provides registration of names in the TLD, in both ASCII and IDN forms, to accredited registrars via EPP and a web-based administration tool.
- Domain renewal: Afiliias provides services that allow registrars the ability to renew domains under sponsorship at any time. Further, the registry performs the automated renewal of all domain names at the expiration of their term, and allows registrars to rescind automatic renewals within a specified number of days after the transaction for a full refund.
- Transfer: Afiliias provides efficient and automated procedures to facilitate the transfer of sponsorship of a domain name between accredited registrars. Further, the registry enables bulk transfers of domains under the provisions of the Registry-Registrar Agreement.
- RGP and restoring deleted domain registrations: Afiliias provides support for the Redemption Grace Period (RGP) as needed, enabling the restoration of deleted registrations.
- Other grace periods and conformance with ICANN guidelines: Afiliias provides support for other grace periods that are evolving as standard practice inside the ICANN community. In addition, the Afiliias registry system supports the evolving ICANN guidelines on IDNs.

Afiliias also supports the basic check, delete, and modify commands.

As required for all new gTLDs, Afiliias provides "thick" registry system functionality. In this model, all key contact details for each domain are stored in the registry. This allows better access to domain data and provides uniformity in storing the information.

Afiliias' SRS complies today and will continue to comply with global best practices including relevant RFCs, ICANN requirements, and this TLD's respective domain policies. With over a decade of experience, Afiliias has fully documented and tested policies and procedures, and our highly skilled team members are active participants of the major relevant technology and standards organizations, so ICANN can be assured that SRS performance and compliance are met. Full details regarding the SRS system and network architecture are provided in responses to questions #31 and #32; please consider those answers incorporated here by reference.

#### SRS servers and software

All applications and databases for this TLD will run in a virtual environment currently hosted by a cluster of servers equipped with the latest Intel Westmere multi-core processors. (It is possible that by the time this application is evaluated and systems deployed, Westmere processors may no longer be the "latest"; the Afiliias policy is to use the most advanced, stable technology available at the time of deployment.) The data for the registry will be stored on storage arrays of solid state drives shared over a fast storage area network. The virtual environment allows the infrastructure to easily scale both vertically and horizontally to cater to changing demand. It also facilitates effective utilization of system resources, thus reducing energy consumption and carbon footprint.

The network firewalls, routers and switches support all applications and servers. Hardware traffic shapers are used to enforce an equitable access policy for connections coming from registrars. The registry system accommodates both IPv4 and IPv6 addresses. Hardware load balancers accelerate TLS/SSL handshaking and distribute load among a pool of application servers.

Each of the servers and network devices are equipped with redundant, hot-swappable components and multiple connections to ancillary systems. Additionally, 24x7 support agreements with a four-hour response time at all our

data centers guarantee replacement of failed parts in the shortest time possible.

Examples of current system and network devices used are:

- Servers: Cisco UCS B230 blade servers
- SAN storage arrays: IBM Storwize V7000 with Solid State Drives
- SAN switches: Brocade 5100
- Firewalls: Cisco ASA 5585-X
- Load balancers: F5 Big-IP 6900
- Traffic shapers: Procera PacketLogic PL8720
- Routers: Juniper MX40 3D
- Network switches: Cisco Nexus 7010, Nexus 5548, Nexus 2232

These system components are upgraded and updated as required, and have usage and performance thresholds which trigger upgrade review points. In each data center, there is a minimum of two of each network component, a minimum of 25 servers, and a minimum of two storage arrays.

Technical components of the SRS include the following items, continually checked and upgraded as needed: SRS, WHOIS, web admin tool, DNS, DNS distributor, reporting, invoicing tools, and deferred revenue system (as needed).

All hardware is massively provisioned to ensure stability under all forecast volumes from launch through "normal" operations of average daily and peak capacities. Each and every system application, server, storage and network device is continuously monitored by the Afiliias Network Operations Center for performance and availability. The data gathered is used by dynamic predictive analysis tools in real-time to raise alerts for unusual resource demands. Should any volumes exceed established thresholds, a capacity planning review is instituted which will address the need for additions well in advance of their actual need.

SRS diagram and interconnectivity description

As with all core registry services, the SRS is run from a global cluster of registry system data centers, located in geographic centers with high Internet bandwidth, power, redundancy and availability. All of the registry systems will be run in a &lt;n+1&gt; setup, with a primary data center and a secondary data center. For detailed site information, please see our responses to questions #32 and #35. Registrars access the SRS in real-time using EPP.

A sample of the Afiliias SRS technical and operational capabilities (displayed in Figure 24-a) include:

- Geographically diverse redundant registry systems;
- Load balancing implemented for all registry services (e.g. EPP, WHOIS, web admin) ensuring equal experience for all customers and easy horizontal scalability;
- Disaster Recovery Point objective for the registry is within one minute of the loss of the primary system;
- Detailed and tested contingency plan, in case of primary site failure, and;
- Daily reports, with secure access for confidentiality protection.

As evidenced in Figure 24-a, the SRS contains several components of the registry system. The interconnectivity ensures near-real-time distribution of the data throughout the registry infrastructure, timely backups, and up-to-date billing information.

The WHOIS servers are directly connected to the registry database and provide real-time responses to queries using the most up-to-date information present in the registry.

Committed DNS-related EPP objects in the database are made available to the DNS

Distributor via a dedicated set of connections. The DNS Distributor extracts committed DNS-related EPP objects in real time and immediately inserts them into the zone for dissemination.

The Afiliias system is architected such that read-only database connections are executed on database replicas and connections to the database master (where write-access is executed) are carefully protected to ensure high availability.

This interconnectivity is monitored, as is the entire registry system, according to the plans detailed in our response to question #42.

#### Synchronization scheme

Registry databases are synchronized both within the same data center and in the backup data center using a database application called Slony. For further details, please see the responses to questions #33 and #37. Slony replication of transactions from the publisher (master) database to its subscribers (replicas) works continuously to ensure the publisher and its subscribers remain synchronized. When the publisher database completes a transaction the Slony replication system ensures that each replica also processes the transaction. When there are no transactions to process, Slony "sleeps" until a transaction arrives or for one minute, whichever comes first. Slony "wakes up" each minute to confirm with the publisher that there has not been a transaction and thus ensures subscribers are synchronized and the replication time lag is minimized. The typical replication time lag between the publisher and subscribers depends on the topology of the replication cluster, specifically the location of the subscribers relative to the publisher. Subscribers located in the same data center as the publisher are typically updated within a couple of seconds, and subscribers located in a secondary data center are typically updated in less than ten seconds. This ensures real-time or near-real-time synchronization between all databases, and in the case where the secondary data center needs to be activated, it can be done with minimal disruption to registrars.

#### SRS SLA performance compliance

Afiliias has a ten-year record of delivering on the demanding ICANN SLAs, and will continue to provide secure, stable and reliable service in compliance with SLA requirements as specified in the new gTLD Registry Agreement, Specification 10, as presented in Figure 24-b.

The Afiliias SRS currently handles over 200 million EPP transactions per month for just .INFO and .ORG. Overall, the Afiliias SRS manages over 700 million EPP transactions per month for all TLDs under management.

Given this robust functionality, and more than a decade of experience supporting a thick TLD registry with a strong performance history, Afiliias will meet or exceed the performance metrics in Specification 10 of the new gTLD Registry Agreement. The Afiliias services and infrastructure are designed to scale both vertically and horizontally without any downtime to provide consistent performance as this TLD grows. The Afiliias architecture is also massively provisioned to meet seasonal demands and marketing campaigns. Afiliias' experience also gives high confidence in the ability to scale and grow registry operations for this TLD in a secure, stable and reliable manner.

#### SRS resourcing plans

Since its founding, Afiliias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afiliias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade,

are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afiliias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afiliias project management methodology allows efficient and effective use of our staff in a focused way.

Over 100 Afiliias team members contribute to the management of the SRS code and network that will support this TLD. The SRS team is composed of Software Engineers, Quality Assurance Analysts, Application Administrators, System Administrators, Storage Administrators, Network Administrators, Database Administrators, and Security Analysts located at three geographically separate Afiliias facilities. The systems and services set up and administered by these team members are monitored 24x7 by skilled analysts at two NOCs located in Toronto, Ontario (Canada) and Horsham, Pennsylvania (USA). In addition to these team members, Afiliias also utilizes trained project management staff to maintain various calendars, work breakdown schedules, utilization and resource schedules and other tools to support the technical and management staff. It is this team who will both deploy this TLD on the Afiliias infrastructure, and maintain it. Together, the Afiliias team has managed 11 registry transitions and six new TLD launches, which illustrate its ability to securely and reliably deliver regularly scheduled updates as well as a secure, stable and reliable SRS service for this TLD.

## 25. Extensible Provisioning Protocol (EPP)

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE " <" and "> " CHARACTERS), WHICH ICANN INFORMS AFILIIAS (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE.

Afiliias has been a pioneer and innovator in the use of EPP. .INFO was the first EPP-based gTLD registry and launched on EPP version 02/00. Afiliias has a track record of supporting TLDs on standards-compliant versions of EPP. Afiliias will operate the EPP registrar interface as well as a web-based interface for this TLD in accordance with RFCs and global best practices. In addition, Afiliias will maintain a proper OT&E (Operational Testing and Evaluation) environment to facilitate registrar system development and testing.

Afiliias' EPP technical performance meets or exceeds all ICANN requirements as demonstrated by:

- A completely functional, state-of-the-art, EPP-based SRS that currently meets the needs of various gTLDs and will meet this new TLD's needs;
- A track record of success in developing extensions to meet client and registrar business requirements such as multi-script support for IDNs;
- Supporting six ICANN gTLDs on EPP: .INFO, .ORG, .MOBI, .AERO, .ASIA and .XXX
- EPP software that is operating today and has been fully tested to be standards-compliant;
- Proven interoperability of existing EPP software with ICANN-accredited registrars, and;
- An SRS that currently processes over 200 million EPP transactions per month for both .INFO and .ORG. Overall, Afiliias processes over 700 million EPP transactions per month for all 16 TLDs under management.

The EPP service is offered in accordance with the performance specifications defined in the new gTLD Registry Agreement, Specification 10.

### EPP Standards

The Afiliias registry system complies with the following revised versions of the

RFCs and operates multiple ICANN TLDs on these standards, including .INFO, .ORG, .MOBI, .ASIA and .XXX. The systems have been tested by our Quality Assurance ("QA") team for RFC compliance, and have been used by registrars for an extended period of time:

- 3735 - Guidelines for Extending EPP
- 3915 - Domain Registry Grace Period Mapping
- 5730 - Extensible Provisioning Protocol (EPP)
- 5731 - Domain Name Mapping
- 5732 - Host Mapping
- 5733 - Contact Mapping
- 5734 - Transport Over TCP
- 5910 - Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)

This TLD will support all valid EPP commands. The following EPP commands are in operation today and will be made available for this TLD. See attachment #25a for the base set of EPP commands and copies of Afilias XSD schema files, which define all the rules of valid, RFC compliant EPP commands and responses that Afilias supports. Any customized EPP extensions, if necessary, will also conform to relevant RFCs.

Afilias staff members actively participated in the Internet Engineering Task Force (IETF) process that finalized the new standards for EPP. Afilias will continue to actively participate in the IETF and will stay abreast of any updates to the EPP standards.

#### EPP software interface and functionality

Afilias will provide all registrars with a free open-source EPP toolkit. Afilias provides this software for use with both Microsoft Windows and Unix/Linux operating systems. This software, which includes all relevant templates and schema defined in the RFCs, is available on sourceforge.net and will be available through the registry operator's website.

Afilias' SRS EPP software complies with all relevant RFCs and includes the following functionality:

- EPP Greeting: A response to a successful connection returns a greeting to the client. Information exchanged can include: name of server, server date and time in UTC, server features, e.g., protocol versions supported, languages for the text response supported, and one or more elements which identify the objects that the server is capable of managing;
- Session management controls: <login> to establish a connection with a server, and <logout> to end a session;
- EPP Objects: Domain, Host and Contact for respective mapping functions;
- EPP Object Query Commands: Info, Check, and Transfer (query) commands to retrieve object information, and;
- EPP Object Transform Commands: five commands to transform objects: <create> to create an instance of an object, <delete> to remove an instance of an object, <renew> to extend the validity period of an object, <update> to change information associated with an object, and <transfer> to manage changes in client sponsorship of a known object.

Currently, 100% of the top domain name registrars in the world have software that has already been tested and certified to be compatible with the Afilias SRS registry. In total, over 375 registrars, representing over 95% of all registration volume worldwide, operate software that has been certified compatible with the Afilias SRS registry. Afilias' EPP Registrar Acceptance Criteria are available in attachment #25b, EPP OT&E Criteria.

#### Free EPP software support

Afilias analyzes and diagnoses registrar EPP activity log files as needed and is available to assist registrars who may require technical guidance regarding how to fix repetitive errors or exceptions caused by misconfigured client

software.

Registrars are responsible for acquiring a TLS/SSL certificate from an approved certificate authority, as the registry-registrar communication channel requires mutual authentication; Afilias will acquire and maintain the server-side TLS/SSL certificate. The registrar is responsible for developing support for TLS/SSL in their client application. Afilias will provide free guidance for registrars unfamiliar with this requirement.

#### Registrar data synchronization

There are two methods available for registrars to synchronize their data with the registry:

- Automated synchronization: Registrars can, at any time, use the EPP `&lt;info&gt;` command to obtain definitive data from the registry for a known object, including domains, hosts (nameservers) and contacts.
- Personalized synchronization: A registrar may contact technical support and request a data file containing all domains (and associated host (nameserver) and contact information) registered by that registrar, within a specified time interval. The data will be formatted as a comma separated values (CSV) file and made available for download using a secure server.

#### EPP modifications

There are no unique EPP modifications planned for this TLD.

All ICANN TLDs must offer a Sunrise as part of a rights protection program. Afilias uses EPP extensions that allow registrars to submit trademark and other intellectual property rights (IPR) data to the registry. These extensions are:

- An `&lt;ipr:name&gt;` element that indicates the name of Registered Mark.
- An `&lt;ipr:number&gt;` element that indicates the registration number of the IPR.
- An `&lt;ipr:ccLocality&gt;` element that indicates the origin for which the IPR is established (a national or international trademark registry).
- An `&lt;ipr:entitlement&gt;` element that indicates whether the applicant holds the trademark as the original "OWNER", "CO-OWNER" or "ASSIGNEE".
- An `&lt;ipr:appDate&gt;` element that indicates the date the Registered Mark was applied for.
- An `&lt;ipr:regDate&gt;` element that indicates the date the Registered Mark was issued and registered.
- An `&lt;ipr:class&gt;` element that indicates the class of the registered mark.
- An `&lt;ipr:type&gt;` element that indicates the Sunrise phase the application applies for.

Note that some of these extensions might be subject to change based on ICANN-developed requirements for the Trademark Clearinghouse.

#### EPP resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

108 Afilias team members directly contribute to the management and development

of the EPP based registry systems. As previously noted, Afiliias is an active member of IETF and has a long documented history developing and enhancing EPP. These contributors include 11 developers and 14 QA engineers focused on maintaining and enhancing EPP server side software. These engineers work directly with business staff to timely address existing needs and forecast registry/registrar needs to ensure the Afiliias EPP software is effective today and into the future. A team of eight data analysts work with the EPP software system to ensure that the data flowing through EPP is securely and reliably stored in replicated database systems. In addition to the EPP developers, QA engineers, and data analysts, other EPP contributors at Afiliias include: Technical Analysts, the Network Operations Center and Data Services team members.

## 26. Whois

Afiliias operates the WHOIS (registration data directory service) infrastructure in accordance with RFCs and global best practices, as it does for the 16 TLDs it currently supports. Designed to be robust and scalable, Afiliias' WHOIS service has exceeded all contractual requirements for over a decade. It has extended search capabilities, and methods of limiting abuse.

The WHOIS service operated by Afiliias meets and exceeds ICANN's requirements. Specifically, Afiliias will:

- Offer a WHOIS service made available on port 43 that is flexible and standards-compliant;
- Comply with all ICANN policies, and meeting or exceeding WHOIS performance requirements in Specification 10 of the new gTLD Registry Agreement;
- Enable a Searchable WHOIS with extensive search capabilities that offers ease of use while enforcing measures to mitigate access abuse, and;
- Employ a team with significant experience managing a compliant WHOIS service.

Such extensive knowledge and experience managing a WHOIS service enables Afiliias to offer a comprehensive plan for this TLD that meets the needs of constituents of the domain name industry and Internet users. The service has been tested by our QA team for RFC compliance, and has been used by registrars and many other parties for an extended period of time. Afiliias' WHOIS service currently serves almost 500 million WHOIS queries per month, with the capacity already built in to handle an order of magnitude increase in WHOIS queries, and the ability to smoothly scale should greater growth be needed.

### WHOIS system description and diagram

The Afiliias WHOIS system, depicted in figure 26-a, is designed with robustness, availability, compliance, and performance in mind. Additionally, the system has provisions for detecting abusive usage (e.g., excessive numbers of queries from one source). The WHOIS system is generally intended as a publicly available single object lookup system. Afiliias uses an advanced, persistent caching system to ensure extremely fast query response times.

Afiliias will develop restricted WHOIS functions based on specific domain policy and regulatory requirements as needed for operating the business (as long as they are standards compliant). It will also be possible for contact and registrant information to be returned according to regulatory requirements. The WHOIS database supports multiple string and field searching through a reliable, free, secure web-based interface.

#### Data objects, interfaces, access and lookups

Registrars can provide an input form on their public websites through which a visitor is able to perform WHOIS queries. The registry operator can also provide a Web-based search on its site. The input form must accept the string



to query, along with the necessary input elements to select the object type and interpretation controls. This input form sends its data to the Afilias port 43 WHOIS server. The results from the WHOIS query are returned by the server and displayed in the visitor's Web browser. The sole purpose of the Web interface is to provide a user-friendly interface for WHOIS queries.

Afilias will provide WHOIS output as per Specification 4 of the new gTLD Registry Agreement. The output for domain records generally consists of the following elements:

- The name of the domain registered and the sponsoring registrar;
- The names of the primary and secondary nameserver(s) for the registered domain name;
- The creation date, registration status and expiration date of the registration;
- The name, postal address, e-mail address, and telephone and fax numbers of the domain name holder;
- The name, postal address, e-mail address, and telephone and fax numbers of the technical contact for the domain name holder;
- The name, postal address, e-mail address, and telephone and fax numbers of the administrative contact for the domain name holder, and;
- The name, postal address, e-mail address, and telephone and fax numbers of the billing contact for the domain name holder.

The following additional features are also present in Afilias' WHOIS service:

- Support for IDNs, including the language tag and the Punycode representation of the IDN in addition to Unicode Hex and Unicode HTML formats;
- Enhanced support for privacy protection relative to the display of confidential information.

Afilias will also provide sophisticated WHOIS search functionality that includes the ability to conduct multiple string and field searches.

#### Query controls

For all WHOIS queries, a user is required to enter the character string representing the information for which they want to search. The object type and interpretation control parameters to limit the search may also be specified. If object type or interpretation control parameter is not specified, WHOIS will search for the character string in the Name field of the Domain object.

WHOIS queries are required to be either an "exact search" or a "partial search," both of which are insensitive to the case of the input string.

An exact search specifies the full string to search for in the database field. An exact match between the input string and the field value is required.

A partial search specifies the start of the string to search for in the database field. Every record with a search field that starts with the input string is considered a match. By default, if multiple matches are found for a query, then a summary containing up to 50 matching results is presented. A second query is required to retrieve the specific details of one of the matching records.

If only a single match is found, then full details will be provided. Full detail consists of the data in the matching object as well as the data in any associated objects. For example: a query that results in a domain object includes the data from the associated host and contact objects.

WHOIS query controls fall into two categories: those that specify the type of field, and those that modify the interpretation of the input or determine the level of output to provide. Each is described below.

The following keywords restrict a search to a specific object type:

- **Domain:** Searches only domain objects. The input string is searched in the Name field.
- **Host:** Searches only nameserver objects. The input string is searched in the

Name field and the IP Address field.

- Contact: Searches only contact objects. The input string is searched in the ID field.
- Registrar: Searches only registrar objects. The input string is searched in the Name field.

By default, if no object type control is specified, then the Name field of the Domain object is searched.

In addition, Afiliias WHOIS systems can perform and respond to WHOIS searches by registrant name, postal address and contact names. Deployment of these features is provided as an option to the registry operator, based upon registry policy and business decision-making.

Figure 26-b presents the keywords that modify the interpretation of the input or determine the level of output to provide.

By default, if no interpretation control keywords are used, the output will include full details if a single match is found and a summary if multiple matches are found.

#### Unique TLD requirements

There are no unique WHOIS requirements for this TLD.

#### Sunrise WHOIS processes

All ICANN TLDs must offer a Sunrise as part of a rights protection program. Afiliias uses EPP extensions that allow registrars to submit trademark and other intellectual property rights (IPR) data to the registry. The following corresponding data will be displayed in WHOIS for relevant domains:

- Trademark Name: element that indicates the name of the Registered Mark.
- Trademark Number: element that indicates the registration number of the IPR.
- Trademark Locality: element that indicates the origin for which the IPR is established (a national or international trademark registry).
- Trademark Entitlement: element that indicates whether the applicant holds the trademark as the original "OWNER", "CO-OWNER" or "ASSIGNEE".
- Trademark Application Date: element that indicates the date the Registered Mark was applied for.
- Trademark Registration Date: element that indicates the date the Registered Mark was issued and registered.
- Trademark Class: element that indicates the class of the Registered Mark.
- IPR Type: element that indicates the Sunrise phase the application applies for.

#### IT and infrastructure resources

All the applications and databases for this TLD will run in a virtual environment hosted by a cluster of servers equipped with the latest Intel Westmere multi-core processors (or a more advanced, stable technology available at the time of deployment). The registry data will be stored on storage arrays of solid-state drives shared over a fast storage area network. The virtual environment allows the infrastructure to easily scale both vertically and horizontally to cater to changing demand. It also facilitates effective utilization of system resources thus reducing energy consumption and carbon footprint.

The applications and servers are supported by network firewalls, routers and switches. The WHOIS system accommodates both IPv4 and IPv6 addresses.

Each of the servers and network devices are equipped with redundant hot-swappable components and multiple connections to ancillary systems. Additionally, 24x7 support agreements with our hardware vendor with a 4-hour response time at all our data centers guarantees replacement of failed parts in the shortest time possible.

Models of system and network devices used are:

- Servers: Cisco UCS B230 blade servers
- SAN storage arrays: IBM Storwize V7000 with Solid State Drives
- Firewalls: Cisco ASA 5585-X
- Load balancers: F5 Big-IP 6900
- Traffic shapers: Procera PacketLogic PL8720
- Routers: Juniper MX40 3D
- Network switches: Cisco Nexus 7010, Nexus 5548, Nexus 2232

There will be at least four virtual machines (VMs) offering WHOIS service. Each VM will run at least two WHOIS server instances - one for registrars and one for the public. All instances of the WHOIS service is made available to registrars and the public are rate limited to mitigate abusive behavior.

Frequency of synchronization between servers

Registration data records from the EPP publisher database will be replicated to the WHOIS system database on a near-real-time basis whenever an update occurs.

Specifications 4 and 10 compliance

The WHOIS service for this TLD will meet or exceed the performance requirements in the new gTLD Registry Agreement, Specification 10. Figure 26-c provides the exact measurements and commitments. Afilias has a 10 year track record of exceeding WHOIS performance and a skilled team to ensure this continues for all TLDs under management.

The WHOIS service for this TLD will meet or exceed the requirements in the new gTLD Registry Agreement, Specification 4.

RFC 3912 compliance

Afilias will operate the WHOIS infrastructure in compliance with RFCs and global best practices, as it does with the 16 TLDs Afilias currently supports.

Afilias maintains a registry-level centralized WHOIS database that contains information for every registered domain and for all host and contact objects. The WHOIS service will be available on the Internet standard WHOIS port (port 43) in compliance with RFC 3912. The WHOIS service contains data submitted by registrars during the registration process. Changes made to the data by a registrant are submitted to Afilias by the registrar and are reflected in the WHOIS database and service in near-real-time, by the instance running at the primary data center, and in under ten seconds by the instance running at the secondary data center, thus providing all interested parties with up-to-date information for every domain. This service is compliant with the new gTLD Registry Agreement, Specification 4.

The WHOIS service maintained by Afilias will be authoritative and complete, as this will be a "thick" registry (detailed domain contact WHOIS is all held at the registry); users do not have to query different registrars for WHOIS information, as there is one central WHOIS system. Additionally, visibility of different types of data is configurable to meet the registry operator's needs.

Searchable WHOIS

Afilias offers a searchable WHOIS on a web-based Directory Service. Partial match capabilities are offered on the following fields: domain name, registrar ID, and IP address. In addition, Afilias WHOIS systems can perform and respond to WHOIS searches by registrant name, postal address and contact names.

Providing the ability to search important and high-value fields such as registrant name, address and contact names increases the probability of abusive behavior. An abusive user could script a set of queries to the WHOIS service and access contact data in order to create or sell a list of names and addresses of registrants in this TLD. Making the WHOIS machine readable, while preventing harvesting and mining of WHOIS data, is a key requirement integrated into the Afiliias WHOIS systems. For instance, Afiliias limits search returns to 50 records at a time. If bulk queries were ever necessary (e.g., to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process), Afiliias makes such query responses available to carefully screened and limited staff members at the registry operator (and customer support staff) via an internal data warehouse. The Afiliias WHOIS system accommodates anonymous access as well as pre-identified and profile-defined uses, with full audit and log capabilities.

The WHOIS service has the ability to tag query responses with labels such as "Do not redistribute" or "Special access granted". This may allow for tiered response and reply scenarios. Further, the WHOIS service is configurable in parameters and fields returned, which allow for flexibility in compliance with various jurisdictions, regulations or laws.

Afiliias offers exact-match capabilities on the following fields: registrar ID, nameserver name, and nameserver's IP address (only applies to IP addresses stored by the registry, i.e., glue records). Search capabilities are fully available, and results include domain names matching the search criteria (including IDN variants). Afiliias manages abuse prevention through rate limiting and CAPTCHA (described below). Queries do not require specialized transformations of internationalized domain names or internationalized data fields

Please see "Query Controls" above for details about search options and capabilities.

#### Deterring WHOIS abuse

Afiliias has adopted two best practices to prevent abuse of the WHOIS service: rate limiting and CAPTCHA.

Abuse of WHOIS services on port 43 and via the Web is subject to an automated rate-limiting system. This ensures that uniformity of service to users is unaffected by a few parties whose activities abuse or otherwise might threaten to overload the WHOIS system.

Abuse of web-based public WHOIS services is subject to the use of CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) technology. The use of CAPTCHA ensures that uniformity of service to users is unaffected by a few parties whose activities abuse or otherwise might threaten to overload the WHOIS system. Afiliias will adopt a CAPTCHA on its Web-based WHOIS.

Data mining of any sort on the WHOIS system is strictly prohibited, and this prohibition is published in WHOIS output and in terms of service.

For rate limiting on IPv4, there are configurable limits per IP and subnet. For IPv6, the traditional limitations do not apply. Whenever a unique IPv6 IP address exceeds the limit of WHOIS queries per minute, the same rate-limit for the given 64 bits of network prefix that the offending IPv6 IP address falls into will be applied. At the same time, a timer will start and rate-limit validation logic will identify if there are any other IPv6 address within the original 80-bit (<48) prefix. If another offending IPv6 address does fall into the <48 prefix then rate-limit validation logic will penalize any other IPv6 addresses that fall into that given 80-bit (<48) network. As a security precaution, Afiliias will not disclose these limits.

Pre-identified and profile-driven role access allows greater granularity and configurability in both access to the WHOIS service, and in volume/frequency of responses returned for queries.

Afilias staff are key participants in the ICANN Security & Stability Advisory Committee's deliberations and outputs on WHOIS, including SAC003, SAC027, SAC033, SAC037, SAC040, and SAC051. Afilias staff are active participants in both technical and policy decision making in ICANN, aimed at restricting abusive behavior.

#### WHOIS staff resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Within Afilias, there are 11 staff members who develop and maintain the compliant WHOIS systems. They keep pace with access requirements, thwart abuse, and continually develop software. Of these resources, approximately two staffers are typically required for WHOIS-related code customization. Other resources provide quality assurance, and operations personnel maintain the WHOIS system itself. This team will be responsible for the implementation and on-going maintenance of the new TLD WHOIS service.

## 27. Registration Life Cycle

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE "<" and ">" CHARACTERS), WHICH ICANN INFORMS AFILIAS (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE.

Afilias has been managing registrations for over a decade. Afilias has had experience managing registrations for over a decade and supports comprehensive registration lifecycle services including the registration states, all standard grace periods, and can address any modifications required with the introduction of any new ICANN policies.

This TLD will follow the ICANN standard domain lifecycle, as is currently implemented in TLDs such as .ORG and .INFO. The below response includes: a diagram and description of the lifecycle of a domain name in this TLD, including domain creation, transfer protocols, grace period implementation and the respective time frames for each; and the existing resources to support the complete lifecycle of a domain.

As depicted in Figure 27-a, prior to the beginning of the Trademark Claims Service or Sunrise IP protection program[s], Afilias will support the reservation of names in accordance with the new gTLD Registry Agreement, Specification 5. After the quiet period for Sunrise closes, there will be a land rush period providing applicants the opportunity to register their domain prior to general availability; this will be followed by a 30 day quiet period.

## Registration period

After the IP protection programs, the landrush and the general launch, eligible registrants may choose an accredited registrar to register a domain name. The registrar will check availability on the requested domain name and if available, will collect specific objects such as, the required contact and host information from the registrant. The registrar will then provision the information into the registry system using standard Extensible Provisioning Protocol ("EPP") commands through a secure connection to the registry backend service provider.

When the domain is created, the standard five day Add Grace Period begins, the domain and contact information are available in WHOIS, and normal operating EPP domain statuses will apply. Other specifics regarding registration rules for an active domain include:

- The domain must be unique;
- Restricted or reserved domains cannot be registered;
- The domain can be registered from 1-10 years;
- The domain can be renewed at any time for 1-10 years, but cannot exceed 10 years;
- The domain can be explicitly deleted at any time;
- The domain can be transferred from one registrar to another except during the first 60 days following a successful registration or within 60 days following a transfer; and,

Contacts and hosts can be modified at any time.

The following describe the domain status values recognized in WHOIS when using the EPP protocol following RFC 5731.

- OK or Active: This is the normal status for a domain that has no pending operations or restrictions.
- Inactive: The domain has no delegated name servers.
- Locked: No action can be taken on the domain. The domain cannot be renewed, transferred, updated, or deleted. No objects such as contacts or hosts can be associated to, or disassociated from the domain. This status includes: Delete Prohibited / Server Delete Prohibited, Update Prohibited / Server Update Prohibited, Transfer Prohibited, Server Transfer Prohibited, Renew Prohibited, Server Renew Prohibited.
- Hold: The domain will not be included in the zone. This status includes: Client Hold, Server Hold.
- Transfer Prohibited: The domain cannot be transferred away from the sponsoring registrar. This status includes: Client Transfer Prohibited, Server Transfer Prohibited.

The following describe the registration operations that apply to the domain name during the registration period.

a. Domain modifications: This operation allows for modifications or updates to the domain attributes to include:

- i. Registrant Contact
- ii. Admin Contact
- iii. Technical Contact
- iv. Billing Contact
- v. Host or nameservers
- vi. Authorization information
- vii. Associated status values

A domain with the EPP status of Client Update Prohibited or Server Update Prohibited may not be modified until the status is removed.

b. Domain renewals: This operation extends the registration period of a domain by changing the expiration date. The following rules apply:

- i. A domain can be renewed at any time during its registration term,
- ii. The registration term cannot exceed a total of 10 years.

A domain with the EPP status of Client Renew Prohibited or Server Renew Prohibited cannot be renewed.

c. Domain deletions: This operation deletes the domain from the Shared Registry Services (SRS). The following rules apply:

- i. A domain can be deleted at any time during its registration term, if the domain is deleted during the Add Grace Period or the Renew/Extend Grace Period, the sponsoring registrar will receive a credit,
- ii. A domain cannot be deleted if it has "child" nameservers that are associated to other domains.

A domain with the EPP status of Client Delete Prohibited or Server Delete Prohibited cannot be deleted.

d. Domain transfers: A transfer of the domain from one registrar to another is conducted by following the steps below.

- i. The registrant must obtain the applicable <authInfo> code from the sponsoring (losing) registrar.
  - Every domain name has an authInfo code as per EPP RFC 5731. The authInfo code is a six- to 16-character code assigned by the registrar at the time the name was created. Its purpose is to aid identification of the domain owner so proper authority can be established (it is the "password" to the domain).
  - Under the Registry-Registrar Agreement, registrars will be required to provide a copy of the authInfo code to the domain registrant upon his or her request.
- ii. The registrant must provide the authInfo code to the new (gaining) registrar, who will then initiate a domain transfer request. A transfer cannot be initiated without the authInfo code.
  - Every EPP <transfer> command must contain the authInfo code or the request will fail. The authInfo code represents authority to the registry to initiate a transfer.
- iii. Upon receipt of a valid transfer request, the registry automatically asks the sponsoring (losing) registrar to approve the request within five calendar days.
  - When a registry receives a transfer request the domain cannot be modified, renewed or deleted until the request has been processed. This status must not be combined with either Client Transfer Prohibited or Server Transfer Prohibited status.
  - If the sponsoring (losing) registrar rejects the transfer within five days, the transfer request is cancelled. A new domain transfer request will be required to reinitiate the process.
  - If the sponsoring (losing) registrar does not approve or reject the transfer within five days, the registry automatically approves the request.
- iv. After a successful transfer, it is strongly recommended that registrars change the authInfo code, so that the prior registrar or registrant cannot use it anymore.
- v. Registrars must retain all transaction identifiers and codes associated with successful domain object transfers and protect them from disclosure.
- vi. Once a domain is successfully transferred the status of TRANSFERPERIOD is added to the domain for a period of five days.
- vii. Successful transfers will result in a one year term extension (resulting in a maximum total of 10 years), which will be charged to the gaining registrar.

e. Bulk transfer: Afiliias supports bulk transfer functionality within the SRS for situations where ICANN may request the registry to perform a transfer of some or all registered objects (includes domain, contact and host objects) from one registrar to another registrar. Once a bulk transfer has been executed, expiry dates for all domain objects remain the same, and all relevant states of each object type are preserved. In some cases the gaining and the losing registrar as well as the registry must approved bulk transfers. A detailed log is captured for each bulk transfer process and is archived for audit purposes.

Afiliias will support ICANN's Transfer Dispute Resolution Process. Afiliias will

also respond to Requests for Enforcement (law enforcement or court orders) and will follow that process.

#### 1. Auto-renew grace period

The Auto-Renew Grace Period displays as AUTORENEWPERIOD in WHOIS. An auto-renew must be requested by the registrant through the sponsoring registrar and occurs if a domain name registration is not explicitly renewed or deleted by the expiration date and is set to a maximum of 45 calendar days. In this circumstance the registration will be automatically renewed by the registry system the first day after the expiration date. If a Delete, Extend, or Transfer occurs within the AUTORENEWPERIOD the following rules apply:

- i. Delete. If a domain is deleted the sponsoring registrar at the time of the deletion receives a credit for the auto-renew fee. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.
- ii. Renew/Extend. A domain can be renewed as long as the total term does not exceed 10 years. The account of the sponsoring registrar at the time of the extension will be charged for the additional number of years the registration is renewed.
- iii. Transfer (other than ICANN-approved bulk transfer). If a domain is transferred, the losing registrar is credited for the auto-renew fee, and the year added by the operation is cancelled. As a result of the transfer, the expiration date of the domain is extended by minimum of one year as long as the total term does not exceed 10 years. The gaining registrar is charged for the additional transfer year(s) even in cases where a full year is not added because of the maximum 10 year registration restriction.

#### 2. Redemption grace period

During this period, a domain name is placed in the PENDING DELETE RESTORABLE status when a registrar requests the deletion of a domain that is not within the Add Grace Period. A domain can remain in this state for up to 30 days and will not be included in the zone file. The only action a registrar can take on a domain is to request that it be restored. Any other registrar requests to modify or otherwise update the domain will be rejected. If the domain is restored it moves into PENDING RESTORE and then OK. After 30 days if the domain is not restored it moves into PENDING DELETE SCHEDULED FOR RELEASE before the domain is released back into the pool of available domains.

#### 3. Pending delete

During this period, a domain name is placed in PENDING DELETE SCHEDULED FOR RELEASE status for five days, and all Internet services associated with the domain will remain disabled and domain cannot be restored. After five days the domain is released back into the pool of available domains.

#### Other grace periods

All ICANN required grace periods will be implemented in the registry backend service provider's system including the Add Grace Period (AGP), Renew/Extend Grace Period (EGP), Transfer Grace Period (TGP), Auto-Renew Grace Period (ARGP), and Redemption Grace Period (RGP). The lengths of grace periods are configurable in the registry system. At this time, the grace periods will be implemented following other gTLDs such as .ORG. More than one of these grace periods may be in effect at any one time. The following are accompanying grace periods to the registration lifecycle.

##### Add grace period

The Add Grace Period displays as ADDPERIOD in WHOIS and is set to five calendar days following the initial registration of a domain. If the domain is deleted by the registrar during this period, the registry provides a credit to the registrar for the cost of the registration. If a Delete, Renew/Extend, or Transfer operation occurs within the five calendar days, the following rules apply.

- i. Delete. If a domain is deleted within this period the sponsoring registrar at the time of the deletion is credited for the amount of the registration. The



domain is deleted from the registry backend service provider's database and is released back into the pool of available domains.

ii. Renew/Extend. If the domain is renewed within this period and then deleted, the sponsoring registrar will receive a credit for both the registration and the extended amounts. The account of the sponsoring registrar at the time of the renewal will be charged for the initial registration plus the number of years the registration is extended. The expiration date of the domain registration is extended by that number of years as long as the total term does not exceed 10 years.

iii. Transfer (other than ICANN-approved bulk transfer). Transfers under Part A of the ICANN Policy on Transfer of Registrations between registrars may not occur during the ADDPERIOD or at any other time within the first 60 days after the initial registration. Enforcement is the responsibility of the registrar sponsoring the domain name registration and is enforced by the SRS.

#### Renew / extend grace period

The Renew / Extend Grace Period displays as RENEWPERIOD in WHOIS and is set to five calendar days following an explicit renewal on the domain by the registrar. If a Delete, Extend, or Transfer occurs within the five calendar days, the following rules apply:

i. Delete. If a domain is deleted within this period the sponsoring registrar at the time of the deletion receives a credit for the renewal fee. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.

ii. Renew/Extend. A domain registration can be renewed within this period as long as the total term does not exceed 10 years. The account of the sponsoring registrar at the time of the extension will be charged for the additional number of years the registration is renewed.

iii. Transfer (other than ICANN-approved bulk transfer). If a domain is transferred within the Renew/Extend Grace Period, there is no credit to the losing registrar for the renewal fee. As a result of the transfer, the expiration date of the domain registration is extended by a minimum of one year as long as the total term for the domain does not exceed 10 years.

If a domain is auto-renewed, then extended, and then deleted within the Renew/Extend Grace Period, the registrar will be credited for any auto-renew fee charged and the number of years for the extension. The years that were added to the domain's expiration as a result of the auto-renewal and extension are removed. The deleted domain is moved to the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.

#### Transfer Grace Period

The Transfer Grace period displays as TRANSFERPERIOD in WHOIS and is set to five calendar days after the successful transfer of domain name registration from one registrar to another registrar. Transfers under Part A of the ICANN Policy on Transfer of Registrations between registrars may not occur during the TRANSFERPERIOD or within the first 60 days after the transfer. If a Delete or Renew/Extend occurs within that five calendar days, the following rules apply:

i. Delete. If the domain is deleted by the new sponsoring registrar during this period, the registry provides a credit to the registrar for the cost of the transfer. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.

ii. Renew/Extend. If a domain registration is renewed within the Transfer Grace Period, there is no credit for the transfer. The registrar's account will be charged for the number of years the registration is renewed. The expiration date of the domain registration is extended by the renewal years as long as the total term does not exceed 10 years.

#### Registration lifecycle resources

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade,

are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way. Virtually all Afilias resource are involved in the registration lifecycle of domains.

There are a few areas where registry staff devote resources to registration lifecycle issues:

- a. Supporting Registrar Transfer Disputes. The registry operator will have a compliance staffer handle these disputes as they arise; they are very rare in the existing gTLDs.
- b. Afilias has its development and quality assurance departments on hand to modify the grace period functionality as needed, if ICANN issues new Consensus Policies or the RFCs change.

Afilias has more than 30 staff members in these departments.

## 28. Abuse Prevention and Mitigation

Afilias will take the requisite operational and technical steps to promote WHOIS data accuracy, limit domain abuse, remove outdated and inaccurate data, and other security measures to ensure the integrity of the TLD. The specific measures include, but are not limited to:

- Posting a TLD Anti-Abuse Policy that clearly defines abuse, and provide point-of-contact information for reporting suspected abuse;
- Committing to rapid identification and resolution of abuse, including suspensions;
- Ensuring completeness of WHOIS information at the time of registration;
- Publishing and maintaining procedures for removing orphan glue records for names removed from the zone, and;
- Establishing measures to deter WHOIS abuse, including rate-limiting, determining data syntax validity, and implementing and enforcing requirements from the Registry-Registrar Agreement.

### Abuse policy

The Anti-Abuse Policy stated below will be enacted under the contractual authority of the registry operator through the Registry-Registrar Agreement, and the obligations will be passed on to and made binding upon registrants. This policy will be posted on the TLD web site along with contact information for registrants or users to report suspected abuse.

The policy is designed to address the malicious use of domain names. The registry operator and its registrars will make reasonable attempts to limit significant harm to Internet users. This policy is not intended to take the place of the Uniform Domain Name Dispute Resolution Policy (UDRP) or the Uniform Rapid Suspension System (URS), and it is not to be used as an alternate form of dispute resolution or as a brand protection mechanism. Its intent is not to burden law-abiding or innocent registrants and domain users; rather, the intent is to deter those who use domain names maliciously by engaging in illegal or fraudulent activity.

Repeat violations of the abuse policy will result in a case-by-case review of the abuser(s), and the registry operator reserves the right to escalate the issue, with the intent of levying sanctions that are allowed under the TLD anti-abuse policy.

The below policy is a recent version of the policy that has been used by

the .INFO registry since 2008, and the .ORG registry since 2009. It has proven to be an effective and flexible tool.

#### .WEB Anti-Abuse Policy

The following Anti-Abuse Policy is effective upon launch of the TLD. Malicious use of domain names will not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars, and registrants, as well as for users of the Internet in general. The registry operator definition of abusive use of a domain includes, without limitation, the following:

- Illegal or fraudulent actions;
- Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of web sites and Internet forums;
- Phishing: The use of counterfeit web pages that are designed to trick recipients into divulging sensitive data such as personally identifying information, usernames, passwords, or financial data;
- Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or poisoning;
- Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and Trojan horses.
- Malicious fast-flux hosting: Use of fast-flux techniques with a botnet to disguise the location of web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities.
- Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct distributed denial-of-service attacks (DDoS attacks);
- Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Pursuant to the Registry-Registrar Agreement, registry operator reserves the right at its sole discretion to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary: (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of registry operator, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement and this Anti-Abuse Policy, or (5) to correct mistakes made by registry operator or any registrar in connection with a domain name registration. Registry operator also reserves the right to place upon registry lock, hold, or similar status a domain name during resolution of a dispute.

The policy stated above will be accompanied by notes about how to submit a report to the registry operator's abuse point of contact, and how to report an orphan glue record suspected of being used in connection with malicious conduct (see below).

#### Abuse point of contact and procedures for handling abuse complaints

The registry operator will establish an abuse point of contact. This contact will be a role-based e-mail address of the form "abuse@registry.WEB". This e-mail address will allow multiple staff members to monitor abuse reports on a 24x7 basis, and then work toward closure of cases as each situation calls for. For tracking purposes, the registry operator will have a ticketing system with which all complaints will be tracked internally. The reporter will be provided

with the ticket reference identifier for potential follow-up. Afilias will integrate its existing ticketing system to ensure uniform tracking and handling of the complaint. This role-based approach has been used successfully by ISPs, e-mail service providers, and registrars for many years, and is considered a global best practice.

The registry operator's designated abuse handlers will then evaluate complaints received via the abuse system address. They will decide whether a particular issue is of concern, and decide what action, if any, is appropriate.

In general, the registry operator will find itself receiving abuse reports from a wide variety of parties, including security researchers and Internet security companies, financial institutions such as banks, Internet users, and law enforcement agencies among others. Some of these parties may provide good forensic data or supporting evidence of the malicious behavior. In other cases, the party reporting an issue may not be familiar with how to provide such data or proof of malicious behavior. It is expected that a percentage of abuse reports to the registry operator will not be actionable, because there will not be enough evidence to support the complaint (even after investigation), and because some reports or reporters will simply not be credible.

The security function includes a communication and outreach function, with information sharing with industry partners regarding malicious or abusive behavior, in order to ensure coordinated abuse mitigation across multiple TLDs.

Assessing abuse reports requires great care, and the registry operator will rely upon professional, trained investigators who are versed in such matters. The goals are accuracy, good record-keeping, and a zero false-positive rate so as not to harm innocent registrants.

Different types of malicious activities require different methods of investigation and documentation. Further, the registry operator expects to face unexpected or complex situations that call for professional advice, and will rely upon professional, trained investigators as needed.

In general, there are two types of domain abuse that must be addressed:

- a) Compromised domains. These domains have been hacked or otherwise compromised by criminals, and the registrant is not responsible for the malicious activity taking place on the domain. For example, the majority of domain names that host phishing sites are compromised. The goal in such cases is to get word to the registrant (usually via the registrar) that there is a problem that needs attention with the expectation that the registrant will address the problem in a timely manner. Ideally such domains do not get suspended, since suspension would disrupt legitimate activity on the domain.
- b) Malicious registrations. These domains are registered by malefactors for the purpose of abuse. Such domains are generally targets for suspension, since they have no legitimate use.

The standard procedure is that the registry operator will forward a credible alleged case of malicious domain name use to the domain's sponsoring registrar with a request that the registrar investigate the case and act appropriately. The registrar will be provided evidence collected as a result of the investigation conducted by the trained abuse handlers. As part of the investigation, if inaccurate or false WHOIS registrant information is detected, the registrar is notified about this. The registrar is the party with a direct relationship with—and a direct contract with—the registrant. The registrar will also have vital information that the registry operator will not, such as:

- Details about the domain purchase, such as the payment method used (credit card, PayPal, etc.);
- The identity of a proxy-protected registrant;
- The purchaser's IP address;
- Whether there is a reseller involved, and;
- The registrant's past sales history and purchases in other TLDs (insofar as the registrar can determine this).

Registrars do not share the above information with registry operators due to privacy and liability concerns, among others. Because they have more information with which to continue the investigation, and because they have a direct relationship with the registrant, the registrar is in the best position to evaluate alleged abuse. The registrar can determine if the use violates the registrar's legal terms of service or the registry Anti-Abuse Policy, and can decide whether or not to take any action. While the language and terms vary, registrars will be expected to include language in their registrar-registrant contracts that indemnifies the registrar if it takes action, and allows the registrar to suspend or cancel a domain name; this will be in addition to the registry Anti-Abuse Policy. Generally, registrars can act if the registrant violates the registrar's terms of service, or violates ICANN policy, or if illegal activity is involved, or if the use violates the registry's Anti-Abuse Policy.

If a registrar does not take action within a time period indicated by the registry operator (usually 24 hours), the registry operator might then decide to take action itself. At all times, the registry operator reserves the right to act directly and immediately if the potential harm to Internet users seems significant or imminent, with or without notice to the sponsoring registrar.

The registry operator will be prepared to call upon relevant law enforcement bodies as needed. There are certain cases, for example, Illegal pharmacy domains, where the registry operator will contact the Law Enforcement Agencies to share information about these domains, provide all the evidence collected and work closely with them before any action will be taken for suspension. The specific action is often dependent upon the jurisdiction of which the registry operator, although the operator in all cases will adhere to applicable laws and regulations.

When valid court orders or seizure warrants are received from courts or law enforcement agencies of relevant jurisdiction, the registry operator will order execution in an expedited fashion. Compliance with these will be a top priority and will be completed as soon as possible and within the defined timelines of the order. There are certain cases where Law Enforcement Agencies request information about a domain including but not limited to:

- Registration information
- History of a domain, including recent updates made
- Other domains associated with a registrant's account
- Patterns of registrant portfolio

Requests for such information is handled on a priority basis and sent back to the requestor as soon as possible. Afilias sets a goal to respond to such requests within 24 hours.

The registry operator may also engage in proactive screening of its zone for malicious use of the domains in the TLD, and report problems to the sponsoring registrars. The registry operator could take advantage of a combination of the following resources, among others:

- Blocklists of domain names and nameservers published by organizations such as SURBL and Spamhaus.
- Anti-phishing feeds, which will provide URLs of compromised and maliciously registered domains being used for phishing.
- Analysis of registration or DNS query data [DNS query data received by the TLD nameservers.]

The registry operator will keep records and track metrics regarding abuse and abuse reports. These will include:

- Number of abuse reports received by the registry's abuse point of contact described above;
- Number of cases and domains referred to registrars for resolution;
- Number of cases and domains where the registry took direct action;
- Resolution times;

- Number of domains in the TLD that have been blacklisted by major anti-spam blacklist providers, and;
- Phishing site uptimes in the TLD.

#### Removal of orphan glue records

By definition, orphan glue records used to be glue records. Glue records are related to delegations and are necessary to guide iterative resolvers to delegated nameservers. A glue record becomes an orphan when its parent nameserver record is removed without also removing the corresponding glue record. (Please reference the ICANN SSAC paper SAC048 at: <http://www.icann.org/en/committees/security/sac048.pdf>.) Orphan glue records may be created when a domain (example.tld) is placed on EPP ServerHold or ClientHold status. When placed on Hold, the domain is removed from the zone and will stop resolving. However, any child nameservers (now orphan glue) of that domain (e.g., ns1.example.tld) are left in the zone. It is important to keep these orphan glue records in the zone so that any innocent sites using that nameserver will continue to resolve. This use of Hold status is an essential tool for suspending malicious domains.

Afilias observes the following procedures, which are being followed by other registries and are generally accepted as DNS best practices. These procedures are also in keeping with ICANN SSAC recommendations.

When a request to delete a domain is received from a registrar, the registry first checks for the existence of glue records. If glue records exist, the registry will check to see if other domains in the registry are using the glue records. If other domains in the registry are using the glue records then the request to delete the domain will fail until no other domains are using the glue records. If no other domains in the registry are using the glue records then the glue records will be removed before the request to delete the domain is satisfied. If no glue records exist then the request to delete the domain will be satisfied.

If a registrar cannot delete a domain because of the existence of glue records that are being used by other domains, then the registrar may refer to the zone file or the "weekly domain hosted by nameserver report" to find out which domains are using the nameserver in question and attempt to contact the corresponding registrar to request that they stop using the nameserver in the glue record. The registry operator does not plan on performing mass updates of the associated DNS records.

The registry operator will accept, evaluate, and respond appropriately to complaints that orphan glue is being used maliciously. Such reports should be made in writing to the registry operator, and may be submitted to the registry's abuse point-of-contact. If it is confirmed that an orphan glue record is being used in connection with malicious conduct, the registry operator will have the orphan glue record removed from the zone file. Afilias has the technical ability to execute such requests as needed.

#### Methods to promote WHOIS accuracy

The creation and maintenance of accurate WHOIS records is an important part of registry management. As described in our response to question #26, WHOIS, the registry operator will manage a secure, robust and searchable WHOIS service for this TLD.

##### WHOIS data accuracy

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

the required fields for WHOIS data (as per the defined policies for the TLD) are enforced at the registry level. This ensures that the registrars are providing required domain registration data. Fields defined by the registry policy to be mandatory are documented as such and must be submitted by registrars. The Afiliias registry system verifies formats for relevant individual data fields (e.g. e-mail, and phone/fax numbers). Only valid country codes are allowed as defined by the ISO 3166 code list. The Afiliias WHOIS system is extensible, and is capable of using the VAULT system, described further below.

Similar to the centralized abuse point of contact described above, the registry operator can institute a contact email address which could be utilized by third parties to submit complaints for inaccurate or false WHOIS data detected. This information will be processed by Afiliias' support department and forwarded to the registrars. The registrars can work with the registrants of those domains to address these complaints. Afiliias will audit registrars on a yearly basis to verify whether the complaints being forwarded are being addressed or not. This functionality, available to all registry operators, is activated based on the registry operator's business policy.

Afiliias also incorporates a spot-check verification system where a randomly selected set of domain names are checked periodically for accuracy of WHOIS data. Afiliias' .PRO registry system incorporates such a verification system whereby 1% of total registrations or 100 domains, whichever number is larger, are spot-checked every month to verify the domain name registrant's critical information provided with the domain registration data. With both a highly qualified corps of engineers and a 24x7 staffed support function, Afiliias has the capacity to integrate such spot-check functionality into this TLD, based on the registry operator's business policy. Note: This functionality will not work for proxy protected WHOIS information, where registrars or their resellers have the actual registrant data. The solution to that problem lies with either registry or registrar policy, or a change in the general marketplace practices with respect to proxy registrations.

Finally, Afiliias' registry systems have a sophisticated set of billing and pricing functionality which aids registry operators who decide to provide a set of financial incentives to registrars for maintaining or improving WHOIS accuracy. For instance, it is conceivable that the registry operator may decide to provide a discount for the domain registration or renewal fees for validated registrants, or levy a larger cost for the domain registration or renewal of proxy domain names. The Afiliias system has the capability to support such incentives on a configurable basis, towards the goal of promoting better WHOIS accuracy.

#### Role of registrars

As part of the RRA (Registry Registrar Agreement), the registry operator will require the registrar to be responsible for ensuring the input of accurate WHOIS data by their registrants. The Registrar/Registered Name Holder Agreement will include a specific clause to ensure accuracy of WHOIS data, and to give the registrar rights to cancel or suspend registrations if the Registered Name Holder fails to respond to the registrar's query regarding accuracy of data. ICANN's WHOIS Data Problem Reporting System (WDPRS) will be available to those who wish to file WHOIS inaccuracy reports, as per ICANN policy (<http://wdprs.internic.net/>).

#### Controls to ensure proper access to domain functions

Several measures are in place in the Afiliias registry system to ensure proper access to domain functions, including authentication provisions in the RRA relative to notification and contact updates via use of AUTH-INFO codes.

IP address access control lists, TLS/SSL certificates and proper authentication are used to control access to the registry system. Registrars are only given

access to perform operations on the objects they sponsor.

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

Information about other registry security measures such as encryption and security of registrar channels are confidential to ensure the security of the registry system. The details can be found in the response to question #30b.

#### Validation and abuse mitigation mechanisms

Afilias has developed advanced validation and abuse mitigation mechanisms. These capabilities and mechanisms are described below. These services and capabilities are discretionary and may be utilized by the registry operator based on their policy and business need.

Afilias has the ability to analyze the registration data for known patterns at the time of registration. A database of these known patterns is developed from domains and other associated objects (e.g., contact information) which have been previously detected and suspended after being flagged as abusive. Any domains matching the defined criteria can be flagged for investigation. Once analyzed and confirmed by the domain anti-abuse team members, these domains may be suspended. This provides proactive detection of abusive domains.

Provisions are available to enable the registry operator to only allow registrations by pre-authorized and verified contacts. These verified contacts are given a unique code that can be used for registration of new domains.

#### Registrant pre-verification and authentication

One of the systems that could be used for validity and identity authentication is VAULT (Validation and Authentication Universal Lookup). It utilizes information obtained from a series of trusted data sources with access to billions of records containing data about individuals for the purpose of providing independent age and id verification as well as the ability to incorporate additional public or private data sources as required. At present it has the following: US Residential Coverage - 90% of Adult Population and also International Coverage - Varies from Country to Country with a minimum of 80% coverage (24 countries, mostly European).

Various verification elements can be used. Examples might include applicant data such as name, address, phone, etc. Multiple methods could be used for verification include integrated solutions utilizing API (XML Application Programming Interface) or sending batches of requests.

- Verification and Authentication requirements would be based on TLD operator requirements or specific criteria.
- Based on required WHOIS Data; registrant contact details (name, address, phone)
- If address/ZIP can be validated by VAULT, the validation process can continue (North America +25 International countries)
- If in-line processing and registration and EPP/API call would go to the verification clearinghouse and return up to 4 challenge questions.



- If two-step registration is required, then registrants would get a link to complete the verification at a separate time. The link could be specific to a domain registration and pre-populated with data about the registrant.
- If WHOIS data is validated a token would be generated and could be given back to the registrar which registered the domain.
- WHOIS data would reflect the Validated Data or some subset, i.e., fields displayed could be first initial and last name, country of registrant and date validated. Other fields could be generic validation fields much like a "privacy service".
- A "Validation Icon" customized script would be sent to the registrants email address. This could be displayed on the website and would be dynamically generated to avoid unauthorized use of the Icon. When clicked on the Icon would should limited WHOIS details i.e. Registrant: jdoe, Country: USA, Date Validated: March 29, 2011, as well as legal disclaimers.
- Validation would be annually renewed, and validation date displayed in the WHOIS.

#### Abuse prevention resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way. Abuse prevention and detection is a function that is staffed across the various groups inside Afilias, and requires a team effort when abuse is either well hidden or widespread, or both. While all of Afilias' 200+ employees are charged with responsibility to report any detected abuse, the engineering and analysis teams, numbering over 30, provide specific support based on the type of abuse and volume and frequency of analysis required. The Afilias security and support teams have the authority to initiate mitigation.

Afilias has developed advanced validation and abuse mitigation mechanisms. These capabilities and mechanisms are described below. These services and capabilities are discretionary and may be utilized by the registry operator based on their policy and business need.

This TLD's anticipated volume of registrations in the first three years of operations is listed in response #46. Afilias' anti-abuse function anticipates the expected volume and type of registrations, and together will adequately cover the staffing needs for this TLD. The registry operator will maintain an abuse response team, which may be a combination of internal staff and outside specialty contractors, adjusting to the needs of the size and type of TLD. The team structure planned for this TLD is based on several years of experience responding to, mitigating, and managing abuse for TLDs of various sizes. The team will generally consist of abuse handlers (probably internal), a junior analyst, (either internal or external), and a senior security consultant (likely an external resource providing the registry operator with extra expertise as needed). These responders will be specially trained in the investigation of abuse complaints, and will have the latitude to act expeditiously to suspend domain names (or apply other remedies) when called for.

The exact resources required to maintain an abuse response team must change with the size and registration procedures of the TLD. An initial abuse handler is necessary as a point of contact for reports, even if a part-time responsibility. The abuse handlers monitor the abuse email address for complaints and evaluate incoming reports from a variety of sources. A large

percentage of abuse reports to the registry operator may be unsolicited commercial email. The designated abuse handlers can identify legitimate reports and then decide what action is appropriate, either to act upon them, escalate to a security analyst for closer investigation, or refer them to registrars as per the above-described procedures. A TLD with rare cases of abuse would conform to this structure.

If multiple cases of abuse within the same week occur regularly, the registry operator will consider staffing internally an additional security analyst to investigate the complaints as they become more frequent. Training an abuse analyst requires 3-6 months and likely requires the active guidance of an experienced senior security analyst for guidance and verification of assessments and recommendations being made.

If this TLD were to regularly experience multiple cases of abuse within the same day, a full-time senior security analyst would likely be necessary. A senior security analyst capable of fulfilling this role should have several years of experience and able to manage and train the internal abuse response team.

The abuse response team will also maintain subscriptions for several security information services, including the blocklists from organizations like SURBL and Spamhaus and anti-phishing and other domain related abuse (malware, fast-flux etc.) feeds. The pricing structure of these services may depend on the size of the domain and some services will include a number of rapid suspension requests for use as needed.

For a large TLD, regular audits of the registry data are required to maintain control over abusive registrations. When a registrar with a significant number of registrations has been compromised or acted maliciously, the registry operator may need to analyze a set of registration or DNS query data. A scan of all the domains of a registrar is conducted only as needed. Scanning and analysis for a large registrar may require as much as a week of full-time effort for a dedicated machine and team.

## 29. Rights Protection Mechanisms

Rights protection is a core responsibility of the TLD operator, and is supported by a fully-developed plan for rights protection that includes:

- Establishing mechanisms to prevent unqualified registrations (e.g., registrations made in violation of the registry's eligibility restrictions or policies);
- Implementing a robust Sunrise program, utilizing the Trademark Clearinghouse, the services of one of ICANN's approved dispute resolution providers, a trademark validation agent, and drawing upon sunrise policies and rules used successfully in previous gTLD launches;
- Implementing a professional trademark claims program that utilizes the Trademark Clearinghouse, and drawing upon models of similar programs used successfully in previous TLD launches;
- Complying with the URS requirements;
- Complying with the UDRP;
- Complying with the PDDRP, and;
- Including all ICANN-mandated and independently developed rights protection mechanisms ("RPMs") in the registry-registrar agreement entered into by ICANN-accredited registrars authorized to register names in the TLD.

The response below details the rights protection mechanisms at the launch of the TLD (Sunrise and Trademark Claims Service) which comply with rights protection policies (URS, UDRP, PDDRP, and other ICANN RPMs), outlines additional provisions made for rights protection, and provides the resourcing plans.

Safeguards for rights protection at the launch of the TLD

The launch of this TLD will include the operation of a trademark claims service according to the defined ICANN processes for checking a registration request and alerting trademark holders of potential rights infringement.

The Sunrise Period will be an exclusive period of time, prior to the opening of public registration, when trademark and service mark holders will be able to reserve marks that are an identical match in the .WEB domain. Following the Sunrise Period, Afilias will open registration to qualified applicants.

The anticipated Rollout Schedule for the Sunrise Period will be approximately as follows:

- Launch of the TLD - Sunrise Period begins for trademark holders and service mark holders to submit registrations for their exact marks in the .ART domain.
- Quiet Period - The Sunrise Period will close and will be followed by a Quiet Period for testing and evaluation.
- Land rush period opens after the Quiet period
- Quiet period of 30 days begins after the close of Land rush
- One month after close of Quiet Period - Registration in the .ART domain will be opened to qualified applicants.

#### Sunrise Period Requirements & Restrictions

Those wishing to reserve their marks in the .WEB domain during the Sunrise Period must own a current trademark or service mark listed in the Trademark Clearinghouse.

Notice will be provided to all trademark holders in the Clearinghouse if someone is seeking a Sunrise registration. This notice will be provided to holders of marks in the Clearinghouse that are an Identical Match (as defined in the Trademark Clearing House) to the name to be registered during Sunrise.

Each Sunrise registration will require a minimum term, to be determined at a later date.

Afilias will establish the following Sunrise eligibility requirements (SERs) as minimum requirements, verified by Clearinghouse data, and incorporate a Sunrise Dispute Resolution Policy (SDRP). The SERs include: (i) ownership of a mark that satisfies the criteria set forth in section 7.2 of the Trademark Clearing House specifications, (ii) description of international class of goods or services covered by registration; (iii) representation that all provided information is true and correct; and (iv) provision of data sufficient to document rights in the trademark.

The SDRP will allow challenges based on the following four grounds: (i) at time the challenged domain name was registered, the registrants did not hold a trademark registration of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; (ii) the domain name is not identical to the mark on which the registrant based its Sunrise registration; (iii) the trademark registration on which the registrant based its Sunrise registration is not of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; or (iv) the trademark registration on which the domain name registrant based its Sunrise registration did not issue on or before the effective date of the Registry Agreement and was not applied for on or before ICANN announced the applications received.

#### Ongoing rights protection mechanisms

Several mechanisms will be in place to protect rights in this TLD. As described in our responses to questions #27 and #28, measures are in place to ensure

domain transfers and updates are only initiated by the appropriate domain holder, and an experienced team is available to respond to legal actions by law enforcement or court orders.

This TLD will conform to all ICANN RPMs including URS (defined below), UDRP, PDDRP, and all measures defined in Specification 7 of the new TLD agreement.

#### Uniform Rapid Suspension (URS)

The registry operator will implement decisions rendered under the URS on an ongoing basis. Per the URS policy posted on ICANN's Web site as of this writing, the registry operator will receive notice of URS actions from the ICANN-approved URS providers. These emails will be directed immediately to the registry operator's support staff, which is on duty 24x7. The support staff will be responsible for creating a ticket for each case, and for executing the directives from the URS provider. All support staff will receive pertinent training.

As per ICANN's URS guidelines, within 24 hours of receipt of the notice of complaint from the URS provider, the registry operator shall "lock" the domain, meaning the registry shall restrict all changes to the registration data, including transfer and deletion of the domain names, but the name will remain in the TLD DNS zone file and will thus continue to resolve. The support staff will "lock" the domain by associating the following EPP statuses with the domain and relevant contact objects:

- ServerUpdateProhibited, with an EPP reason code of "URS"
- ServerDeleteProhibited, with an EPP reason code of "URS"
- ServerTransferProhibited, with an EPP reason code of "URS"
- The registry operator's support staff will then notify the URS provider immediately upon locking the domain name, via email.

The registry operator's support staff will retain all copies of emails from the URS providers, assign them a tracking or ticket number, and will track the status of each opened URS case through to resolution via spreadsheet or database.

The registry operator's support staff will execute further operations upon notice from the URS providers. The URS provider is required to specify the remedy and required actions of the registry operator, with notification to the registrant, the complainant, and the registrar.

As per the URS guidelines, if the complainant prevails, the "registry operator shall suspend the domain name, which shall remain suspended for the balance of the registration period and would not resolve to the original web site. The nameservers shall be redirected to an informational web page provided by the URS provider about the URS. The WHOIS for the domain name shall continue to display all of the information of the original registrant except for the redirection of the nameservers. In addition, the WHOIS shall reflect that the domain name will not be able to be transferred, deleted or modified for the life of the registration."

#### Rights protection via the RRA

The following will be memorialized and be made binding via the Registry-Registrar and Registrar-Registrant Agreements:

- The registry may reject a registration request or a reservation request, or may delete, revoke, suspend, cancel, or transfer a registration or reservation under the following criteria:
  - a. to enforce registry policies and ICANN requirements; each as amended from time to time;
  - b. that is not accompanied by complete and accurate information as required by ICANN requirements and/or registry policies or where required information is not updated and/or corrected as required by ICANN requirements and/or registry policies;
  - c. to protect the integrity and stability of the registry, its operations, and

the TLD system;

d. to comply with any applicable law, regulation, holding, order, or decision issued by a court, administrative authority, or dispute resolution service provider with jurisdiction over the registry;

e. to establish, assert, or defend the legal rights of the registry or a third party or to avoid any civil or criminal liability on the part of the registry and/or its affiliates, subsidiaries, officers, directors, representatives, employees, contractors, and stockholders;

f. to correct mistakes made by the registry or any accredited registrar in connection with a registration; or

g. as otherwise provided in the Registry-Registrar Agreement and/or the Registrar-Registrant Agreement.

Reducing opportunities for behaviors such as phishing or pharming

In our response to question #28, the registry operator has described its anti-abuse program. Rather than repeating the policies and procedures here, please see our response to question #28 for full details.

In the case of this TLD, Afilias will apply an approach that addresses registered domain names (rather than potentially registered domains). This approach will not infringe upon the rights of eligible registrants to register domains, and allows Afilias internal controls, as well as community-developed UDRP and URS policies and procedures if needed, to deal with complaints, should there be any.

Afilias is a member of various security fora which provide access to lists of names in each TLD which may be used for malicious purposes. Such identified names will be subject to the TLD anti-abuse policy, including rapid suspensions after due process.

Rights protection resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Supporting RPMs requires several departments within the registry operator as well as within Afilias. The implementation of Sunrise and the Trademark Claims service and on-going RPM activities will pull from the 102 Afilias staff members of the engineering, product management, development, security and policy teams at Afilias which are on duty 24x7. A trademark validator will also be assigned within the registry operator, whose responsibilities may require as much as 50% of full-time employment if the domains under management were to exceed several million. No additional hardware or software resources are required to support this as Afilias has fully-operational capabilities to manage abuse today.

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

Afilias aggressively and actively protects the registry system from known threats and vulnerabilities, and has deployed an extensive set of security protocols, policies and procedures to thwart compromise. Afilias' robust and detailed plans are continually updated and tested to ensure new threats are mitigated prior to becoming issues. Afilias will continue these rigorous security measures, which include:

- Multiple layers of security and access controls throughout registry and support systems;
- 24x7 monitoring of all registry and DNS systems, support systems and facilities;
- Unique, proven registry design that ensures data integrity by granting only authorized access to the registry system, all while meeting performance requirements;
- Detailed incident and problem management processes for rapid review, communications, and problem resolution, and;
- Yearly external audits by independent, industry-leading firms, as well as twice-yearly internal audits.

#### Security policies and protocols

Afilias has included security in every element of its service, including facilities, hardware, equipment, connectivity, Internet services, systems, computer systems, organizational security, outage prevention, monitoring, disaster mitigation, and escrow/insurance, from the original design, through development, and finally as part of production deployment. Examples of threats and the confidential and proprietary mitigation procedures are detailed in our response to question #30(b).

There are several important aspects of the security policies and procedures to note:

- Afilias hosts domains in data centers around the world that meet or exceed global best practices.
- Afilias' DNS infrastructure is massively provisioned as part of its DDoS mitigation strategy, thus ensuring sufficient capacity and redundancy to support new gTLDs.
- Diversity is an integral part of all of our software and hardware stability and robustness plan, thus avoiding any single points of failure in our infrastructure.
- Access to any element of our service (applications, infrastructure and data) is only provided on an as-needed basis to employees and a limited set of others to fulfill their job functions. The principle of least privilege is applied.
- All registry components-critical and non-critical-are monitored 24x7 by staff at our NOCs, and the technical staff has detailed plans and procedures that have stood the test of time for addressing even the smallest anomaly. Well-documented incident management procedures are in place to quickly involve the on-call technical and management staff members to address any issues.

Afilias follows the guidelines from the ISO 27001 Information Security Standard (Reference:

[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=42103](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103) ) for the management and implementation of its Information Security Management System. Afilias also utilizes the COBIT IT governance framework to facilitate policy development and enable controls for appropriate management of risk (Reference: <http://www.isaca.org/cobit>). Best practices defined in ISO 27002 are followed for defining the security controls within the organization. Afilias continually looks to improve the efficiency and effectiveness of our processes, and follows industry best practices as defined by the IT Infrastructure Library, or ITIL (Reference: <http://www.itil-officialsite.com/>).

The Afiliias registry system is located within secure data centers that implement a multitude of security measures both to minimize any potential points of vulnerability and to limit any damage should there be a breach. The characteristics of these data centers are described fully in our response to question #30(b).

The Afiliias registry system employs a number of multi-layered measures to prevent unauthorized access to its network and internal systems. Before reaching the registry network, all traffic is required to pass through a firewall system. Packets passing to and from the Internet are inspected, and unauthorized or unexpected attempts to connect to the registry servers are both logged and denied. Management processes are in place to ensure each request is tracked and documented, and regular firewall audits are performed to ensure proper operation. 24x7 monitoring is in place and, if potential malicious activity is detected, appropriate personnel are notified immediately.

Afiliias employs a set of security procedures to ensure maximum security on each of its servers, including disabling all unnecessary services and processes and regular application of security-related patches to the operating system and critical system applications. Regular external vulnerability scans are performed to verify that only services intended to be available are accessible.

Regular detailed audits of the server configuration are performed to verify that the configurations comply with current best security practices. Passwords and other access means are changed on a regular schedule and are revoked whenever a staff member's employment is terminated.

#### Access to registry system

Access to all production systems and software is strictly limited to authorized operations staff members. Access to technical support and network operations teams where necessary are read only and limited only to components required to help troubleshoot customer issues and perform routine checks. Strict change control procedures are in place and are followed each time a change is required to the production hardware/application. User rights are kept to a minimum at all times. In the event of a staff member's employment termination, all access is removed immediately.

Afiliias applications use encrypted network communications. Access to the registry server is controlled. Afiliias allows access to an authorized registrar only if each of the authentication factors matches the specific requirements of the requested authorization. These mechanisms are also used to secure any web-based tools that allow authorized registrars to access the registry. Additionally, all write transactions in the registry (whether conducted by authorized registrars or the registry's own personnel) are logged.

EPP connections are encrypted using TLS/SSL, and mutually authenticated using both certificate checks and login/password combinations. Web connections are encrypted using TLS/SSL for an encrypted tunnel to the browser, and authenticated to the EPP server using login/password combinations.

All systems are monitored for security breaches from within the data center and without, using both system-based and network-based testing tools. Operations staff also monitor systems for security-related performance anomalies. Triple-redundant continual monitoring ensures multiple detection paths for any potential incident or problem. Details are provided in our response to questions #30(b) and #42. Network Operations and Security Operations teams perform regular audits in search of any potential vulnerability.

To ensure that registrar hosts configured erroneously or maliciously cannot deny service to other registrars, Afiliias uses traffic shaping technologies to prevent attacks from any single registrar account, IP address, or subnet. This additional layer of security reduces the likelihood of performance degradation for all registrars, even in the case of a security compromise at a subset of

registrars.

There is a clear accountability policy that defines what behaviors are acceptable and unacceptable on the part of non-staff users, staff users, and management. Periodic audits of policies and procedures are performed to ensure that any weaknesses are discovered and addressed. Aggressive escalation procedures and well-defined Incident Response management procedures ensure that decision makers are involved at early stages of any event.

In short, security is a consideration in every aspect of business at Afilias, and this is evidenced in a track record of a decade of secure, stable and reliable service.

#### Independent assessment

Supporting operational excellence as an example of security practices, Afilias performs a number of internal and external security audits each year of the existing policies, procedures and practices for:

- Access control;
- Security policies;
- Production change control;
- Backups and restores;
- Batch monitoring;
- Intrusion detection, and
- Physical security.

Afilias has an annual Type 2 SSAE 16 audit performed by PricewaterhouseCoopers (PwC). Further, PwC performs testing of the general information technology controls in support of the financial statement audit. A Type 2 report opinion under SSAE 16 covers whether the controls were properly designed, were in place, and operating effectively during the audit period (calendar year). This SSAE 16 audit includes testing of internal controls relevant to Afilias' domain registry system and processes. The report includes testing of key controls related to the following control objectives:

- Controls provide reasonable assurance that registrar account balances and changes to the registrar account balances are authorized, complete, accurate and timely.
- Controls provide reasonable assurance that billable transactions are recorded in the Shared Registry System (SRS) in a complete, accurate and timely manner.
- Controls provide reasonable assurance that revenue is systemically calculated by the Deferred Revenue System (DRS) in a complete, accurate and timely manner.
- Controls provide reasonable assurance that the summary and detail reports, invoices, statements, registrar and registry billing data files, and ICANN transactional reports provided to registry operator(s) are complete, accurate and timely.
- Controls provide reasonable assurance that new applications and changes to existing applications are authorized, tested, approved, properly implemented and documented.
- Controls provide reasonable assurance that changes to existing system software and implementation of new system software are authorized, tested, approved, properly implemented and documented.
- Controls provide reasonable assurance that physical access to data centers is restricted to properly authorized individuals.
- Controls provide reasonable assurance that logical access to system resources is restricted to properly authorized individuals.
- Controls provide reasonable assurance that processing and backups are appropriately authorized and scheduled and that deviations from scheduled processing and backups are identified and resolved.

The last Type 2 report issued was for the year 2010, and it was unqualified, i.e., all systems were evaluated with no material problems found.

During each year, Afilias monitors the key controls related to the SSAE



controls. Changes or additions to the control objectives or activities can result due to deployment of new services, software enhancements, infrastructure changes or process enhancements. These are noted and after internal review and approval, adjustments are made for the next review.

In addition to the PricewaterhouseCoopers engagement, Afilias performs internal security audits twice a year. These assessments are constantly being expanded based on risk assessments and changes in business or technology.

Additionally, Afilias engages an independent third-party security organization, PivotPoint Security, to perform external vulnerability assessments and penetration tests on the sites hosting and managing the Registry infrastructure. These assessments are performed with major infrastructure changes, release of new services or major software enhancements. These independent assessments are performed at least annually. A report from a recent assessment is attached with our response to question #30(b).

Afilias has engaged with security companies specializing in application and web security testing to ensure the security of web-based applications offered by Afilias, such as the Web Admin Tool (WAT) for registrars and registry operators.

Finally, Afilias has engaged IBM's Security services division to perform ISO 27002 gap assessment studies so as to review alignment of Afilias' procedures and policies with the ISO 27002 standard. Afilias has since made adjustments to its security procedures and policies based on the recommendations by IBM.

#### Special TLD considerations

Afilias' rigorous security practices are regularly reviewed; if there is a need to alter or augment procedures for this TLD, they will be done so in a planned and deliberate manner.

#### Commitments to registrant protection

With over a decade of experience protecting domain registration data, Afilias understands registrant security concerns. Afilias supports a "thick" registry system in which data for all objects are stored in the registry database that is the centralized authoritative source of information. As an active member of IETF (Internet Engineering Task Force), ICANN's SSAC (Security & Stability Advisory Committee), APWG (Anti-Phishing Working Group), MAAWG (Messaging Anti-Abuse Working Group), USENIX, and ISACA (Information Systems Audits and Controls Association), the Afilias team is highly attuned to the potential threats and leading tools and procedures for mitigating threats. As such, registrants should be confident that:

- Any confidential information stored within the registry will remain confidential;
- The interaction between their registrar and Afilias is secure;
- The Afilias DNS system will be reliable and accessible from any location;
- The registry system will abide by all policies, including those that address registrant data;
- Afilias will not introduce any features or implement technologies that compromise access to the registry system or that compromise registrant security.

Afilias has directly contributed to the development of the documents listed below and we have implemented them where appropriate. All of these have helped improve registrants' ability to protect their domains name(s) during the domain name lifecycle.

- [SAC049]: SSAC Report on DNS Zone Risk Assessment and Management (03 June 2011)
- [SAC044]: A Registrant's Guide to Protecting Domain Name Registration

Accounts (05 November 2010)

- [SAC040]: Measures to Protect Domain Registration Services Against Exploitation or Misuse (19 August 2009)
- [SAC028]: SSAC Advisory on Registrar Impersonation Phishing Attacks (26 May 2008)
- [SAC024]: Report on Domain Name Front Running (February 2008)
- [SAC022]: Domain Name Front Running (SAC022, SAC024) (20 October 2007)
- [SAC011]: Problems caused by the non-renewal of a domain name associated with a DNS Name Server (7 July 2006)
- [SAC010]: Renewal Considerations for Domain Name Registrants (29 June 2006)
- [SAC007]: Domain Name Hijacking Report (SAC007) (12 July 2005)

To protect any unauthorized modification of registrant data, Afilias mandates TLS/SSL transport (per RFC 5246) and authentication methodologies for access to the registry applications. Authorized registrars are required to supply a list of specific individuals (five to ten people) who are authorized to contact the registry. Each such individual is assigned a pass phrase. Any support requests made by an authorized registrar to registry customer service are authenticated by registry customer service. All failed authentications are logged and reviewed regularly for potential malicious activity. This prevents unauthorized changes or access to registrant data by individuals posing to be registrars or their authorized contacts.

These items reflect an understanding of the importance of balancing data privacy and access for registrants, both individually and as a collective, worldwide user base.

The Afilias 24/7 Customer Service Center consists of highly trained staff who collectively are proficient in 15 languages, and who are capable of responding to queries from registrants whose domain name security has been compromised—for example, a victim of domain name hijacking. Afilias provides specialized registrant assistance guides, including specific hand-holding and follow-through in these kinds of commonly occurring circumstances, which can be highly distressing to registrants

Security resourcing plans

Please refer to our response to question #30b for security resourcing plans.

© *Internet Corporation For Assigned Names and Numbers.*



# **Annex 7.**



## New gTLD Application Submitted to ICANN by: Ruby Glen, LLC

String: web

Originally Posted: 13 June 2012

Application ID: 1-1527-54849

### Applicant Information

#### 1. Full legal name

Ruby Glen, LLC

#### 2. Address of the principal place of business

Contact Information Redacted

#### 3. Phone number

Contact Information Redacted

#### 4. Fax number

Contact Information Redacted

## 5. If applicable, website or URL

### Primary Contact

#### 6(a). Name

Daniel Schindler

#### 6(b). Title

EVP, Donuts Inc.

#### 6(c). Address

#### 6(d). Phone Number

Contact Information Redacted

#### 6(e). Fax Number

#### 6(f). Email Address

Contact Information Redacted

### Secondary Contact

#### 7(a). Name

Jonathon Nevett

#### 7(b). Title

EVP, Donuts Inc.

**7(c). Address****7(d). Phone Number**

Contact Information Redacted

**7(e). Fax Number****7(f). Email Address**

Contact Information Redacted

**Proof of Legal Establishment****8(a). Legal form of the Applicant**

Limited Liability Company

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

Delaware.

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

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

Attachments are not displayed on this form.

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

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

Covered TLD, LLC

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

## Applicant Background

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

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

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

Covered TLD, LLC	N/A
------------------	-----

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

Paul Stahura	CEO, Donuts Inc.
--------------	------------------

## Applied-for gTLD string

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

web

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



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

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

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

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

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

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

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

Attachments are not displayed on this form.

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

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

**16. Describe the applicant's efforts to ensure that there are no known operational or rendering problems concerning the applied-for gTLD**

## **string. If such issues are known, describe steps that will be taken to mitigate these issues in software and other applications.**

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

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

### **## Compliance and Interoperability**

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

### **## Mixing Scripts**

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

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

### **## Interaction Between Labels**

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

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

### **## Immature Scripts**

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

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

### **## Other Issues**

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

Donuts understands that the following may be construed as operational or rendering issues, but considers them out of the scope of this question.

Nevertheless, it will take reasonable steps to protect registrants and Internet users by working with vendors and relevant language communities to mitigate such issues.

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

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

## Mission/Purpose

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

Q18A CHAR: 7985

#### ABOUT DONUTS

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

#### DONUTS' PLACE WITHIN ICANN'S MISSION

ICANN and the new TLD program share the following purposes:

1. to make sure that the Internet remains as safe, stable and secure as possible, while
2. helping to ensure there is a vibrant competitive marketplace to efficiently bring the benefits of the namespace to registrants and users alike.

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

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

#### ABOUT DONUTS' RESOURCES

Donuts' financial resources are extensive. The company has raised more than US\$100 million from a number of capital sources including multiple multi-billion dollar venture capital and private equity funds, a top-tier bank, and other well-capitalized investors. Should circumstances warrant, Donuts is

prepared to raise additional funding from current or new investors. Donuts also has in place pre-funded, Continued Operations Instruments to protect future registrants. These resource commitments mean Donuts has the capability and intent to launch, expand and operate its TLDs in a secure manner, and to properly protect Internet users and rights-holders from potential abuse.

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

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

#### THIS TLD

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

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

#### DONUTS' APPROACH TO PROTECTIONS

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

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

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

#### OUR PROTECTIONS

Donuts has consulted with and evaluated the ideas of international law enforcement, consumer privacy advocacy organizations, intellectual property interests and other Internet industry groups to create a set of protections that far exceed those in existing TLDs, and bring to the Internet namespace

nearly two dozen new rights and protection mechanisms to raise user safety and protection to a new level.

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

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

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

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

#### DONUTS' INTENTION FOR THIS TLD

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

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

Q18B CHAR: 6457

Donuts will be the industry leader in customer service, reputation and choice. The reputation of this, and other TLDs in the Donuts portfolio, will be built on:

1. Our successful launch and marketplace reach;
2. The stability of registry operations; and
3. The effectiveness of our protection mechanisms.

#### THE GOAL OF THIS TLD

This and other Donuts TLDs represent discrete segments of commerce and human interest, and will give Internet users a better vehicle for reaching audiences. In reviewing potential strings, we deeply researched discrete industries and

sectors of human activity and consulted extensive data sources relevant to the online experience. Our methodology resulted in the selection of this TLD - one that offers a very high level of user utility, precision in content delivery, and ability to contribute positively to economic growth.

#### SERVICE LEVELS

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

#### REPUTATION

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

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

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

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

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

#### NAMESPACE COMPETITION

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

#### INNOVATION

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

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

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

registrants.

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

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

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

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

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

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

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

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

Q18C Standard CHAR: 1440

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

Donuts may offer reduced pricing for registrants interested in long-term registration, and potentially to those who commit to publicizing their use of

the TLD. Other advantaged pricing may apply in selective cases, including bulk purchase pricing.

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

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

## Community-based Designation

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

No

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

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

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

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

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



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

Attachments are not displayed on this form.

## Geographic Names

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

No

## Protection of Geographic Names

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

Q22 CHAR: 4979

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

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

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

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

1. All two-character labels will be initially reserved, and released only upon agreement between Donuts and the relevant government and country code manager.
2. At the second level, country and territory names will be reserved at the second and other levels according to these standards:
  - 2.1. Short form (in English) of country and territory names documented in the ISO 3166-1 list;
  - 2.2. Names of countries and territories as documented by the United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World; and
  - 2.3. The list of United Nations member states in six official UN languages, as

prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names.

Donuts will initially reserve country and territory names at the second level and at all other levels within the TLD. Donuts supports this requirement by using the following internationally recognized lists to develop a comprehensive master list of all geographic names that are initially reserved:

1. The short form (in English) of all country and territory names contained on the ISO 3166-1 list, including the European Union, which is exceptionally reserved on the ISO 3166-1 List, and its scope extended in August 1999 to any application needing to represent the name European Union [http://www.iso.org/iso/support/country\_codes/iso\_3166\_code\_lists/iso-3166-1\_decoding\_table.htm#EU].

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

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

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

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

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

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

For purposes of clarity the following will occur for a domain that is reserved by the registry:

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

## Registry Services

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

Q23 CHAR: 22971

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

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

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

#### 1.0. EXECUTIVE SUMMARY

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

#### 2.0. REGISTRY SERVICES

##### 2.1. Receipt of Data from registrars

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

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

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

The registry is implemented as a "thick" registry meaning that domain

registrations must have contact information associated with each. Contact information will be collected by registrars and associated with domain registrations.

#### 2.1.1. SRS EPP Interface

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

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

##### 2.1.1.1. SRS EPP Interface Security Considerations

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

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

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

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

##### 2.1.1.2. SRS EPP Interface Stability Considerations

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

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

#### 2.1.2. SRS Web Interface

The SRS web interface is an alternative way to access EPP functionality using a web interface, providing the features necessary for effective operations of the registry. This interface uses the HTTPS protocol for secure web communication.

Because users can be located worldwide, as with the EPP interface, the web interface is available to all registrars over multiple network paths. Additional functionality is available to registrars to assist them in managing their account. For instance, registrars are able to view their account balance in near real time as well as the status of the registry services. In addition, notifications that are sent out in email are available for viewing.

#### 2.1.2.1. Web Interface Security Considerations

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

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

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

#### 2.1.2.2. Web Interface Stability Considerations

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

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

### 2.2. Dissemination of TLD Zone Files

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

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

Normal operations are:

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

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

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

#### 2.2.2. Communication Policy

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

A contact database containing relevant contact information for each registrar is maintained. In many cases, this includes multiple forms of contact,

including email, phone and physical mailing address. Additionally, up-to-date status information of the TLD zone servers is provided within the SRS Web Interface.

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

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

### 2.2.3. Security and Stability Considerations

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

### 2.3. Zone File Access Provider Integration

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

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

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

### 2.4. Zone File Update

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

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

### 2.5. Operation of Zone Servers

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

#### 2.5.1. Security and Operational Considerations of Zone Server Operations

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

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

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

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

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

#### 2.6. Dissemination of Domain Registration Information

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

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

##### 2.6.1. Whois Port 43 Interface

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

### 2.6.2. Whois Web Interface

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

### 2.6.3. Security and Stability Considerations

Abuse of the Whois system through data mining is a concern as it can impact system performance and reduce the quality of service to legitimate users. The Whois system mitigates this type of abuse by detecting and limiting bulk query access from single sources. It does this in two ways: 1) by rate limiting queries by non-authorized parties; and 2) by ensuring all queries result in responses that do not include data sets representing significant portions of the registration database.

In addition, the Whois web interface adds a simple challenge-response CAPCHA that requires a user to type in the characters displayed in image format. Both systems have blacklist functionality to provide a complete block to individual IPs or IP ranges.

## 2.7. Internationalized Domain Names (IDNs)

An Internationalized Domain Name (IDN) contains at least one label that is displayed in a specific language script in IDN aware software. We will offer registration of second level IDN labels at launch, IDNs are published into the TLD zone. The SRS EPP and Web Interfaces also support IDNs.

The IDN implementation is fully compliant with the IDNA 2008 suite of standards (RFC 5890, 5891, 5892 and 5893) as well as the ICANN Guidelines for the Implementation of IDN Version 3.0

(<http://www.icann.org/en/resources/idn/implementation-guidelines>). To ensure stability and security, we have adopted a conservative approach in our IDN registration policies, as well as technical implementation.

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

### 2.7.1. IDN Stability Considerations

To avoid the intentional or accidental registration of visually similar characters, and to avoid identity confusion between domains, there are several restrictions on the registration of IDNs.

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

## 2.8. DNSSEC

DNSSEC provides a set of extensions to the DNS that allow an Internet user (normally the resolver acting on a user's behalf) to validate that the DNS responses they receive were not manipulated en-route.

This type of fraud, commonly called 'man in the middle', allows a malicious party to misdirect Internet users. DNSSEC allows a domain owner to sign their



domain and to publish the signature, so that all DNS consumers who visit that domain can validate that the responses they receive are as the domain owner intended.

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

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

#### 2.8.1. Stability and Operational Considerations for DNSSEC

##### 2.8.1.1. DNSSEC Practice Statement

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

##### 2.8.1.2. Resolution Stability

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

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

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

#### 3.0. APPROACH TO SECURITY AND STABILITY

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

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

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

# Demonstration of Technical & Operational Capability

## 24. Shared Registration System (SRS) Performance

Q24 CHAR: 19964

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

### 1.0. INTRODUCTION

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

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

### 2.0. TECHNICAL OVERVIEW

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

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

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

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

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

### 3.0. ROBUST AND RELIABLE ARCHITECTURE

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

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

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

### 4.0. SOFTWARE QUALITY

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

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

### 5.0. SOFTWARE COMPLIANCE

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

We strive to be forward-thinking and will support the emerging standards of both IPv6 and DNSSEC on our SRS platform. The SRS was designed and has been tested to accept IPv6 format addresses for nameserver glue records and provision them to the gTLD zone. In addition, key registry services will be accessible over both IPv4 and IPv6. These include both the SRS EPP and SRS web-

based interfaces, both port 43 and web-based WHOIS interfaces and DNS, among others. For details regarding our IPv6 reachability plans, please refer to our response to Question 36.

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

#### 6.0. DATABASE OPERATIONS

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

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

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

#### 7.0. REDUNDANT HARDWARE

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

#### 8.0. HORIZONTALLY SCALABLE

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

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

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

#### 9.0. REDUNDANT HOT FAILOVER SITE

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

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

#### 10.0. SECURE ACCESS

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

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

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

#### 11.0. OPERATING A ROBUST AND RELIABLE SRS

##### 11.1. AUTOMATED DEPLOYMENT

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

##### 11.2. CHANGE MANAGEMENT

We use a change management system for changes and deployments to critical systems. Because the SRS is considered a critical system, it is also subject to all change management procedures. The change management system covers all software development changes, operating system and networking hardware changes and patching. Before implementation, all change orders entered into the system

must be reviewed with careful scrutiny and approved by appropriate management. New documentation and procedures are written; and customer service, operations, and monitoring staff are trained on any new functionality added that may impact their areas.

#### 11.3. PATCH MANAGEMENT

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

#### 11.4. REGULAR BACKUPS

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

#### 11.5. DATA ESCROW

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

#### 11.6. REGULAR TRAINING

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

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

#### 11.7. ACCESS CONTROL

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

#### 11.8. 24/7 MONITORING AND REGISTRAR TECHNICAL SUPPORT

We employ a full-time staff trained specifically on monitoring and supporting the services we provide. This staff is equipped with documentation outlining our processes for providing first-tier analysis, issue troubleshooting, and incident handling. This team is also equipped with specialty tools developed

specifically to safely aid in diagnostics. On-call staff second-tier support is available to assist when necessary. To optimize the service we provide, we conduct ongoing training in both basic and more advanced customer support and conduct additional training, as needed, when new system or tool features are introduced or solutions to common issues are developed.

#### 12.0. SRS INFRASTRUCTURE

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

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

#### 13.0 RESOURCING PLAN

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

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

##### Software Engineering:

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

##### Systems Engineering:

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

##### Network Engineering:

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

##### Database Operations:

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

##### Information Security Team:

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

##### Network Operations Center (NOC):

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

## 25. Extensible Provisioning Protocol (EPP)

Q25 CHAR: 20820

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

### 1.0. INTRODUCTION

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

### 2.0. IMPLEMENTATION EXPERIENCE

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

### 3.0. TRANSPORT

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

### 4.0. REGISTRARS' EXPERIENCE

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

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

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

Once a registrar has completed testing and is prepared to go live, the



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

#### 5.0. SESSIONS

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

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

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

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

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

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

#### 6.0. EPP SERVICE SCALE

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

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

which consists of Microsoft SQL Server databases for storage.

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

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

#### 7.0. COMPLIANCE WITH CORE AND EPP EXTENSION RFCs

The EPP interface is highly compliant with the following RFCs:

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

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

##### 7.1. RFC 5730 EXTENSIBLE PROVISIONING PROTOCOL

Section 2.1 Transport Mapping Considerations - ack.

Transmission Control Protocol (TCP) in compliance with RFC 5734 with TLS.

Section 2.4 Greeting Format - compliant

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

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

Section 2.7 Extension Framework - compliant

Each mapping and extension, if offered, will comply with RFC 3735 Guidelines for Extending EPP.

Section 2.9 Protocol Commands - compliant

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

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

Section 4 Formal syntax - compliant

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

Section 5 Internationalization Considerations - compliant

EPP XML recognizes both UTF-8 and UTF-16. All date-time values are presented in

Universal Coordinated Time using Gregorian calendar.

## 7.2. RFC 5731 EPP DOMAIN NAME MAPPING

### Section 2.1 Domain and Host names - compliant

The domain and host names are validated to meet conformance requirements mentioned in RFC 0952, 1123 and 3490.

### Section 2.2 Contact and Client Identifiers - compliant

All EPP contacts are identified by a server-unique identifier. Contact identifiers conform to "clIDType" syntax described in RFC 5730.

### Section 2.3 Status Values - compliant

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

### Section 2.4 Dates and Times - compliant

Date and time attribute values are represented in Universal Coordinated Time (UTC) using Gregorian calendar, in conformance with XML schema.

### Section 2.5 Validity Periods - compliant

Our SRS implementation supports validity periods in unit year ("y"). The default period is 1y.

### Section 3.1.1 EPP <check> Command - compliant

A maximum of 5 domains can be checked in a single command request as defined by server policy.

### Section 3.1.2 EPP <info> Command - compliant

EPP <info> command is used to retrieve information associated with a domain object. If the querying Registrar is not the sponsoring registrar and the registrar does not provide valid authorization information, the server does not send any domain elements in response per server policy.

### Section 3.1.3 EPP <transfer> Query Command - compliant

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

### Section 3.2.4 EPP <transfer> Command - compliant

All subordinate host objects to the domain are transferred along with the domain object.

## 7.3. RFC 5732 EPP HOST MAPPING

### Section 2.1 Host Names - compliant

The host names are validated to meet conformance requirements mentioned in RFC 0952, 1123 and 3490.

### Section 2.2 Contact and Client Identifiers - compliant

All EPP clients are identified by a server-unique identifier. Client identifiers conform to "clIDType" syntax described in RFC 5730.

### Section 2.5 IP Addresses - compliant

The syntax for IPv4 addresses conform to RFC0791. The syntax for IPv6 addresses conform to RFC4291.

### Section 3.1.1 EPP <check> Command - compliant

Maximum of five host names can be checked in a single command request set by server policy.

#### Section 3.1.2 EPP <info> Command - compliant

If the querying client is not a sponsoring client, the server does not send any host object elements in response and the request is rejected for authorization according to server policy.

#### Section 3.2.2 EPP <delete> Command - compliant

A delete is permitted only if the host is not delegated.

#### Section 3.2.2 EPP <update> Command - compliant

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

### 7.4. RFC 5733 EPP CONTACT MAPPING

#### Section 2.1 Contact and Client Identifiers - compliant

Contact identifiers conform to "clIDType" syntax described in RFC 5730.

#### Section 2.6 Email Addresses - compliant

Email address validation conforms to syntax defined in RFC5322.

#### Section 3.1.1 EPP <check> Command - compliant

Maximum of 5 contact id can be checked in a single command request.

#### Section 3.1.2 EPP <info> Command - compliant

If querying client is not sponsoring client, server does not send any contact object elements in response and the request is rejected for authorization.

#### Section 3.2.2 EPP <delete> Command - compliant

A delete is permitted only if the contact object is not associated with other known objects.

### 7.5. RFC 5734 EPP TRANSPORT OVER TCP

#### Section 2 Session Management - compliant

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

#### Section 3 Message Exchange - compliant

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

#### Section 8 Security considerations - ack.

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

#### Section 9 TLS Usage Profile - ack.

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

### 8.0. EPP EXTENSIONS

### 8.1. STANDARDIZED EXTENSIONS

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

### 8.2. COMPLIANCE WITH RFC 3735

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

### 8.3. COMPLIANCE WITH DOMAIN REGISTRY GRACE PERIOD MAPPING RFC 3915

#### Section 1 Introduction - compliant

Our SRS implementation supports all specified grace periods particularly, add grace period, auto-renew grace period, renew grace period, and transfer grace period.

#### Section 3.2 Registration Data and Supporting Information - compliant

Our SRS implementation supports free text and XML markup in the restore report.

#### Section 3.4 Client Statements - compliant

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

#### Section 5 Formal syntax - compliant

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

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

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

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

#### Section 4 DS Data Interface and Key Data Interface - compliant

Our SRS implementation supports only DS Data Interface across all commands applicable with DNSSEC extension.

#### Section 4.1 DS Data Interface - compliant

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

#### Section 4.2 Key Data Interface - compliant

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

#### Section 5.1.2 EPP <info> Command - compliant

This extension does not add any elements to the EPP <info> command. When an <info> command is processed successfully, the EPP <resData> contains child elements for EPP domain mapping. In addition, it contains a child <secDNS:infData> element that identifies extension namespace if the domain object has data associated with this extension. It is conditionally based on

whether or the client added the `<extURI>` element for this extension in the `<login>` command. Multiple DS data elements are supported.

#### Section 5.2.1 EPP `<create>` Command - compliant

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

#### Section 5.2.5 EPP `<update>` Command - compliant

Since the SRS implementation does not support the `<secDNS:update>` element's optional "urgent" attribute, an EPP error result code of 2102 is returned if the "urgent" attribute is specified in the command with value of Boolean true.

### 8.5. PROPRIETARY EXTENSION DOCUMENTATION

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

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

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

### 9.0. RESOURCING PLAN

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

#### Software Engineering:

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

#### Systems Engineering:

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

#### Network Engineering:

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

#### Database Operations:

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

#### Information Security Team:

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

#### Network Operations Center (NOC):

- Existing Department Personnel: Manager, two NOC Supervisors, 12 NOC Analysts

- First Year New Hires: Eight NOC Analysts

## 26. Whois

Q26 CHAR: 19908

### 1.0. INTRODUCTION

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

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

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

### 2.0. HIGH-LEVEL WHOIS SYSTEM DESCRIPTION

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

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

The other medium used for Whois is via web interface using clear, unencrypted text. The web interface is in an HTML format suitable for web browsers. This

interface is also available over an encrypted channel on port 443 using the HTTPS protocol.

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

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

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

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

#### 2.1. PII POLICY

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

#### 3.0. RELEVANT NETWORK DIAGRAM(S)

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

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

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

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

#### 4.0. INTERCONNECTIVITY WITH OTHER REGISTRY SYSTEMS

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



the rapid addition of new servers, typically same-day, should load require them.

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

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

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

#### 5.0. FREQUENCY OF SYNCHRONIZATION BETWEEN SERVERS

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

#### 6.0. POTENTIAL FORMS OF ABUSE

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

##### 6.1. DATA MINING ABUSE

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

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

##### 6.2. INVALID DATA INJECTION

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

##### 6.3. DISCLOSURE OF PRIVATE INFORMATION

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

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

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

#### 7.1. COMPLIANCE WITH SPECIFICATION 4

Compliance of Whois specifications with Specification 4 is as follows:

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

Evidence of Whois system compliance with this specification consists of:

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

#### 7.2. COMPLIANCE WITH SPECIFICATION 10 FOR WHOIS

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

##### 7.2.1. Emergency Thresholds

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

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

##### 7.2.2. Emergency Escalation

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

#### 8.0. COMPLIANCE WITH RFC 3912

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

- RFC 3912 Element, "A Whois server listens on TCP port 43 for requests from Whois clients": This requirement is properly implemented, as described in Section 1 above. Further, running Whois on ports other than port 43 is an option.
- RFC 3912 Element, "The Whois client makes a text request to the Whois server, then the Whois server replies with text content": The port 43 Whois service is a text-based query and response system. Thus, this requirement is also properly implemented.

- RFC 3912 Element, "All requests are terminated with ASCII CR and then ASCII LF. The response might contain more than one line of text, so the presence of ASCII CR or ASCII LF characters does not indicate the end of the response": This requirement is properly implemented for our TLD.
- RFC 3912 Element, "The Whois server closes its connection as soon as the output is finished": This requirement is properly implemented for our TLD, as described in Section 1 above.
- RFC 3912 Element, "The closed TCP connection is the indication to the client that the response has been received": This requirement is properly implemented.

#### 9.0. RESOURCING PLAN

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

##### Software Engineering:

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

##### Systems Engineering:

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

##### Network Engineering:

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

##### Database Operations:

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

##### Information Security Team:

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

##### Network Operations Center (NOC):

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

#### 11.0. PROVISION FOR SEARCHABLE WHOIS CAPABILITIES

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

meet or exceed the requirements indicated in section 1.8 of specification 4.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 27. Registration Life Cycle

Q27 CHAR: 19951

### 1.0. INTRODUCTION

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

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

### 2.0. INDUSTRY STANDARDS

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

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

### 3.0. REGISTRATION STATES

For a visual guide to this registration lifecycle discussion, please refer to

the attachment, Registration Lifecycle Illustrations. Please note that this text makes many references to the status of a domain. For brevity, we do not distinguish between the domain mapping status `<domain:status>` and the EPP Grace Period Mapping status `<rgp:rgpStatus>` as making this differentiation in every case would make this document more difficult to read and in this context does not improve understanding.

#### 4.0. AVAILABILITY

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

Before a user can register a new domain name, the registry performs an availability check. Possible outcomes of this availability check include:

1. Domain name is available for registration.
2. Domain name is already registered, regardless of the current state and not available for registration.
3. Domain name has been reserved by the registry.
4. Domain name string has been blocked because of a trademark claim.

#### 5.0. INITIAL REGISTRATION

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

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

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

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

#### 6.0. REGISTERED STATE - ADD GRACE PERIOD

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

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

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

#### 7.0. REGISTERED STATE

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

#### 8.0. REGISTRATION PERIOD EXTENSION

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

##### 8.1. EXTENSION VIA RENEW REQUEST

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

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

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

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

##### 8.2. EXTENSION VIA TRANSFER PROCESS

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

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

##### 8.3. EXTENSION VIA AUTO-RENEW

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

The Auto Renew Grace Period lasts for 45 days. At any time during this period, the Registrar can do one of four things: 1) passively accept the renewal; 2)

actively renew (to adjust renewal options); 3) delete the registration; or 4) transfer the registration.

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

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

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

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

#### 9.0. REQUEST TRANSFER

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

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

There are four ways to complete the transfer (and move it out of Pending Transfer status):

1. The transfer is auto-approved.
2. The losing registrar approves the transfer.
3. The losing registrar rejects the transfer.
4. The requesting registrar cancels the transfer.

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

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

During the five-day Pending Transfer state, the losing registrar can accelerate the process by explicitly accepting or rejecting the transfer. If the losing registrar takes either of these actions, the pendingTransfer status is removed.



Both of these actions are illustrated in Fig. 10 - Approve Transfer and Fig. 11 - Reject Transfer.

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

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

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

#### 10.0. REDEMPTION GRACE PERIOD

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

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

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

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

#### 11.0. DELETE

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

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

The registry then checks the various domain statuses for any restrictions that

might prevent deletion. If the domain's status includes either the `transferPending` or `deleteProhibited`, the name is not deleted and an error is returned to the registrar.

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

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

#### 12.0. ADDITIONAL STATUSES

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

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

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

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

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

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

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

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

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

#### 13.0. RESOURCING

Software Engineering:

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

Systems Engineering:

- Existing Department Personnel: Sr. Director IT Operations, 2 Sr. Systems Administrators, 2 Systems Administrators, 2 Sr. Systems Engineers, 2 Systems

#### Engineers

- New Hires: Systems Engineer

#### Network Engineering:

- Existing Department Personnel: Sr. Director IT Operations, two Sr. Network Engineers, 2 Network Engineers
- New Hires: Network Engineer

#### Database Operations:

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

#### Network Operations Center:

- Existing Department Personnel: Manager, 2 NOC Supervisors, 12 NOC Analysts
- New Hires: Eight NOC Analysts

## 28. Abuse Prevention and Mitigation

Q28 Standard CHAR: 29543

### 1.0. INTRODUCTION

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

Our approach to abuse prevention and mitigation includes the following:

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

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

### 2.0. ANTI-ABUSE POLICY

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

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

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

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

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

### 3.0. TLD ANTI-ABUSE POLICY

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

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

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

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

### 4.0. SINGLE ABUSE POINT OF CONTACT

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

The APOC e-mail address will be listed on the registry web site. We also will

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

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

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

#### 5.0. ABUSE INVESTIGATION AND MITIGATION

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

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

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

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

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

#### 6.0. POLICIES, PROCEDURES, AND SERVICE LEVELS

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

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

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

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

A "compromised" domain is one that has been hacked or otherwise compromised by

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

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

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

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

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

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

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

#### 7.0. ABUSE MONITORING AND METRICS

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

To enable active reporting of problems to the sponsoring registrars, our plan includes proactive monitoring for malicious use of the domains in the TLD. Our goal is to keep malicious activity at an acceptably low level, and mitigate it actively when it occurs—we may do so by using professional blocklists of domain names. For example, professional advisors such as LegitScript

(www.legitscript.com) may be used to identify and close down illegal "rogue" Internet pharmacies.

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

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

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

#### 8.0. HANDLING REPORTS FROM LAW ENFORCEMENT, COURT ORDERS

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

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

#### 9.0. PROHIBITING DOMAIN HIJACKINGS AND UNAPPROVED UPDATES

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

#### 10.0. ABUSE POLICY: ADDRESSING INTELLECTUAL PROPERTY INFRINGEMENT

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

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

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

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

#### 11.0. PROPOSED MEASURES FOR REMOVAL OF ORPHAN GLUE RECORDS

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

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

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

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

#### 12.0. METHODS TO PROMOTE WHOIS ACCURACY

##### 12.1. ENFORCING REQUIRED CONTACT DATA FIELDS

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

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

Contact Name [MANDATORY]  
Street1 [MANDATORY]  
City [MANDATORY]  
State/Province [optional]  
Country [MANDATORY]  
Postal Code [optional]  
Registrar Phone [MANDATORY]



Phone Ext [optional]  
Fax [optional]  
Fax Ext [optional]  
Email [MANDATORY]

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

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

## 12.2. POLICIES AND PROCEDURES TO ENHANCE WHOIS ACCURACY COMPLIANCE

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

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

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

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

<http://www.cira.ca/assets/Documents/Legal/Registrants/registantagreement.pdf>

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

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

## 12.3. PROXY/PRIVACY SERVICE POLICY TO CURB ABUSE

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

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

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

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

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

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

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

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

#### 14.0. CONTROLS TO ENSURE PROPER ACCESS TO DOMAIN FUNCTIONS

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

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

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

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

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

#### 15.0. RESOURCING PLAN

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

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

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

## 29. Rights Protection Mechanisms

Q29 Standard CHAR: 25023

### 1.0. INTRODUCTION

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

Protected Marks List (DPML) for the blocking of trademarked strings across multiple TLDs; and (ii) a Claims Plus product to alert registrars to registrations that potentially infringe existing marks.

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

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

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

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

## 2.0. NARRATIVE FOR Q29 FIGURE 1 OF 1

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

## 3.0. PRE-SUNRISE: RESERVED AND PREMIUM NAMES

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

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

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

#### 4.0. SUNRISE

##### 4.1. SUNRISE OVERVIEW

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

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

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

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

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

##### 4.2. SUNRISE: ELIGIBLE RIGHTS

Our Sunrise Eligibility Requirements (SERs) are:

###### 1. Ownership of a qualifying mark.

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

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

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

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

##### 4.3. SUNRISE TRADEMARK VALIDATION

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

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

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

To defray the costs of trademark validation and the Trademark Claims Service,

we will charge an application and/or validation fee for every application.

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

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

#### 4.5. CONTENDING APPLICATIONS, SUNRISE AUCTIONS

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

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

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

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

#### 4.6. SUNRISE DISPUTE RESOLUTION PROCESS (SUNRISE CHALLENGES)

We will retain the services of a well-known dispute resolution provider (such as WIPO) to help formulate the language of our Sunrise Dispute Resolution Process (SDRP, or "Sunrise Challenge") and hear the challenges filed under it. All applicants and registrars will be contractually obligated to follow the decisions handed down by the dispute resolution provider.

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

- (i) at the time the challenged domain name was registered, the registrant did not hold a trademark registration of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty;
- (ii) the domain name is not identical to the mark on which the registrant based its Sunrise registration;
- (iii) the trademark registration on which the registrant based its Sunrise registration is not of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; or

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

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

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

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

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

#### 5.0. TRADEMARK CLAIMS SERVICES

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

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

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

The Trademark Claims Notice will provide the prospective registrant access to the Trademark Clearinghouse Database information referenced in the Trademark Claims Notice. The notice will be provided in real time (or as soon as

possible) without cost to the prospective registrant or to those notified.

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

#### 6.0. GENERAL REGISTRATION

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

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

#### 7.0. UNIFORM RAPID SUSPENSION (URS)

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

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

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

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

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

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

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

#### 8.0. ONGOING RIGHTS PROTECTION MECHANISMS - UDRP



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

#### 9.0 ADDITIONAL RIGHTS PROTECTION MECHANISMS NOT REQUIRED BY ICANN

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

9.1 Claims Plus: This service will become available at the conclusion of the Trademark Claims service, and will remain available for at least the first five years of registry operations. Trademark owners who are fully registered in the Trademark Clearinghouse may obtain Claims Plus for their marks. We expect the service will be at low or no cost to trademark owners (contingent on Trademark Clearinghouse costs to registries). Claims Plus operates much like Trademark Claims with the exception that notices of potential trademark infringement are sent by the registry to any registrar whose customer performs a check-command or Whois query for a string subject to Claims Plus. Registrars may then take further implementation steps to advise their customers, or use this data to better improve the customer experience. In addition, the Whois at the registry website will output a full Trademark Claims notice for any query of an unregistered name that is subject to Claims Plus. (Note: The ongoing availability of Claims Plus will be contingent on continued access to a Trademark Clearinghouse. The technical viability of some Claims Plus features will be affected by eventual Trademark Clearinghouse rules on database caching).

9.2 Domain Protected Marks List: The DPML is a rights protection mechanism to assist trademark holders in protecting their intellectual property against undesired registrations of strings containing their marks. The DPML prevents (blocks) registration of second level domains that contain a trademarked term (note: the standard for DPML is "contains"—the protected string must contain the trademarked term). DPML requests will be validated against the Trademark Clearinghouse and the process will be similar to registering a domain name so the process will not be onerous to trademark holders. An SLD subject to DPML will be protected at the second level across all Donuts TLDs (i.e. all TLDs for which this SLD is available for registration). Donuts may cooperate with other registries to extend DPML to TLDs that are not operated by Donuts. The cost of DPML to trademark owners is expected to be significantly less than the cost of actually registering a name.

#### 10.0 ABUSIVE USE POLICIES AND TAKEDOWN PROCEDURES

In our response to Question #28, we describe our anti-abuse program, which is designed to address malware, phishing, spam, and other forms of abuse that may harm Internet users. This program is designed to actively discover, verify, and mitigate problems without infringing upon the rights of legitimate registrants. This program is designed for use in the open registration period. These procedures include the reporting of compromised websites/domains to registrars for cleanup by the registrants and their hosting providers. It also describes takedown procedures, and the timeframes and circumstances that apply for suspending domain names used improperly. Please see the response to Question #28 for full details.

We will institute a contractual obligation that proxy protection be stripped away if a domain is proven to be used for malicious purposes. For details, please see "Proxy/Privacy Service Policy to Curb Abuse" in the response to Question 28.

#### 11.0. REGISTRY-REGISTRAR CODE OF CONDUCT AS RELATED TO RIGHTS PROTECTION

We will comply fully with the Registry Code of Conduct specified in the New TLD Registry Agreement, Specification 9. In rights protection matters, we will comply by establishing an adequate "firewall" between the operations of any registrar we establish and the operations of the registry. As the Code requires, we will not "directly or indirectly show any preference or provide any special consideration to any registrar with respect to operational access to registry systems and related registry services". Here is a non-exhaustive list of specific steps we will take to accomplish this:

- We will evaluate and execute upon all rights protection tasks impartially, using the same criteria and procedures, regardless of a domain's sponsoring registrar.
- Any registrar we establish or have established at the time of registry launch will not receive preferential access to any premium names, any auctions, etc. Registry personnel and any registrar personnel that we may employ in the future will be prohibited from participating as bidders in any auctions for Landrush names.
- Any registrar staff we may employ in the future will have access to data and records relating only to the applications and registrations made by any registrar we establish, and will not have special access to data related to the applications and registrations made by other registrars.
- If a compliance function is involved, the compliance staffer will be responsible to the registry only, and not to a registrar we own or are "affiliated" with. For example, if a compliance staff member is assigned to conduct audits of WHOIS data, that staffer will not have duties with the registrar business. The staffer will be free of conflicts of interest, and will be enabled to discharge his or her duties to the registry effectively and impartially, regardless of the consequences to the registrar.

#### 12.0. RESOURCING PLAN

Overall management of RPMs is the responsibility of Donuts' VP of Business Operations. Our back-end registry operator will perform the majority of operational work associated with RPMs, as required by our agreement with them. Donuts VP of Business Operations will supervise the activity of this vendor.

Resources applied to RPMs include:

1. Legal team
  - a. We will have at least one legal counsel who will be dedicated to the registry with previous experience in domain disputes and Sunrise periods and will oversee the compliance and support teams with regard to the legal issues related to Sunrise and RPM's
  - b. We have outside counsel with domain and rights protection experience that is available to us as necessary
2. Dispute Resolution Provider (DRP): The DRP will help formulate Sunrise Rules and Policy, Sunrise Dispute Resolution Policy. The DRP will also examine challenges, but the challenger will be required to pay DRP fees directly to the DRP.
3. Compliance Department and Tech Support: There will be three dedicated personnel assigned to these areas. This staff will oversee URS requests and abuse reports on an ongoing basis.
4. Programming and technical operations. There are four dedicated personnel assigned to these functions.
5. Project Manager: There will be one person to coordinate the technical needs of this group with the registry IT department.

#### 13.0. ENDNOTES

- 1 "Regional" is understood to be a trans-national trademark registry, such as the European Union registry or the Benelux Office for Intellectual Property.

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

Q30A Standard CHAR: 19646

### 1.0. INTRODUCTION

Our Information Security (IS) Program and associated IS Policy, Standards and Procedures apply to all Company entities, employees, contractors, temps, systems, data, and processes. The Security Program is managed and maintained by the IS Team, supported by Executive Management and the Board of Directors.

Data and systems vary in sensitivity and criticality and do not unilaterally require the same control requirements. Our security policy classifies data and systems types and their applicable control requirements. All registry systems have the same data classification and are all managed to common security control framework. The data classification applied to all registry systems is our highest classification for confidentiality, availability and integrity, and the supporting control framework is consistent with the technical and operational requirements of a registry, and any supporting gTLD string, regardless of its nature or size. We have the experienced staff, robust system architecture and managed security controls to operate a registry and TLD of any size while providing reasonable assurance over the security, availability, and confidentiality of the systems supporting critical registry functions (i.e., registration services, registry databases, zone administration, and provision of domain name resolution services).

This document describes the governance of our IS Program and the control frameworks our security program aligns to (section 1.0), Security Policy requirements (section 2.0); security assessments conducted (see section 3.0), our process for executive oversight and visibility of risks to ensure continuous improvement (section 4.0), and security commitments to registrants (section 5). Details regarding how these control requirements are implemented, security roles and responsibilities and resources supporting these efforts are included in Security Policy B response.

### 2.0. INFORMATION SECURITY PROGRAM

The IS Program for our registry is governed by an IS Policy aligned to the general clauses of ISO 27001 requirements for an Information Security Management System (ISMS) and follows the control objectives where appropriate, given the data type and resulting security requirements. (ISO 27001 certification for the registry is not planned, however, our DNS/DNSSEC solution is 27001 certified). The IS Program follows a Plan-Do-Check-Act (PDCA) model of continuous improvement to ensure that the security program grows in maturity and that we provide reasonable assurance to our shareholders and Board of Directors that our systems and data are secure.

The High Security Top Level Domain (HSTLD) control framework incorporates ISO 27002, the code of practice for implementing an ISO 27001 ISMS. Therefore, our security program is already closely aligned HSTLD control framework. Furthermore, we agree to abide by the HSTLD Principle 1 and criteria 1.1 - 1.3. (See specifics in Security Policy B response):

Registry systems will be in-scope for Sarbanes-Oxley (SOX) compliance and will follow the SOX control framework governing access control, account management, change management, software development life cycle (SDLC), and job monitoring of all systems. Registry systems will be tested frequently by the IS team for compliance and audited by our internal audit firm, Protiviti, and external audit firm, Price Waterhouse Coopers (PWC), for compliance.

## 2.1. SECURITY PROGRAM GOVERNANCE

Our Information Security Program is governed by IS Policy, supported by standards, and guided by procedures to ensure uniformed compliance to the program. Standards and associated procedures in support of the policy are shown in Attachment A, Figure 1. Security Program documents are updated annually or upon any system or environment change, new legal or regulatory requirements, and/or findings from risk assessments. Any updates to security program are reviewed and approved by the Executive Vice President (EVP) of Information Technology (IT), EVP of Legal & General Counsel, and the EVP of People Operations before dissemination to all employees.

All employees are required to sign the IS Policy upon hire, upon any major changes, and/or annually. By signing the IS Policy, employees agree to abide by the supporting Standards and Procedures applicable to their job roles. To enable signing of the IS Policy, employees must pass a test to ensure competent understanding of the IS Policy and its key requirements.

## 3.0. INFORMATION SECURITY POLICY

### 3.1. INFORMATION ASSET CLASSIFICATION

The following data classification is applied to registry systems: High Business Impact (HBI): Business Confidential in accordance with the integrity, availability and confidentiality requirements of registry operations. All registry systems will follow Security Policy requirements for HBI systems regardless of the nature of the TLD string, financial materiality or size. HBI data if not properly secured, poses a high degree of risk to the Company and includes data pertaining to the Company's adherence to legal, regulatory and compliance requirements, mergers and acquisitions (M&A), and confidential data inclusive of, but is not limited to: Personally Identifiable Information (PII) (credit card data, Social Security Numbers (SSN) and account numbers); materially important financial information (before public disclosure), and information which the Board of Directors/Executive team deems to be a trade secret, which, if compromised, would cause grave harm to the execution of our business model.

HBI safeguards are designed, implemented and measured in alignment with confidentiality, integrity, availability and privacy requirements characterized by legal, regulatory and compliance obligations, or through directives issued by the Board of Directors (BOD) and Executive team. Where guidance is provided, such as the Payment Card Industry (PCI) Data Security Standard (DSS) Internal Audit Risk Control Matrices (RCMs), local, state and federal laws, and other applicable regulations, we put forth the appropriate level of effort and resources to meet those obligations. Where there is a lack of guidance or recommended safeguards, Risk Treatment Plans (RTP's) are designed in alignment with our standard risk management practices.

Other data classifications for Medium Business Impact (MBI): Business Sensitive and Low Business Impact (LBI): Public do not apply to registry systems.

### 3.2. INFORMATION ASSET MANAGEMENT

All registry systems have a designated owner and/or custodian who ensures appropriate security classifications are implemented and maintained throughout the lifecycle of the asset and that a periodic review of that classification is conducted. The system owner is also responsible for approving access and the type of access granted. The IS team, in conjunction with Legal, is responsible for defining the legal, regulatory and compliance requirements for registry system and data.

### 3.3. INFORMATION ASSET HANDLING, STORAGE & DISPOSAL

Media and documents containing HBI data must adhere to their respective legal,

regulatory and compliance requirements and follow the HBI Handling Standard and the retention requirements within the Document Retention Policy.

#### 3.4. ACCESS CONTROL

User authentication is required to access our network and system resources. We follow a least-privileged role based access model. Users are only provided access to the systems, services or information they have specifically been authorized to use by the system owner based on their job role. Each user is uniquely identified by an ID associated only with that user. User IDs must be disabled promptly upon a user's termination, or job role change.

Visitors must sign-in at the front desk of any company office upon arrival and escorted by an employee at all times. Visitors must wear a badge while on-site and return the badge when signing out at the front desk. Dates and times of all visitors as well as the name of the employee escorting them must be tracked for audit purposes.

Individuals permitted to access registry systems and HBI information must follow the HBI Identity & Access Management Standard. Details of our access controls are described in Part B of Question 30 response including; technical specifications of access management through Active Directory, our ticketing system, physical access controls to systems and environmental conditions at the datacenter.

#### 3.5. COMMUNICATIONS & OPERATIONAL SECURITY

##### 3.5.1. MALICIOUS CODE

Controls shall be implemented to protect against malicious code including but not limited to:

- Identification of vulnerabilities and applicable remediation activities, such as patching, operating system & software upgrades and/or remediation of web application code vulnerabilities.
- File-integrity monitoring shall be used, maintained and updated appropriately.
- An Intrusion Detection Solution (IDS) must be implemented on all HBI systems, maintained & updated continuously.
- Anti-virus (AV) software must be installed on HBI classified web & application systems and systems that provide access to HBI systems. AV software and virus definitions are updated on a regular basis and logs are retained for no less than one year.

##### 3.5.2. THREAT ANALYSIS & VULNERABILITY MANAGEMENT

On a regular basis, IS personnel must review newly identified vulnerability advisories from trusted organizations such as the Center for Internet Security, Microsoft, SANS Institute, SecurityFocus, and the CERT at Carnegie-Mellon University. Exposure to such vulnerabilities must be evaluated in a timely manner and appropriate measures taken to communicate vulnerabilities to the system owners, and remediate as required by the Vulnerability Management Standard. Internal and external network vulnerability scans, application & network layer penetration testing must be performed by qualified internal resource or an external third party at least quarterly or upon any significant network change. Web application vulnerability scanning is to be performed on a continual basis for our primary web properties applicable to their release cycles.

##### 3.5.3. CHANGE CONTROL

Changes to HBI systems including operating system upgrades, computing hardware, networks and applications must follow the Change Control Standard and procedures described in Security Policy question 30b.

#### 3.5.4. BACKUP & RESTORATION

Data critical to our operations shall be backed up according to our Backup and Restoration Standard. Specifics regarding Backup and Restoration requirements for registry systems are included in questions 37 & 38.

#### 3.6. NETWORK CONTROLS

- Appropriate controls must be established for ensuring the network is operated consistently and as planned over its entire lifecycle.
- Network systems must be synchronized with an agreed upon time source to ensure that all logs correctly reflect the same accurate time.
- Networked services will be managed in a manner that ensures connected users or services do not compromise the security of the other applications or services as required in the HBI Network Configuration Standard. Additional details are included in Question 32: Architecture response.

#### 3.7. DISASTER RECOVERY & BUSINESS CONTINUITY

The SVP of IT has responsibility for the management of disaster recovery and business continuity. Redundancy and fault-tolerance shall be built into systems whenever possible to minimize outages caused by hardware failures. Risk assessments shall be completed to identify events that may cause an interruption and the probability that an event may occur. Details regarding our registry continuity plan are included in our Question 39 response.

#### 3.8 SOFTWARE DEVELOPMENT LIFECYCLE

Advance planning and preparation is required to ensure new or modified systems have adequate security, capacity and resources to meet present and future requirements. Criteria for new information systems or upgrades must be established and acceptance testing carried out to ensure that the system performs as expected. Registry systems must follow the HBI Software Development Lifecycle (SDLC) Standard.

#### 3.9. SECURITY MONITORING

Audit logs that record user activities, system errors or faults, exceptions and security events shall be produced and retained according to legal, regulatory, and compliance requirements. Log files must be protected from unauthorized access or manipulation. IS is responsible for monitoring activity and access to HBI systems through regular log reviews.

#### 3.10. INVESTIGATION & INCIDENT MANAGEMENT RESPONSE

Potential security incidents must be immediately reported to the IS Team, EVP of IT, the Legal Department and/or the Incident Response. The Incident Response Team (IRT) is required to investigate: any real or suspected event that could impact the security of our network or computer systems; impose significant legal liabilities or financial loss, loss of proprietary data/trade secret, and/or harm to our goodwill. The Director of IS is responsible for the organization and maintenance of the IRT that provides accelerated problem notification, damage control, investigation and incident response services in the event of security incidents. Investigation and response processes follow the requirements of the Investigation and Incident Management Standard and supporting Incident Response Procedure (see Question 30b for details).

#### 3.11. LEGAL & REGULATORY COMPLIANCE

All relevant legal, regulatory and contractual requirements are defined, documented and maintained within the IS Policy. Critical records are protected from loss, destruction and falsification, in accordance with legal, contractual and business requirements as described in our Document Retention Policy. Compliance programs implemented that are applicable to Registry Services

include:

- Sarbanes Oxley (SOX): All employees managing and accessing SOX systems and/or data are required to follow SOX compliance controls.
- Data Privacy and Disclosure of Personally Identifiable Information (PII): data protection and privacy shall be ensured as required by legal and regulatory requirements, which may include state breach and disclosure laws, US and EU Safe Harbor compliance directives.

Other compliance programs implemented but not applicable to Registry systems include the Payment Card Industry (PCI) Data Security Standard (DSS), Office of Foreign Assets Control (OFAC) requirements, Copyright Infringement & DMCA.

#### 4.0. SECURITY ASSESSMENTS

Our IS team conducts frequent security assessments to analyze threats, vulnerabilities and risks associated with our systems and data. Additionally, we contract with several third parties to conduct independent security posture assessments as described below. Details of these assessments are provided in our Security Policy B response.

##### 4.1. THIRD PARTY SECURITY ASSESSMENTS

We outsource the following third party security assessments (scope, vendor, frequency and remediation requirements of any issues found are detailed in our Security Policy B response); Web Application Security Vulnerability testing, quarterly PCI ASV scans, Sarbanes-Oxley (SOX) control design and operating effectiveness testing and Network and System Security Analysis.

##### 4.2. INTERNAL SECURITY ASSESSMENTS

The IS team conducts routine and continual internal testing (scope, frequency, and remediation requirements of any issues found are detailed in our Security Policy B response) including; web application security vulnerability testing, external and internal vulnerability scanning, system and network infrastructure penetration testing, access control appropriateness reviews, wireless access point discovery, network security device configuration analysis and an annual comprehensive enterprise risk analysis.

#### 5.0. EXECUTIVE OVERSIGHT & CONTINUOUS IMPROVEMENT

In addition to the responsibility for Information Security residing within the IS team and SVP of IT, risk treatment decisions are also the responsibility of the executive of the business unit responsible for the risk. Any risk with potential to impact the business financially or legally in a material way is overseen by the Incident Response Management team and/or the Audit Committee. See Figure 2 in Attachment A. The Incident Response Management Team or Audit Committee will provide assistance with management action plans and remediation.

##### 5.1. GOVERNANCE RISK & COMPLIANCE

We have deployed RSA's Archer Enterprise Governance Risk and Compliance (eGRC) Tool to provide an independent benchmarking of risk, compliance and security metrics, assist with executive risk reporting and reduce risk treatment decision making time, enforcing continuous improvement. The eGRC provides automated reporting of registry systems compliance with the security program as a whole, SOX Compliance, and our Vulnerability Management Standard. The eGRC dashboard continuously monitors risks and threats (through automated feeds from our vulnerability testing tools and third party data feeds such as Microsoft, CERT, WhiteHat, etc.) that are actionable. See Attachment A for more details on the GRC solutions deployed.

#### 6.0. SECURITY COMMITMENTS TO REGISTRANTS

We operate all registry systems in a highly secured environment with appropriate controls for protecting HBI data and ensuring all systems remain confidential, have integrity, and are highly available. Registrants can assume that:

1. We safeguard the confidentiality, integrity and availability of registrant data through access control and change management:
  - Access to data is restricted to personnel based on job role and requires 2 factors of authentication.
  - All system changes follow SOX-compliant controls and adequate testing is performed to ensure production pushes are stable and secure.
2. The network and systems are deployed in high availability with a redundant hot datacenter to ensure maximum availability.
3. Systems are continually assessed for threats and vulnerabilities and remediated as required by the Vulnerability Management Standard to ensure protection from external malicious acts.
  - We conduct continual testing for web code security vulnerabilities (cross-site scripting, SQL Injection, etc.) during the development cycle and in production.
4. All potential security incidents are investigated and remediated as required by our Incident Investigation & Response Standard, any resulting problems are managed to prevent any recurrence throughout the registry.

We believe the security measures detailed in this application are commensurate with the nature of the TLD string being applied for. In addition to the system/infrastructure security policies and measures described in our response to this Q30, we also provide additional safety and security measures for this string.

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

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

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

**© Internet Corporation For Assigned Names and Numbers.**





# **Annex 8.**



## **New gTLD Application Submitted to ICANN by: Schlund Technologies GmbH**

**String: WEB**

**Originally Posted: 13 June 2012**

**Application ID: 1-1013-77165**

### **Applicant Information**

#### **1. Full legal name**

Schlund Technologies GmbH

#### **2. Address of the principal place of business**

Contact Information Redacted

#### **3. Phone number**

Contact Information Redacted

#### **4. Fax number**

Contact Information Redacted

## 5. If applicable, website or URL

<http://www.schlundtech.com>

## Primary Contact

### 6(a). Name

John Kane

### 6(b). Title

Vice President, Corporate Services

### 6(c). Address

### 6(d). Phone Number

Contact Information Redacted

### 6(e). Fax Number

### 6(f). Email Address

Contact Information Redacted

## Secondary Contact

### 7(a). Name

Alex Howerton

**7(b). Title**

Account Manager

**7(c). Address****7(d). Phone Number**

Contact Information Redacted

**7(e). Fax Number****7(f). Email Address**

Contact Information Redacted

**Proof of Legal Establishment****8(a). Legal form of the Applicant**

limited liability corporation (Gesellschaft mit beschränkter Haftung, GmbH)

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

Germany

**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.**

InterNetX GmbH

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

not a joint venture

## Applicant Background

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

Thomas Mörz	CEO
-------------	-----

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

InterNetX GmbH	not applicable
----------------	----------------

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

## Applied-for gTLD string

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

WEB

**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.**

Schlund Technologies GmbH, supported by Afilias, the back-end provider of registry services, anticipates the introduction of this TLD without operational or rendering problems. Based on a decade of experience launching and operating new TLDs, Afilias, the back-end provider of registry services for this TLD, is confident the launch and operation of this TLD presents no known challenges. The rationale for this opinion includes:

- The string is not complex and is represented in standard ASCII characters and follows relevant technical, operational and policy standards;
- The string length is within lengths currently supported in the root and by ubiquitous Internet programs such as web browsers and mail applications;
- There are no new standards required for the introduction of this TLD;
- No onerous requirements are being made on registrars, registrants or Internet users, and;
- The existing secure, stable and reliable Afilias SRS, DNS, WHOIS and supporting systems and staff are amply provisioned and prepared to meet the needs of this TLD.

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

## Mission/Purpose

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

.WEB is intended to become one of the most common and easily accessible TLDs on the Internet, vastly expanding options for creating domains, and giving new opportunities to those who were unable to obtain a desired domain name under the existing TLD structure.

At the end of 2011, there were 95.5 million registered .com domain names and 220 million total registered domain names (Source: <http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/>). The interest and demand for new domains is only expected to grow. The .WEB TLD will help facilitate the expansion of those opportunities for Internet users, with a concise and memorable extension.

We expect that the demand to create and own new domains will drive the rapid expansion of the .WEB TLD. In conjunction with our branding and registrar promotion, we forecast 1,371,900 domains under management (DUMs) after three years.



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

.WEB will quickly develop into one of the premier, open TLDs on the Internet.

### i General goals

Schlund Technologies GmbH will engage in general marketing and branding, as well as outreach and marketing support to registrars to establish awareness of the .WEB TLD and its intended uses in the minds of the public. The anticipated popularity of this TLD will make it very attractive to registrars, incentivizing them to work with Schlund Technologies GmbH to make the TLD grow rapidly.

### ii How .WEB adds to the current space

.WEB facilitates greatly expanded opportunities for domain creation and innovative use of the Internet. Individuals and entities who have felt limited in their opportunities to obtain a desired domain name will have new options available to them.

With a TLD as concise and memorable as .WEB, Internet users will have a truly unburdened space to create an online entity devoid of associations with a commercial enterprise. Despite its broad use, the .com extension has a market perception of domains with a business or commercially focused purpose. With a .WEB domain, the average consumer has an option to create content, host mail servers or provide other services with a name that does not carry images of a business. For the online-only retailer, there will exist the opportunity to create a brand without a brick-and-mortar expectations. Overall, the vast and Internet-focused character of .WEB adds a universally understandable new home for domains.

### iii User experience goals

Schlund Technologies GmbH intends for .WEB to be one of the most recognizable and useful TLDs on the Internet. .WEB will be positioned as not simply an alternative to existing generic gTLDs, but as an expanded option beyond existing opportunities to develop an Internet identity and presence. The explosion of new domain possibilities will foster innovation and creativity on the part of registrants, who will then create new and diverse user experiences for users. The competition among new registrants, as well as with established site operators, will improve the user experience.

### iv Registry policies

.WEB will be an open TLD, generally available to all registrants (except in the Sunrise period).

In general, domains will be offered for periods of one to ten years, but no greater than ten years. Initial registrations made in the Sunrise period may have a minimum number of years required. For example, there may be a policy that all Sunrise names must be registered for an initial term of at least two years.

The roll-out of our TLD is anticipated to feature the following phases:

- Reservation of reserved names and premium names, which will be distributed through special mechanisms (detailed below).
- Sunrise – the required period for trademark owners to secure their domains before availability to the general public. This phase will feature applications for domain strings, verification of trademarks via Trademark Clearinghouse and a trademark verification agent, auctions between qualified parties who wish to secure the same string, and a Trademark Claims Service.
- General Availability period – real-time registrations, made on a first-come first-served basis. Trademark Claims Service will be in use at least for the first 60 days after General Availability applications open.

The registration of domain names in the .WEB TLD will follow the standard practices, procedures and policies Afiliias, the back-end provider of registry

services, currently has in place. This includes the following:

- Domain registration policies (for example, grace periods, transfer policies, etc.) are defined in response #27.
- Abuse prevention tools and policies, for example, measures to promote WHOIS accuracy and efforts to reduce phishing and pharming, are discussed in detail in our response #28.
- Rights protection mechanisms and dispute resolution mechanism policies (for example, UDRP, URS) are detailed in #29.

Other detailed policies for this domain include policies for reserved names.

#### Reserved names

There are two categories of reserved names for this TLD: registry reserved and premium names.

##### Registry reserved names

We will reserve the following classes of domain names, which will not be made generally available to registrants via the Sunrise or subsequent periods:

- All of the reserved names required in Specification 5 of the new gTLD Registry Agreement;
- The geographic names required in Specification 5 of the new gTLD Registry Agreement, and may be released to the extent that Registry Operator reaches agreement with the government and country-code manager;
- The registry operator's own name and variations thereof, and registry operations names (such as registry.tld, and www.tld), for internal use;
- Names related to ICANN and Internet standards bodies (iana.tld, ietf.tld, w3c.tld, etc.), and may be released to the extent that Registry Operator reaches agreement with ICANN.

The list of reserved names will be published publicly before the Sunrise period begins, so that registrars and potential registrants will know which names have been set aside.

##### Premium names

The registry will also designate a set of premium domain names, set aside for distribution via special mechanisms. The list of premium names will be published publicly before the Sunrise period begins, so that registrars and potential registrants will know that these names are not available. Premium names may be distributed via mechanisms such as requests for proposals, contests, direct sales, and auctions.

For the auctioning of premium names, we intend to contract with an established auction provider that has successfully conducted domain auctions. This will ensure that there is a tested, trustworthy technical platform for the auctions, auditable records, and reliable collection mechanisms. With our chosen auction provider, we will create and post policies and procedures that ensure clear, fair, and ethical auctions. As an example of such a policy, all employees of the registry operator and its contractors will be strictly prohibited from bidding in auctions for domains in the TLD. We expect a comprehensive and robust set of auction rules to cover possible scenarios, such as how domains will be awarded if the winning bidder does not make payment.

##### v. Privacy and confidential information protection

As per the New gTLD Registry Agreement, we will make domain contact data (and other fields) freely and publicly available via a Web-based WHOIS server. This default set of fields includes the mandatory publication of registrant data. Our Registry-Registrar Agreement will require that registrants consent to this publication.

We shall notify each of our registrars regarding the purposes for which data about any identified or identifiable natural person ("Personal Data") submitted to the Registry Operator by such registrar is collected and used, and the intended recipients (or categories of recipients) of such Personal Data (the

data in question is essentially the registrant and contact data required to be published in the WHOIS). We will require each registrar to obtain the consent of each registrant in the TLD for the collection and use of such Personal Data. The policies will be posted publicly on our TLD web site. As the registry operator, we shall not use or authorize the use of Personal Data in any way that is incompatible with the notice provided to registrars.

Our privacy and data use policies are as follows:

- As registry operator, we do not plan on selling bulk WHOIS data. We will not sell contact data in any way. We will not allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations.
- We may use registration data in the aggregate for marketing purposes.
- DNS query data will never be sold in a way that is personally identifiable.
- We may from time to time use the demographic data collected for statistical analysis, provided that this analysis will not disclose individual Personal Data and provided that such use is compatible with the notice provided to registrars regarding the purpose and procedures for such use.

As the registry operator we shall take significant steps to protect Personal Data collected from registrars from loss, misuse, unauthorized disclosure, alteration, or destruction. In our responses to Question 30 ("Security Policy") and Question 38 ("Escrow") we detail the security policies and procedures we will use to protect the registry system and the data contained therein from unauthorized access and loss.

Please see our response to Question 26 ("WHOIS") regarding "searchable WHOIS" and rate-limiting. That section contains details about how we will limit the mining of WHOIS data by spammers and other parties who abuse access to the WHOIS.

In order to acquire and maintain accreditation for our TLD, we will require registrars to adhere to certain information technology policies designed to help protect registrant data. These will include standards for access to the registry system and password management protocols. Our response to Question 30, "Security Policy" provides details of implementation.

We will allow the use of proxy and privacy services, which can protect the personal data of registrants from spammers and other parties that mine zone files and WHOIS data. We are aware that there are parties who may use privacy services to protect their free speech rights, or to avoid religious or political persecution.

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

Schlund Technologies GmbH, supported by Afilias, the back-end provider of registry services, has adopted the above-mentioned and other policies to ensure fair and equitable access and cost structures to the Internet community, including:

- no new burdens placed on the Internet community to resolve name disputes
- utilization of standard registration practices and policies (as detailed in responses to questions 27, 28, 29)
- protection of trademarks at launch and on-going operations (as detailed in the response to question 29)
- fair and reasonable wholesale prices
- fair and equitable treatment of registrars

As per the ICANN Registry Agreement, we will use only ICANN-accredited registrars, and will provide non-discriminatory access to registry services to those registrars.

### Pricing Policies and Commitments

Pricing for domain names at General Availability will be €6 per domain year for the first year, then increase 5.0% per year in subsequent years for the next five years. Applicant reserves the right to reduce this pricing for promotional purposes in a manner available to all accredited registrars. Registry Operator reserves the right to work with ICANN to initiate an increase in the wholesale price of domains if required. Registry Operator will provide reasonable notice to the registrars of any approved price increase.

## Community-based Designation

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

No

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

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

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

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

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

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

Attachments are not displayed on this form.

## Geographic Names

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

No

## Protection of Geographic Names

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

We will protect names with national or geographic significance by reserving the country and territory names at the second level and at all other levels within the TLD, as per the requirements in the New TLD Registry Agreement (Specification 5, paragraph 5).

We will employ a series of rules to translate the geographical names required to be reserved by Specification 5, paragraph 5 to a form consistent with the "host names" format used in domain names.

Considering the Governmental Advisory Committee (GAC) advice "Principles regarding new gTLDs", these domains will be blocked, at no cost to governments, public authorities, or IGOs, before the TLD is introduced (Sunrise), so that no parties may apply for them. We will publish a list of these names before Sunrise, so our registrars and their prospective applicants can be aware that these names are reserved.

We will define a procedure so that governments can request the above reserved domain(s) if they would like to take possession of them. This procedure will be based on existing methodology developed for the release of country names in the .INFO TLD. For example, we will require a written request from the country's GAC representative, or a written request from the country's relevant Ministry or Department. We will allow the designated beneficiary (the Registrant) to register the name, with an accredited Afilias Registrar, possibly using an authorization number transmitted directly to the designated beneficiary in the country concerned.

As defined by Specification 5, paragraph 5, such geographic domains may be released to the extent that Registry Operator reaches agreement with the applicable government(s). Registry operator will work with respective GAC representatives of the country's relevant Ministry of Department to obtain their release of the names to the Registry Operator.

If internationalized domains names (IDNs) are introduced in the TLD in the future, we will also reserve the IDN versions of the country names in the

relevant script(s) before IDNs become available to the public. If we find it advisable and practical, we will confer with relevant language authorities so that we can reserve the IDN domains properly along with their variants.

Regarding GAC advice regarding second-level domains not specified via Specification 5, paragraph 5: All domains awarded to registrants are subject to the Uniform Domain Name Dispute Resolution Policy (UDRP), and to any properly-situated court proceeding. We will ensure appropriate procedures to allow governments, public authorities or IGO's to challenge abuses of names with national or geographic significance at the second level. In its registry-registrar agreement, and flowing down to registrar-registrant agreements, the registry operator will institute a provision to suspend domains names in the event of a dispute. We may exercise that right in the case of a dispute over a geographic name.

## Registry Services

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

Throughout the technical portion (#23 - #44) of this application, answers are provided directly from Afiliias, the back-end provider of registry services for this TLD. Schlund Technologies GmbH chose Afiliias as its back-end provider because Afiliias has more experience successfully applying to ICANN and launching new TLDs than any other provider. Afiliias is the ICANN-contracted registry operator of the .INFO and .MOBI TLDs, and Afiliias is the back-end registry services provider for other ICANN TLDs including .ORG, .ASIA, .AERO, and .XXX.

Registry services for this TLD will be performed by Afiliias in the same responsible manner used to support 16 top level domains today. Afiliias supports more ICANN-contracted TLDs (6) than any other provider currently. Afiliias' primary corporate mission is to deliver secure, stable and reliable registry services. This TLD will utilize an existing, proven team and platform for registry services with:

- A stable and secure, state-of-the-art, EPP-based SRS with ample storage capacity, data security provisions and scalability that is proven with registrars who account for over 95% of all gTLD domain name registration activity (over 375 registrars);
- A reliable, 100% available DNS service (zone file generation, publication and dissemination) tested to withstand severe DDoS attacks and dramatic growth in Internet use;
- A WHOIS service that is flexible and standards compliant, with search capabilities to address both registrar and end-user needs; includes consideration for evolving standards, such as RESTful, or draft-kucherawy-wierds;
- Experience introducing IDNs in the following languages: German (DE), Spanish (ES), Polish (PL), Swedish (SV), Danish (DA), Hungarian (HU), Icelandic (IS), Latvian (LV), Lithuanian (LT), Korean (KO), Simplified and Traditional Chinese (CN), Devanagari (HI-DEVA), Russian (RU), Belarusian (BE), Ukrainian (UK), Bosnian (BS), Serbian (SR), Macedonian (MK) and Bulgarian (BG) across the TLDs it serves;
- A registry platform that is both IPv6 and DNSSEC enabled;
- An experienced, respected team of professionals active in standards development of innovative services such as DNSSEC and IDN support;
- Methods to limit domain abuse, remove outdated and inaccurate data, and ensure the integrity of the SRS, and;

- Customer support and reporting capabilities to meet financial and administrative needs, e.g., 24x7 call center support, integration support, billing, and daily, weekly, and monthly reporting.

Afilias will support this TLD in accordance with the specific policies and procedures of Schlund Technologies GmbH (the "registry operator"), leveraging a proven registry infrastructure that is fully operational, staffed with professionals, massively provisioned, and immediately ready to launch and maintain this TLD.

The below response includes a description of the registry services to be provided for this TLD, additional services provided to support registry operations, and an overview of Afilias' approach to registry management.

#### Registry services to be provided

To support this TLD, Schlund Technologies GmbH and Afilias will offer the following registry services, all in accordance with relevant technical standards and policies:

- Receipt of data from registrars concerning registration for domain names and nameservers, and provision to registrars of status information relating to the EPP-based domain services for registration, queries, updates, transfers, renewals, and other domain management functions. Please see our responses to questions #24, #25, and #27 for full details, which we request be incorporated here by reference.
- Operation of the registry DNS servers: The Afilias DNS system, run and managed by Afilias, is a massively provisioned DNS infrastructure that utilizes among the most sophisticated DNS architecture, hardware, software and redundant design created. Afilias' industry-leading system works in a seamless way to incorporate nameservers from any number of other secondary DNS service vendors. Please see our response to question #35 for full details, which we request be incorporated here by reference.
- Dissemination of TLD zone files: Afilias' distinctive architecture allows for real-time updates and maximum stability for zone file generation, publication and dissemination. Please see our response to question #34 for full details, which we request be incorporated here by reference.
- Dissemination of contact or other information concerning domain registrations: A port 43 WHOIS service with basic and expanded search capabilities with requisite measures to prevent abuse. Please see our response to question #26 for full details, which we request be incorporated here by reference.
- Internationalized Domain Names (IDNs): Ability to support all protocol valid Unicode characters at every level of the TLD, including alphabetic, ideographic and right-to-left scripts, in conformance with the ICANN IDN Guidelines. Please see our response to question #44 for full details, which we request be incorporated here by reference.
- DNS Security Extensions (DNSSEC): A fully DNSSEC-enabled registry, with a stable and efficient means of signing and managing zones. This includes the ability to safeguard keys and manage keys completely. Please see our response to question #43 for full details, which we request be incorporated here by reference.

Each service will meet or exceed the contract service level agreement. All registry services for this TLD will be provided in a standards-compliant manner.

#### Security

Afilias addresses security in every significant aspect - physical, data and network as well as process. Afilias' approach to security permeates every aspect of the registry services provided. A dedicated security function exists within the company to continually identify existing and potential threats, and to put in place comprehensive mitigation plans for each identified threat. In addition, a rapid security response plan exists to respond comprehensively to

unknown or unidentified threats. The specific threats and Afilias mitigation plans are defined in our response to question #30(b); please see that response for complete information. In short, Afilias is committed to ensuring the confidentiality, integrity, and availability of all information.

#### New registry services

No new registry services are planned for the launch of this TLD.

#### Additional services to support registry operation

Numerous supporting services and functions facilitate effective management of the TLD. These support services are also supported by Afilias, including:

- Customer support: 24x7 live phone and e-mail support for customers to address any access, update or other issues they may encounter. This includes assisting the customer identification of the problem as well as solving it. Customers include registrars and the registry operator, but not registrants except in unusual circumstances. Customers have access to a web-based portal for a rapid and transparent view of the status of pending issues.
- Financial services: billing and account reconciliation for all registry services according to pricing established in respective agreements.

Reporting is an important component of supporting registry operations. Afilias will provide reporting to the registry operator and registrars, and financial reporting.

#### Reporting provided to registry operator

Afilias provides an extensive suite of reports to the registry operator, including daily, weekly and monthly reports with data at the transaction level that enable the registry operator to track and reconcile at whatever level of detail preferred. Afilias provides the exact data required by ICANN in the required format to enable the registry operator to meet its technical reporting requirements to ICANN.

In addition, Afilias offers access to a data warehouse capability that will enable near real-time data to be available 24x7. This can be arranged by informing the Afilias Account Manager regarding who should have access. Afilias' data warehouse capability enables drill-down analytics all the way to the transaction level.

#### Reporting available to registrars

Afilias provides an extensive suite of reporting to registrars and has been doing so in an exemplary manner for more than ten years. Specifically, Afilias provides daily, weekly and monthly reports with detail at the transaction level to enable registrars to track and reconcile at whatever level of detail they prefer.

Reports are provided in standard formats, facilitating import for use by virtually any registrar analytical tool. Registrar reports are available for download via a secure administrative interface. A given registrar will only have access to its own reports. These include the following:

- Daily Reports: Transaction Report, Billable Transactions Report, and Transfer Reports;
- Weekly: Domain Status and Nameserver Report, Weekly Nameserver Report, Domains Hosted by Nameserver Weekly Report, and;
- Monthly: Billing Report and Monthly Expiring Domains Report.

Weekly registrar reports are maintained for each registrar for four weeks. Weekly reports older than four weeks will be archived for a period of six months, after which they will be deleted.

#### Financial reporting



Registrar account balances are updated real-time when payments and withdrawals are posted to the registrars' accounts. In addition, the registrar account balances are updated as and when they perform billable transactions at the registry level.

Afilias provides Deposit/Withdrawal Reports that are updated periodically to reflect payments received or credits and withdrawals posted to the registrar accounts.

The following reports are also available: a) Daily Billable Transaction Report, containing details of all the billable transactions performed by all the registrars in the SRS, b) daily e-mail reports containing the number of domains in the registry and a summary of the number and types of billable transactions performed by the registrars, and c) registry operator versions of most registrar reports (for example, a daily Transfer Report that details all transfer activity between all of the registrars in the SRS).

#### Afilias approach to registry support

Afilias, the back end registry services provider for this TLD, is dedicated to managing the technical operations and support of this TLD in a secure, stable and reliable manner. Afilias has worked closely with Schlund Technologies GmbH to review specific needs and objectives of this TLD. The resulting comprehensive plans are illustrated in technical responses #24-44, drafted by Afilias given Schlund Technologies GmbH requirements. Afilias and Schlund Technologies GmbH also worked together to provide financial responses for this application which demonstrate cost and technology consistent with the size and objectives of this TLD.

Afilias is the registry services provider for this and several other TLD applications. Over the past 11 years of providing services for gTLD and ccTLDs, Afilias has accumulated experience about resourcing levels necessary to provide high quality services with conformance to strict service requirements. Afilias currently supports over 20 million domain names, spread across 16 TLDs, with over 400 accredited registrars.

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

With over a decade of registry experience, Afilias has the depth and breadth of experience that ensure existing and new needs are addressed, all while meeting or exceeding service level requirements and customer expectations. This is evident in Afilias' participation in business, policy and technical organizations supporting registry and Internet technology within ICANN and related organizations. This allows Afilias to be at the forefront of security initiatives such as: DNSSEC, wherein Afilias worked with Public Interest Registry (PIR) to make the .ORG registry the first DNSSEC enabled gTLD and the largest TLD enabled at the time; in enhancing the Internet experience for users across the globe by leading development of IDNs; in pioneering the use of open-source technologies by its usage of PostgreSQL, and; being the first to offer near-real-time dissemination of DNS zone data.

The ability to observe tightening resources for critical functions and the capacity to add extra resources ahead of a threshold event are factors that Afilias is well versed in. Afilias' human resources team, along with well-

established relationships with external organizations, enables it to fill both long-term and short-term resource needs expediently.

Afilias' growth from a few domains to serving 20 million domain names across 16 TLDs and 400 accredited registrars indicates that the relationship between the number of people required and the volume of domains supported is not linear. In other words, servicing 100 TLDs does not automatically require 6 times more staff than servicing 16 TLDs. Similarly, an increase in the number of domains under management does not require in a linear increase in resources. Afilias carefully tracks the relationship between resources deployed and domains to be serviced, and pro-actively reviews this metric in order to retain a safe margin of error. This enables Afilias to add, train and prepare new staff well in advance of the need, allowing consistent delivery of high quality services.

## Demonstration of Technical & Operational Capability

### 24. Shared Registration System (SRS) Performance

Answers for this question (#24) are provided directly from Afilias, the back-end provider of registry services for this TLD.

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE " <" and "> " CHARACTERS), WHICH ICANN INFORMS AFILIAS (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE.

Afilias operates a state-of-the-art EPP-based Shared Registration System (SRS) that is secure, stable and reliable. The SRS is a critical component of registry operations that must balance the business requirements for the registry and its customers, such as numerous domain acquisition and management functions. The SRS meets or exceeds all ICANN requirements given that Afilias:

- Operates a secure, stable and reliable SRS which updates in real-time and in full compliance with Specification 6 of the new gTLD Registry Agreement;
- Is committed to continuously enhancing our SRS to meet existing and future needs;
- Currently exceeds contractual requirements and will perform in compliance with Specification 10 of the new gTLD Registry Agreement;
- Provides SRS functionality and staff, financial, and other resources to more than adequately meet the technical needs of this TLD, and;
- Manages the SRS with a team of experienced technical professionals who can seamlessly integrate this TLD into the Afilias registry platform and support the TLD in a secure, stable and reliable manner.

Description of operation of the SRS, including diagrams

Afilias' SRS provides the same advanced functionality as that used in the .INFO and .ORG registries, as well as the fourteen other TLDs currently supported by Afilias. The Afilias registry system is standards-compliant and utilizes proven technology, ensuring global familiarity for registrars, and it is protected by our massively provisioned infrastructure that mitigates the risk of disaster.

EPP functionality is described fully in our response to question #25; please consider those answers incorporated here by reference. An abbreviated list of Afilias SRS functionality includes:

- Domain registration: Afilias provides registration of names in the TLD, in both ASCII and IDN forms, to accredited registrars via EPP and a web-based administration tool.

- Domain renewal: Afiliias provides services that allow registrars the ability to renew domains under sponsorship at any time. Further, the registry performs the automated renewal of all domain names at the expiration of their term, and allows registrars to rescind automatic renewals within a specified number of days after the transaction for a full refund.
- Transfer: Afiliias provides efficient and automated procedures to facilitate the transfer of sponsorship of a domain name between accredited registrars. Further, the registry enables bulk transfers of domains under the provisions of the Registry-Registrar Agreement.
- RGP and restoring deleted domain registrations: Afiliias provides support for the Redemption Grace Period (RGP) as needed, enabling the restoration of deleted registrations.
- Other grace periods and conformance with ICANN guidelines: Afiliias provides support for other grace periods that are evolving as standard practice inside the ICANN community. In addition, the Afiliias registry system supports the evolving ICANN guidelines on IDNs.

Afiliias also supports the basic check, delete, and modify commands.

As required for all new gTLDs, Afiliias provides "thick" registry system functionality. In this model, all key contact details for each domain are stored in the registry. This allows better access to domain data and provides uniformity in storing the information.

Afiliias' SRS complies today and will continue to comply with global best practices including relevant RFCs, ICANN requirements, and this TLD's respective domain policies. With over a decade of experience, Afiliias has fully documented and tested policies and procedures, and our highly skilled team members are active participants of the major relevant technology and standards organizations, so ICANN can be assured that SRS performance and compliance are met. Full details regarding the SRS system and network architecture are provided in responses to questions #31 and #32; please consider those answers incorporated here by reference.

#### SRS servers and software

All applications and databases for this TLD will run in a virtual environment currently hosted by a cluster of servers equipped with the latest Intel Westmere multi-core processors. (It is possible that by the time this application is evaluated and systems deployed, Westmere processors may no longer be the "latest"; the Afiliias policy is to use the most advanced, stable technology available at the time of deployment.) The data for the registry will be stored on storage arrays of solid state drives shared over a fast storage area network. The virtual environment allows the infrastructure to easily scale both vertically and horizontally to cater to changing demand. It also facilitates effective utilization of system resources, thus reducing energy consumption and carbon footprint.

The network firewalls, routers and switches support all applications and servers. Hardware traffic shapers are used to enforce an equitable access policy for connections coming from registrars. The registry system accommodates both IPv4 and IPv6 addresses. Hardware load balancers accelerate TLS/SSL handshaking and distribute load among a pool of application servers.

Each of the servers and network devices are equipped with redundant, hot-swappable components and multiple connections to ancillary systems. Additionally, 24x7 support agreements with a four-hour response time at all our data centers guarantee replacement of failed parts in the shortest time possible.

Examples of current system and network devices used are:

- Servers: Cisco UCS B230 blade servers
- SAN storage arrays: IBM Storwize V7000 with Solid State Drives
- SAN switches: Brocade 5100
- Firewalls: Cisco ASA 5585-X

- Load balancers: F5 Big-IP 6900
- Traffic shapers: Procera PacketLogic PL8720
- Routers: Juniper MX40 3D
- Network switches: Cisco Nexus 7010, Nexus 5548, Nexus 2232

These system components are upgraded and updated as required, and have usage and performance thresholds which trigger upgrade review points. In each data center, there is a minimum of two of each network component, a minimum of 25 servers, and a minimum of two storage arrays.

Technical components of the SRS include the following items, continually checked and upgraded as needed: SRS, WHOIS, web admin tool, DNS, DNS distributor, reporting, invoicing tools, and deferred revenue system (as needed).

All hardware is massively provisioned to ensure stability under all forecast volumes from launch through "normal" operations of average daily and peak capacities. Each and every system application, server, storage and network device is continuously monitored by the Afilias Network Operations Center for performance and availability. The data gathered is used by dynamic predictive analysis tools in real-time to raise alerts for unusual resource demands. Should any volumes exceed established thresholds, a capacity planning review is instituted which will address the need for additions well in advance of their actual need.

#### SRS diagram and interconnectivity description

As with all core registry services, the SRS is run from a global cluster of registry system data centers, located in geographic centers with high Internet bandwidth, power, redundancy and availability. All of the registry systems will be run in a  $\langle n+1 \rangle$  setup, with a primary data center and a secondary data center. For detailed site information, please see our responses to questions #32 and #35. Registrars access the SRS in real-time using EPP.

A sample of the Afilias SRS technical and operational capabilities (displayed in Figure 24-a) include:

- Geographically diverse redundant registry systems;
- Load balancing implemented for all registry services (e.g. EPP, WHOIS, web admin) ensuring equal experience for all customers and easy horizontal scalability;
- Disaster Recovery Point objective for the registry is within one minute of the loss of the primary system;
- Detailed and tested contingency plan, in case of primary site failure, and;
- Daily reports, with secure access for confidentiality protection.

As evidenced in Figure 24-a, the SRS contains several components of the registry system. The interconnectivity ensures near-real-time distribution of the data throughout the registry infrastructure, timely backups, and up-to-date billing information.

The WHOIS servers are directly connected to the registry database and provide real-time responses to queries using the most up-to-date information present in the registry.

Committed DNS-related EPP objects in the database are made available to the DNS Distributor via a dedicated set of connections. The DNS Distributor extracts committed DNS-related EPP objects in real time and immediately inserts them into the zone for dissemination.

The Afilias system is architected such that read-only database connections are executed on database replicas and connections to the database master (where write-access is executed) are carefully protected to ensure high availability.

This interconnectivity is monitored, as is the entire registry system, according to the plans detailed in our response to question #42.

#### Synchronization scheme

Registry databases are synchronized both within the same data center and in the backup data center using a database application called Slony. For further details, please see the responses to questions #33 and #37. Slony replication of transactions from the publisher (master) database to its subscribers (replicas) works continuously to ensure the publisher and its subscribers remain synchronized. When the publisher database completes a transaction the Slony replication system ensures that each replica also processes the transaction. When there are no transactions to process, Slony "sleeps" until a transaction arrives or for one minute, whichever comes first. Slony "wakes up" each minute to confirm with the publisher that there has not been a transaction and thus ensures subscribers are synchronized and the replication time lag is minimized. The typical replication time lag between the publisher and subscribers depends on the topology of the replication cluster, specifically the location of the subscribers relative to the publisher. Subscribers located in the same data center as the publisher are typically updated within a couple of seconds, and subscribers located in a secondary data center are typically updated in less than ten seconds. This ensures real-time or near-real-time synchronization between all databases, and in the case where the secondary data center needs to be activated, it can be done with minimal disruption to registrars.

#### SRS SLA performance compliance

Afilias has a ten-year record of delivering on the demanding ICANN SLAs, and will continue to provide secure, stable and reliable service in compliance with SLA requirements as specified in the new gTLD Registry Agreement, Specification 10, as presented in Figure 24-b.

The Afilias SRS currently handles over 200 million EPP transactions per month for just .INFO and .ORG. Overall, the Afilias SRS manages over 700 million EPP transactions per month for all TLDs under management.

Given this robust functionality, and more than a decade of experience supporting a thick TLD registry with a strong performance history, Afilias, on behalf of Schlund Technologies GmbH, will meet or exceed the performance metrics in Specification 10 of the new gTLD Registry Agreement. The Afilias services and infrastructure are designed to scale both vertically and horizontally without any downtime to provide consistent performance as this TLD grows. The Afilias architecture is also massively provisioned to meet seasonal demands and marketing campaigns. Afilias' experience also gives high confidence in the ability to scale and grow registry operations for this TLD in a secure, stable and reliable manner.

#### SRS resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Over 100 Afiliias team members contribute to the management of the SRS code and network that will support this TLD. The SRS team is composed of Software Engineers, Quality Assurance Analysts, Application Administrators, System Administrators, Storage Administrators, Network Administrators, Database Administrators, and Security Analysts located at three geographically separate Afiliias facilities. The systems and services set up and administered by these team members are monitored 24x7 by skilled analysts at two NOCs located in Toronto, Ontario (Canada) and Horsham, Pennsylvania (USA). In addition to these team members, Afiliias also utilizes trained project management staff to maintain various calendars, work breakdown schedules, utilization and resource schedules and other tools to support the technical and management staff. It is this team who will both deploy this TLD on the Afiliias infrastructure, and maintain it. Together, the Afiliias team has managed 11 registry transitions and six new TLD launches, which illustrate its ability to securely and reliably deliver regularly scheduled updates as well as a secure, stable and reliable SRS service for this TLD.

## 25. Extensible Provisioning Protocol (EPP)

Answers for this question (#25) are provided by Afiliias, the back-end provider of registry services for this TLD.

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE " <" and "> " CHARACTERS), WHICH ICANN INFORMS AFILIIAS (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE.

Afiliias has been a pioneer and innovator in the use of EPP. .INFO was the first EPP-based gTLD registry and launched on EPP version 02/00. Afiliias has a track record of supporting TLDs on standards-compliant versions of EPP. Afiliias will operate the EPP registrar interface as well as a web-based interface for this TLD in accordance with RFCs and global best practices. In addition, Afiliias will maintain a proper OT&E (Operational Testing and Evaluation) environment to facilitate registrar system development and testing.

Afiliias' EPP technical performance meets or exceeds all ICANN requirements as demonstrated by:

- A completely functional, state-of-the-art, EPP-based SRS that currently meets the needs of various gTLDs and will meet this new TLD's needs;
- A track record of success in developing extensions to meet client and registrar business requirements such as multi-script support for IDNs;
- Supporting six ICANN gTLDs on EPP: .INFO, .ORG, .MOBI, .AERO, .ASIA and .XXX
- EPP software that is operating today and has been fully tested to be standards-compliant;
- Proven interoperability of existing EPP software with ICANN-accredited registrars, and;
- An SRS that currently processes over 200 million EPP transactions per month for both .INFO and .ORG. Overall, Afiliias processes over 700 million EPP transactions per month for all 16 TLDs under management.

The EPP service is offered in accordance with the performance specifications defined in the new gTLD Registry Agreement, Specification 10.

### EPP Standards

The Afiliias registry system complies with the following revised versions of the RFCs and operates multiple ICANN TLDs on these standards, including .INFO, .ORG, .MOBI, .ASIA and .XXX. The systems have been tested by our Quality Assurance ("QA") team for RFC compliance, and have been used by registrars for an extended period of time:

- 3735 - Guidelines for Extending EPP
- 3915 - Domain Registry Grace Period Mapping
- 5730 - Extensible Provisioning Protocol (EPP)
- 5731 - Domain Name Mapping
- 5732 - Host Mapping
- 5733 - Contact Mapping
- 5734 - Transport Over TCP
- 5910 - Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)

This TLD will support all valid EPP commands. The following EPP commands are in operation today and will be made available for this TLD. See attachment #25a for the base set of EPP commands and copies of Afiliias XSD schema files, which define all the rules of valid, RFC compliant EPP commands and responses that Afiliias supports. Any customized EPP extensions, if necessary, will also conform to relevant RFCs.

Afiliias staff members actively participated in the Internet Engineering Task Force (IETF) process that finalized the new standards for EPP. Afiliias will continue to actively participate in the IETF and will stay abreast of any updates to the EPP standards.

#### EPP software interface and functionality

Afiliias will provide all registrars with a free open-source EPP toolkit. Afiliias provides this software for use with both Microsoft Windows and Unix/Linux operating systems. This software, which includes all relevant templates and schema defined in the RFCs, is available on sourceforge.net and will be available through the registry operator's website.

Afiliias' SRS EPP software complies with all relevant RFCs and includes the following functionality:

- EPP Greeting: A response to a successful connection returns a greeting to the client. Information exchanged can include: name of server, server date and time in UTC, server features, e.g., protocol versions supported, languages for the text response supported, and one or more elements which identify the objects that the server is capable of managing;
- Session management controls: <login> to establish a connection with a server, and <logout> to end a session;
- EPP Objects: Domain, Host and Contact for respective mapping functions;
- EPP Object Query Commands: Info, Check, and Transfer (query) commands to retrieve object information, and;
- EPP Object Transform Commands: five commands to transform objects: <create> to create an instance of an object, <delete> to remove an instance of an object, <renew> to extend the validity period of an object, <update> to change information associated with an object, and <transfer> to manage changes in client sponsorship of a known object.

Currently, 100% of the top domain name registrars in the world have software that has already been tested and certified to be compatible with the Afiliias SRS registry. In total, over 375 registrars, representing over 95% of all registration volume worldwide, operate software that has been certified compatible with the Afiliias SRS registry. Afiliias' EPP Registrar Acceptance Criteria are available in attachment #25b, EPP OT&E Criteria.

#### Free EPP software support

Afiliias analyzes and diagnoses registrar EPP activity log files as needed and is available to assist registrars who may require technical guidance regarding how to fix repetitive errors or exceptions caused by misconfigured client software.

Registrars are responsible for acquiring a TLS/SSL certificate from an approved certificate authority, as the registry-registrar communication channel requires

mutual authentication; Afiliias will acquire and maintain the server-side TLS/SSL certificate. The registrar is responsible for developing support for TLS/SSL in their client application. Afiliias will provide free guidance for registrars unfamiliar with this requirement.

#### Registrar data synchronization

There are two methods available for registrars to synchronize their data with the registry:

- Automated synchronization: Registrars can, at any time, use the EPP `<info>` command to obtain definitive data from the registry for a known object, including domains, hosts (nameservers) and contacts.
- Personalized synchronization: A registrar may contact technical support and request a data file containing all domains (and associated host (nameserver) and contact information) registered by that registrar, within a specified time interval. The data will be formatted as a comma separated values (CSV) file and made available for download using a secure server.

#### EPP modifications

There are no unique EPP modifications planned for this TLD.

All ICANN TLDs must offer a Sunrise as part of a rights protection program. Afiliias uses EPP extensions that allow registrars to submit trademark and other intellectual property rights (IPR) data to the registry. These extensions are:

- An `<ipr:name>` element that indicates the name of Registered Mark.
- An `<ipr:number>` element that indicates the registration number of the IPR.
- An `<ipr:ccLocality>` element that indicates the origin for which the IPR is established (a national or international trademark registry).
- An `<ipr:entitlement>` element that indicates whether the applicant holds the trademark as the original "OWNER", "CO-OWNER" or "ASSIGNEE".
- An `<ipr:appDate>` element that indicates the date the Registered Mark was applied for.
- An `<ipr:regDate>` element that indicates the date the Registered Mark was issued and registered.
- An `<ipr:class>` element that indicates the class of the registered mark.
- An `<ipr:type>` element that indicates the Sunrise phase the application applies for.

Note that some of these extensions might be subject to change based on ICANN-developed requirements for the Trademark Clearinghouse.

#### EPP resourcing plans

Since its founding, Afiliias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afiliias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afiliias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afiliias project management methodology allows efficient and effective use of our staff in a focused way.

108 Afiliias team members directly contribute to the management and development of the EPP based registry systems. As previously noted, Afiliias is an active member of IETF and has a long documented history developing and enhancing EPP. These contributors include 11 developers and 14 QA engineers focused on maintaining and enhancing EPP server side software. These engineers work directly with business staff to timely address existing needs and forecast



registry/registrar needs to ensure the Afiliias EPP software is effective today and into the future. A team of eight data analysts work with the EPP software system to ensure that the data flowing through EPP is securely and reliably stored in replicated database systems. In addition to the EPP developers, QA engineers, and data analysts, other EPP contributors at Afiliias include: Technical Analysts, the Network Operations Center and Data Services team members.

## 26. Whois

Answers for this question (#26) are provided by Afiliias, the back-end provider of registry services for this TLD.

Afiliias operates the WHOIS (registration data directory service) infrastructure in accordance with RFCs and global best practices, as it does for the 16 TLDs it currently supports. Designed to be robust and scalable, Afiliias' WHOIS service has exceeded all contractual requirements for over a decade. It has extended search capabilities, and methods of limiting abuse.

The WHOIS service operated by Afiliias meets and exceeds ICANN's requirements. Specifically, Afiliias will:

- Offer a WHOIS service made available on port 43 that is flexible and standards-compliant;
- Comply with all ICANN policies, and meeting or exceeding WHOIS performance requirements in Specification 10 of the new gTLD Registry Agreement;
- Enable a Searchable WHOIS with extensive search capabilities that offers ease of use while enforcing measures to mitigate access abuse, and;
- Employ a team with significant experience managing a compliant WHOIS service.

Such extensive knowledge and experience managing a WHOIS service enables Afiliias to offer a comprehensive plan for this TLD that meets the needs of constituents of the domain name industry and Internet users. The service has been tested by our QA team for RFC compliance, and has been used by registrars and many other parties for an extended period of time. Afiliias' WHOIS service currently serves almost 500 million WHOIS queries per month, with the capacity already built in to handle an order of magnitude increase in WHOIS queries, and the ability to smoothly scale should greater growth be needed.

### WHOIS system description and diagram

The Afiliias WHOIS system, depicted in figure 26-a, is designed with robustness, availability, compliance, and performance in mind. Additionally, the system has provisions for detecting abusive usage (e.g., excessive numbers of queries from one source). The WHOIS system is generally intended as a publicly available single object lookup system. Afiliias uses an advanced, persistent caching system to ensure extremely fast query response times.

Afiliias will develop restricted WHOIS functions based on specific domain policy and regulatory requirements as needed for operating the business (as long as they are standards compliant). It will also be possible for contact and registrant information to be returned according to regulatory requirements. The WHOIS database supports multiple string and field searching through a reliable, free, secure web-based interface.

#### Data objects, interfaces, access and lookups

Registrars can provide an input form on their public websites through which a visitor is able to perform WHOIS queries. The registry operator can also provide a Web-based search on its site. The input form must accept the string to query, along with the necessary input elements to select the object type and interpretation controls. This input form sends its data to the Afiliias port 43

WHOIS server. The results from the WHOIS query are returned by the server and displayed in the visitor's Web browser. The sole purpose of the Web interface is to provide a user-friendly interface for WHOIS queries.

Afilias will provide WHOIS output as per Specification 4 of the new gTLD Registry Agreement. The output for domain records generally consists of the following elements:

- The name of the domain registered and the sponsoring registrar;
- The names of the primary and secondary nameserver(s) for the registered domain name;
- The creation date, registration status and expiration date of the registration;
- The name, postal address, e-mail address, and telephone and fax numbers of the domain name holder;
- The name, postal address, e-mail address, and telephone and fax numbers of the technical contact for the domain name holder;
- The name, postal address, e-mail address, and telephone and fax numbers of the administrative contact for the domain name holder, and;
- The name, postal address, e-mail address, and telephone and fax numbers of the billing contact for the domain name holder.

The following additional features are also present in Afilias' WHOIS service:

- Support for IDNs, including the language tag and the Punycode representation of the IDN in addition to Unicode Hex and Unicode HTML formats;
- Enhanced support for privacy protection relative to the display of confidential information.

Afilias will also provide sophisticated WHOIS search functionality that includes the ability to conduct multiple string and field searches.

#### Query controls

For all WHOIS queries, a user is required to enter the character string representing the information for which they want to search. The object type and interpretation control parameters to limit the search may also be specified. If object type or interpretation control parameter is not specified, WHOIS will search for the character string in the Name field of the Domain object.

WHOIS queries are required to be either an "exact search" or a "partial search," both of which are insensitive to the case of the input string.

An exact search specifies the full string to search for in the database field. An exact match between the input string and the field value is required.

A partial search specifies the start of the string to search for in the database field. Every record with a search field that starts with the input string is considered a match. By default, if multiple matches are found for a query, then a summary containing up to 50 matching results is presented. A second query is required to retrieve the specific details of one of the matching records.

If only a single match is found, then full details will be provided. Full detail consists of the data in the matching object as well as the data in any associated objects. For example: a query that results in a domain object includes the data from the associated host and contact objects.

WHOIS query controls fall into two categories: those that specify the type of field, and those that modify the interpretation of the input or determine the level of output to provide. Each is described below.

The following keywords restrict a search to a specific object type:

- **Domain:** Searches only domain objects. The input string is searched in the Name field.
- **Host:** Searches only nameserver objects. The input string is searched in the Name field and the IP Address field.
- **Contact:** Searches only contact objects. The input string is searched in the

ID field.

- Registrar: Searches only registrar objects. The input string is searched in the Name field.

By default, if no object type control is specified, then the Name field of the Domain object is searched.

In addition, Afiliias WHOIS systems can perform and respond to WHOIS searches by registrant name, postal address and contact names. Deployment of these features is provided as an option to the registry operator, based upon registry policy and business decision making.

Figure 26-b presents the keywords that modify the interpretation of the input or determine the level of output to provide.

By default, if no interpretation control keywords are used, the output will include full details if a single match is found and a summary if multiple matches are found.

#### Unique TLD requirements

There are no unique WHOIS requirements for this TLD.

#### Sunrise WHOIS processes

All ICANN TLDs must offer a Sunrise as part of a rights protection program. Afiliias uses EPP extensions that allow registrars to submit trademark and other intellectual property rights (IPR) data to the registry. The following corresponding data will be displayed in WHOIS for relevant domains:

- Trademark Name: element that indicates the name of the Registered Mark.
- Trademark Number: element that indicates the registration number of the IPR.
- Trademark Locality: element that indicates the origin for which the IPR is established (a national or international trademark registry).
- Trademark Entitlement: element that indicates whether the applicant holds the trademark as the original "OWNER", "CO-OWNER" or "ASSIGNEE".
- Trademark Application Date: element that indicates the date the Registered Mark was applied for.
- Trademark Registration Date: element that indicates the date the Registered Mark was issued and registered.
- Trademark Class: element that indicates the class of the Registered Mark.
- IPR Type: element that indicates the Sunrise phase the application applies for.

#### IT and infrastructure resources

All the applications and databases for this TLD will run in a virtual environment hosted by a cluster of servers equipped with the latest Intel Westmere multi-core processors (or a more advanced, stable technology available at the time of deployment). The registry data will be stored on storage arrays of solid-state drives shared over a fast storage area network. The virtual environment allows the infrastructure to easily scale both vertically and horizontally to cater to changing demand. It also facilitates effective utilization of system resources thus reducing energy consumption and carbon footprint.

The applications and servers are supported by network firewalls, routers and switches.

The WHOIS system accommodates both IPv4 and IPv6 addresses.

Each of the servers and network devices are equipped with redundant hot-swappable components and multiple connections to ancillary systems. Additionally, 24x7 support agreements with our hardware vendor with a 4-hour response time at all our data centers guarantees replacement of failed parts in the shortest time possible.

Models of system and network devices used are:

- Servers: Cisco UCS B230 blade servers
- SAN storage arrays: IBM Storwize V7000 with Solid State Drives

- Firewalls: Cisco ASA 5585-X
- Load balancers: F5 Big-IP 6900
- Traffic shapers: Procera PacketLogic PL8720
- Routers: Juniper MX40 3D
- Network switches: Cisco Nexus 7010, Nexus 5548, Nexus 2232

There will be at least four virtual machines (VMs) offering WHOIS service. Each VM will run at least two WHOIS server instances - one for registrars and one for the public. All instances of the WHOIS service is made available to registrars and the public are rate limited to mitigate abusive behavior.

Frequency of synchronization between servers

Registration data records from the EPP publisher database will be replicated to the WHOIS system database on a near-real-time basis whenever an update occurs.

Specifications 4 and 10 compliance

The WHOIS service for this TLD will meet or exceed the performance requirements in the new gTLD Registry Agreement, Specification 10. Figure 26-c provides the exact measurements and commitments. Afilias has a 10 year track record of exceeding WHOIS performance and a skilled team to ensure this continues for all TLDs under management.

The WHOIS service for this TLD will meet or exceed the requirements in the new gTLD Registry Agreement, Specification 4.

RFC 3912 compliance

Afilias will operate the WHOIS infrastructure in compliance with RFCs and global best practices, as it does with the 16 TLDs Afilias currently supports.

Afilias maintains a registry-level centralized WHOIS database that contains information for every registered domain and for all host and contact objects. The WHOIS service will be available on the Internet standard WHOIS port (port 43) in compliance with RFC 3912. The WHOIS service contains data submitted by registrars during the registration process. Changes made to the data by a registrant are submitted to Afilias by the registrar and are reflected in the WHOIS database and service in near-real-time, by the instance running at the primary data center, and in under ten seconds by the instance running at the secondary data center, thus providing all interested parties with up-to-date information for every domain. This service is compliant with the new gTLD Registry Agreement, Specification 4.

The WHOIS service maintained by Afilias will be authoritative and complete, as this will be a "thick" registry (detailed domain contact WHOIS is all held at the registry); users do not have to query different registrars for WHOIS information, as there is one central WHOIS system. Additionally, visibility of different types of data is configurable to meet the registry operator's needs.

Searchable WHOIS

Afilias offers a searchable WHOIS on a web-based Directory Service. Partial match capabilities are offered on the following fields: domain name, registrar ID, and IP address. In addition, Afilias WHOIS systems can perform and respond to WHOIS searches by registrant name, postal address and contact names.

Providing the ability to search important and high-value fields such as registrant name, address and contact names increases the probability of abusive behavior. An abusive user could script a set of queries to the WHOIS service and access contact data in order to create or sell a list of names and addresses of registrants in this TLD. Making the WHOIS machine readable, while

preventing harvesting and mining of WHOIS data, is a key requirement integrated into the Afiliias WHOIS systems. For instance, Afiliias limits search returns to 50 records at a time. If bulk queries were ever necessary (e.g., to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process), Afiliias makes such query responses available to carefully screened and limited staff members at the registry operator (and customer support staff) via an internal data warehouse. The Afiliias WHOIS system accommodates anonymous access as well as pre-identified and profile-defined uses, with full audit and log capabilities.

The WHOIS service has the ability to tag query responses with labels such as "Do not redistribute" or "Special access granted". This may allow for tiered response and reply scenarios. Further, the WHOIS service is configurable in parameters and fields returned, which allow for flexibility in compliance with various jurisdictions, regulations or laws.

Afiliias offers exact-match capabilities on the following fields: registrar ID, nameserver name, and nameserver's IP address (only applies to IP addresses stored by the registry, i.e., glue records). Search capabilities are fully available, and results include domain names matching the search criteria (including IDN variants). Afiliias manages abuse prevention through rate limiting and CAPTCHA (described below). Queries do not require specialized transformations of internationalized domain names or internationalized data fields

Please see "Query Controls" above for details about search options and capabilities.

#### Deterring WHOIS abuse

Afiliias has adopted two best practices to prevent abuse of the WHOIS service: rate limiting and CAPTCHA.

Abuse of WHOIS services on port 43 and via the Web is subject to an automated rate-limiting system. This ensures that uniformity of service to users is unaffected by a few parties whose activities abuse or otherwise might threaten to overload the WHOIS system.

Abuse of web-based public WHOIS services is subject to the use of CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) technology. The use of CAPTCHA ensures that uniformity of service to users is unaffected by a few parties whose activities abuse or otherwise might threaten to overload the WHOIS system. The registry operator will adopt a CAPTCHA on its Web-based WHOIS.

Data mining of any sort on the WHOIS system is strictly prohibited, and this prohibition is published in WHOIS output and in terms of service.

For rate limiting on IPv4, there are configurable limits per IP and subnet. For IPv6, the traditional limitations do not apply. Whenever a unique IPv6 IP address exceeds the limit of WHOIS queries per minute, the same rate-limit for the given 64 bits of network prefix that the offending IPv6 IP address falls into will be applied. At the same time, a timer will start and rate-limit validation logic will identify if there are any other IPv6 address within the original 80-bit (<48) prefix. If another offending IPv6 address does fall into the <48 prefix then rate-limit validation logic will penalize any other IPv6 addresses that fall into that given 80-bit (<48) network. As a security precaution, Afiliias will not disclose these limits.

Pre-identified and profile-driven role access allows greater granularity and configurability in both access to the WHOIS service, and in volume/frequency of responses returned for queries.

Afilias staff are key participants in the ICANN Security & Stability Advisory Committee's deliberations and outputs on WHOIS, including SAC003, SAC027, SAC033, SAC037, SAC040, and SAC051. Afilias staff are active participants in both technical and policy decision making in ICANN, aimed at restricting abusive behavior.

#### WHOIS staff resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Within Afilias, there are 11 staff members who develop and maintain the compliant WHOIS systems. They keep pace with access requirements, thwart abuse, and continually develop software. Of these resources, approximately two staffers are typically required for WHOIS-related code customization. Other resources provide quality assurance, and operations personnel maintain the WHOIS system itself. This team will be responsible for the implementation and on-going maintenance of the new TLD WHOIS service.

## 27. Registration Life Cycle

Answers for this question (#27) are provided by Afilias, the back-end provider of registry services for this TLD.

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE " <" and "> " CHARACTERS), WHICH ICANN INFORMS AFILIAS (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE.

Afilias has had experience managing registrations for over a decade and supports comprehensive registration lifecycle services including the registration states, all standard grace periods, and can address any modifications required with the introduction of any new ICANN policies.

This TLD will follow the ICANN standard domain lifecycle, as is currently implemented in TLDs such as .ORG and .INFO. The below response includes: a diagram and description of the lifecycle of a domain name in this TLD, including domain creation, transfer protocols, grace period implementation and the respective time frames for each; and the existing resources to support the complete lifecycle of a domain.

As depicted in Figure 27-a, prior to the beginning of the Trademark Claims Service or Sunrise IP protection program, Afilias will support the reservation of names in accordance with the new gTLD Registry Agreement, Specification 5.

#### Registration period

After the IP protection programs and the general launch, eligible registrants may choose an accredited registrar to register a domain name. The registrar will check availability on the requested domain name and if available, will collect specific objects such as, the required contact and host information

from the registrant. The registrar will then provision the information into the registry system using standard Extensible Provisioning Protocol ("EPP") commands through a secure connection to the registry backend service provider.

When the domain is created, the standard five day Add Grace Period begins, the domain and contact information are available in WHOIS, and normal operating EPP domain statuses will apply. Other specifics regarding registration rules for an active domain include:

- The domain must be unique;
- Restricted or reserved domains cannot be registered;
- The domain can be registered from 1-10 years;
- The domain can be renewed at any time for 1-10 years, but cannot exceed 10 years;
- The domain can be explicitly deleted at any time;
- The domain can be transferred from one registrar to another except during the first 60 days following a successful registration or within 60 days following a transfer; and,

Contacts and hosts can be modified at any time.

The following describe the domain status values recognized in WHOIS when using the EPP protocol following RFC 5731.

- OK or Active: This is the normal status for a domain that has no pending operations or restrictions.
- Inactive: The domain has no delegated name servers.
- Locked: No action can be taken on the domain. The domain cannot be renewed, transferred, updated, or deleted. No objects such as contacts or hosts can be associated to, or disassociated from the domain. This status includes: Delete Prohibited / Server Delete Prohibited, Update Prohibited / Server Update Prohibited, Transfer Prohibited, Server Transfer Prohibited, Renew Prohibited, Server Renew Prohibited.
- Hold: The domain will not be included in the zone. This status includes: Client Hold, Server Hold.
- Transfer Prohibited: The domain cannot be transferred away from the sponsoring registrar. This status includes: Client Transfer Prohibited, Server Transfer Prohibited.

The following describe the registration operations that apply to the domain name during the registration period.

a. Domain modifications: This operation allows for modifications or updates to the domain attributes to include:

- i. Registrant Contact
- ii. Admin Contact
- iii. Technical Contact
- iv. Billing Contact
- v. Host or nameservers
- vi. Authorization information
- vii. Associated status values

A domain with the EPP status of Client Update Prohibited or Server Update Prohibited may not be modified until the status is removed.

b. Domain renewals: This operation extends the registration period of a domain by changing the expiration date. The following rules apply:

- i. A domain can be renewed at any time during its registration term,
- ii. The registration term cannot exceed a total of 10 years.

A domain with the EPP status of Client Renew Prohibited or Server Renew Prohibited cannot be renewed.

c. Domain deletions: This operation deletes the domain from the Shared Registry Services (SRS). The following rules apply:

- i. A domain can be deleted at any time during its registration term, if the domain is deleted during the Add Grace Period or the Renew/Extend Grace Period,

the sponsoring registrar will receive a credit,

ii. A domain cannot be deleted if it has "child" nameservers that are associated to other domains.

A domain with the EPP status of Client Delete Prohibited or Server Delete Prohibited cannot be deleted.

d. Domain transfers: A transfer of the domain from one registrar to another is conducted by following the steps below.

i. The registrant must obtain the applicable <authInfo> code from the sponsoring (losing) registrar.

- Every domain name has an authInfo code as per EPP RFC 5731. The authInfo code is a six- to 16-character code assigned by the registrar at the time the name was created. Its purpose is to aid identification of the domain owner so proper authority can be established (it is the "password" to the domain).

- Under the Registry-Registrar Agreement, registrars will be required to provide a copy of the authInfo code to the domain registrant upon his or her request.

ii. The registrant must provide the authInfo code to the new (gaining) registrar, who will then initiate a domain transfer request. A transfer cannot be initiated without the authInfo code.

- Every EPP <transfer> command must contain the authInfo code or the request will fail. The authInfo code represents authority to the registry to initiate a transfer.

iii. Upon receipt of a valid transfer request, the registry automatically asks the sponsoring (losing) registrar to approve the request within five calendar days.

- When a registry receives a transfer request the domain cannot be modified, renewed or deleted until the request has been processed. This status must not be combined with either Client Transfer Prohibited or Server Transfer Prohibited status.

- If the sponsoring (losing) registrar rejects the transfer within five days, the transfer request is cancelled. A new domain transfer request will be required to reinitiate the process.

- If the sponsoring (losing) registrar does not approve or reject the transfer within five days, the registry automatically approves the request.

iv. After a successful transfer, it is strongly recommended that registrars change the authInfo code, so that the prior registrar or registrant cannot use it anymore.

v. Registrars must retain all transaction identifiers and codes associated with successful domain object transfers and protect them from disclosure.

vi. Once a domain is successfully transferred the status of TRANSFERPERIOD is added to the domain for a period of five days.

vii. Successful transfers will result in a one year term extension (resulting in a maximum total of 10 years), which will be charged to the gaining registrar.

e. Bulk transfer: Afilias, supports bulk transfer functionality within the SRS for situations where ICANN may request the registry to perform a transfer of some or all registered objects (includes domain, contact and host objects) from one registrar to another registrar. Once a bulk transfer has been executed, expiry dates for all domain objects remain the same, and all relevant states of each object type are preserved. In some cases the gaining and the losing registrar as well as the registry must approved bulk transfers. A detailed log is captured for each bulk transfer process and is archived for audit purposes.

Schlund Technologies GmbH will support ICANN's Transfer Dispute Resolution Process. Schlund Technologies GmbH will work with Afilias to respond to Requests for Enforcement (law enforcement or court orders) and will follow that process.

1. Auto-renew grace period

The Auto-Renew Grace Period displays as AUTORENEWPERIOD in WHOIS. An auto-renew must be requested by the registrant through the sponsoring registrar and occurs



if a domain name registration is not explicitly renewed or deleted by the expiration date and is set to a maximum of 45 calendar days. In this circumstance the registration will be automatically renewed by the registry system the first day after the expiration date. If a Delete, Extend, or Transfer occurs within the AUTORENEWPERIOD the following rules apply:

- i. Delete. If a domain is deleted the sponsoring registrar at the time of the deletion receives a credit for the auto-renew fee. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.
- ii. Renew/Extend. A domain can be renewed as long as the total term does not exceed 10 years. The account of the sponsoring registrar at the time of the extension will be charged for the additional number of years the registration is renewed.
- iii. Transfer (other than ICANN-approved bulk transfer). If a domain is transferred, the losing registrar is credited for the auto-renew fee, and the year added by the operation is cancelled. As a result of the transfer, the expiration date of the domain is extended by minimum of one year as long as the total term does not exceed 10 years. The gaining registrar is charged for the additional transfer year(s) even in cases where a full year is not added because of the maximum 10 year registration restriction.

## 2. Redemption grace period

During this period, a domain name is placed in the PENDING DELETE RESTORABLE status when a registrar requests the deletion of a domain that is not within the Add Grace Period. A domain can remain in this state for up to 30 days and will not be included in the zone file. The only action a registrar can take on a domain is to request that it be restored. Any other registrar requests to modify or otherwise update the domain will be rejected. If the domain is restored it moves into PENDING RESTORE and then OK. After 30 days if the domain is not restored it moves into PENDING DELETE SCHEDULED FOR RELEASE before the domain is released back into the pool of available domains.

## 3. Pending delete

During this period, a domain name is placed in PENDING DELETE SCHEDULED FOR RELEASE status for five days, and all Internet services associated with the domain will remain disabled and domain cannot be restored. After five days the domain is released back into the pool of available domains.

## Other grace periods

All ICANN required grace periods will be implemented in the registry backend service provider's system including the Add Grace Period (AGP), Renew/Extend Grace Period (EGP), Transfer Grace Period (TGP), Auto-Renew Grace Period (ARGP), and Redemption Grace Period (RGP). The lengths of grace periods are configurable in the registry system. At this time, the grace periods will be implemented following other gTLDs such as .ORG. More than one of these grace periods may be in effect at any one time. The following are accompanying grace periods to the registration lifecycle.

## Add grace period

The Add Grace Period displays as ADDPERIOD in WHOIS and is set to five calendar days following the initial registration of a domain. If the domain is deleted by the registrar during this period, the registry provides a credit to the registrar for the cost of the registration. If a Delete, Renew/Extend, or Transfer operation occurs within the five calendar days, the following rules apply.

- i. Delete. If a domain is deleted within this period the sponsoring registrar at the time of the deletion is credited for the amount of the registration. The domain is deleted from the registry backend service provider's database and is released back into the pool of available domains.
- ii. Renew/Extend. If the domain is renewed within this period and then deleted, the sponsoring registrar will receive a credit for both the registration and the extended amounts. The account of the sponsoring registrar at the time of

the renewal will be charged for the initial registration plus the number of years the registration is extended. The expiration date of the domain registration is extended by that number of years as long as the total term does not exceed 10 years.

iii. Transfer (other than ICANN-approved bulk transfer). Transfers under Part A of the ICANN Policy on Transfer of Registrations between registrars may not occur during the ADDPERIOD or at any other time within the first 60 days after the initial registration. Enforcement is the responsibility of the registrar sponsoring the domain name registration and is enforced by the SRS.

#### Renew / extend grace period

The Renew / Extend Grace Period displays as RENEWPERIOD in WHOIS and is set to five calendar days following an explicit renewal on the domain by the registrar. If a Delete, Extend, or Transfer occurs within the five calendar days, the following rules apply:

i. Delete. If a domain is deleted within this period the sponsoring registrar at the time of the deletion receives a credit for the renewal fee. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.

ii. Renew/Extend. A domain registration can be renewed within this period as long as the total term does not exceed 10 years. The account of the sponsoring registrar at the time of the extension will be charged for the additional number of years the registration is renewed.

iii. Transfer (other than ICANN-approved bulk transfer). If a domain is transferred within the Renew/Extend Grace Period, there is no credit to the losing registrar for the renewal fee. As a result of the transfer, the expiration date of the domain registration is extended by a minimum of one year as long as the total term for the domain does not exceed 10 years.

If a domain is auto-renewed, then extended, and then deleted within the Renew/Extend Grace Period, the registrar will be credited for any auto-renew fee charged and the number of years for the extension. The years that were added to the domain's expiration as a result of the auto-renewal and extension are removed. The deleted domain is moved to the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.

#### Transfer Grace Period

The Transfer Grace period displays as TRANSFERPERIOD in WHOIS and is set to five calendar days after the successful transfer of domain name registration from one registrar to another registrar. Transfers under Part A of the ICANN Policy on Transfer of Registrations between registrars may not occur during the TRANSFERPERIOD or within the first 60 days after the transfer. If a Delete or Renew/Extend occurs within that five calendar days, the following rules apply:

i. Delete. If the domain is deleted by the new sponsoring registrar during this period, the registry provides a credit to the registrar for the cost of the transfer. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.

ii. Renew/Extend. If a domain registration is renewed within the Transfer Grace Period, there is no credit for the transfer. The registrar's account will be charged for the number of years the registration is renewed. The expiration date of the domain registration is extended by the renewal years as long as the total term does not exceed 10 years.

#### Auction

This TLD will conduct an auction for certain domain names. Afilias will manage the domain name auction using existing technology. Upon the completion of the auction, any domain name acquired will then follow the standard lifecycle of a domain.

#### Registration lifecycle resources

Since its founding, Afiliias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afiliias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afiliias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afiliias project management methodology allows efficient and effective use of our staff in a focused way. Virtually all Afiliias resource are involved in the registration lifecycle of domains.

There are a few areas where registry staff devote resources to registration lifecycle issues:

- a. Supporting Registrar Transfer Disputes. The registry operator will have a compliance staffer handle these disputes as they arise; they are very rare in the existing gTLDs.
- b. Afiliias has its development and quality assurance departments on hand to modify the grace period functionality as needed, if ICANN issues new Consensus Policies or the RFCs change.

Afiliias has more than 30 staff members in these departments.

## 28. Abuse Prevention and Mitigation

Schlund Technologies GmbH, working with Afiliias, will take the requisite operational and technical steps to promote WHOIS data accuracy, limit domain abuse, remove outdated and inaccurate data, and other security measures to ensure the integrity of the TLD. The specific measures include, but are not limited to:

- Posting a TLD Anti-Abuse Policy that clearly defines abuse, and provide point-of-contact information for reporting suspected abuse;
- Committing to rapid identification and resolution of abuse, including suspensions;
- Ensuring completeness of WHOIS information at the time of registration;
- Publishing and maintaining procedures for removing orphan glue records for names removed from the zone, and;
- Establishing measures to deter WHOIS abuse, including rate-limiting, determining data syntax validity, and implementing and enforcing requirements from the Registry-Registrar Agreement.

### Abuse policy

The Anti-Abuse Policy stated below will be enacted under the contractual authority of the registry operator through the Registry-Registrar Agreement, and the obligations will be passed on to and made binding upon registrants. This policy will be posted on the TLD web site along with contact information for registrants or users to report suspected abuse.

The policy is designed to address the malicious use of domain names. The registry operator and its registrars will make reasonable attempts to limit significant harm to Internet users. This policy is not intended to take the place of the Uniform Domain Name Dispute Resolution Policy (UDRP) or the Uniform Rapid Suspension System (URS), and it is not to be used as an alternate form of dispute resolution or as a brand protection mechanism. Its intent is not to burden law-abiding or innocent registrants and domain users; rather, the intent is to deter those who use domain names maliciously by engaging in illegal or fraudulent activity.

Repeat violations of the abuse policy will result in a case-by-case review of the abuser(s), and the registry operator reserves the right to escalate the issue, with the intent of levying sanctions that are allowed under the TLD anti-abuse policy.

The below policy is a recent version of the policy that has been used by the .INFO registry since 2008, and the .ORG registry since 2009. It has proven to be an effective and flexible tool.

#### .WEB Anti-Abuse Policy

The following Anti-Abuse Policy is effective upon launch of the TLD. Malicious use of domain names will not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars, and registrants, as well as for users of the Internet in general. The registry operator definition of abusive use of a domain includes, without limitation, the following:

- Illegal or fraudulent actions;
- Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of web sites and Internet forums;
- Phishing: The use of counterfeit web pages that are designed to trick recipients into divulging sensitive data such as personally identifying information, usernames, passwords, or financial data;
- Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or poisoning;
- Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and Trojan horses.
- Malicious fast-flux hosting: Use of fast-flux techniques with a botnet to disguise the location of web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities.
- Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct distributed denial-of-service attacks (DDoS attacks);
- Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Pursuant to the Registry-Registrar Agreement, registry operator reserves the right at its sole discretion to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary: (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of registry operator, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement and this Anti-Abuse Policy, or (5) to correct mistakes made by registry operator or any registrar in connection with a domain name registration. Registry operator also reserves the right to place upon registry lock, hold, or similar status a domain name during resolution of a dispute.

The policy stated above will be accompanied by notes about how to submit a report to the registry operator's abuse point of contact, and how to report an orphan glue record suspected of being used in connection with malicious conduct (see below).

Abuse point of contact and procedures for handling abuse complaints

The registry operator will establish an abuse point of contact. This contact will be a role-based e-mail address of the form "abuse@registry.WEB". This e-mail address will allow multiple staff members to monitor abuse reports on a 24x7 basis, and then work toward closure of cases as each situation calls for. For tracking purposes, the registry operator will have a ticketing system with which all complaints will be tracked internally. The reporter will be provided with the ticket reference identifier for potential follow-up. Afilias will integrate its existing ticketing system with the registry operator's to ensure uniform tracking and handling of the complaint. This role-based approach has been used successfully by ISPs, e-mail service providers, and registrars for many years, and is considered a global best practice.

The registry operator's designated abuse handlers will then evaluate complaints received via the abuse system address. They will decide whether a particular issue is of concern, and decide what action, if any, is appropriate.

In general, the registry operator will find itself receiving abuse reports from a wide variety of parties, including security researchers and Internet security companies, financial institutions such as banks, Internet users, and law enforcement agencies among others. Some of these parties may provide good forensic data or supporting evidence of the malicious behavior. In other cases, the party reporting an issue may not be familiar with how to provide such data or proof of malicious behavior. It is expected that a percentage of abuse reports to the registry operator will not be actionable, because there will not be enough evidence to support the complaint (even after investigation), and because some reports or reporters will simply not be credible.

The security function includes a communication and outreach function, with information sharing with industry partners regarding malicious or abusive behavior, in order to ensure coordinated abuse mitigation across multiple TLDs.

Assessing abuse reports requires great care, and the registry operator will rely upon professional, trained investigators who are versed in such matters. The goals are accuracy, good record-keeping, and a zero false-positive rate so as not to harm innocent registrants.

Different types of malicious activities require different methods of investigation and documentation. Further, the registry operator expects to face unexpected or complex situations that call for professional advice, and will rely upon professional, trained investigators as needed.

In general, there are two types of domain abuse that must be addressed:

- a) Compromised domains. These domains have been hacked or otherwise compromised by criminals, and the registrant is not responsible for the malicious activity taking place on the domain. For example, the majority of domain names that host phishing sites are compromised. The goal in such cases is to get word to the registrant (usually via the registrar) that there is a problem that needs attention with the expectation that the registrant will address the problem in a timely manner. Ideally such domains do not get suspended, since suspension would disrupt legitimate activity on the domain.
- b) Malicious registrations. These domains are registered by malefactors for the purpose of abuse. Such domains are generally targets for suspension, since they have no legitimate use.

The standard procedure is that the registry operator will forward a credible alleged case of malicious domain name use to the domain's sponsoring registrar with a request that the registrar investigate the case and act appropriately. The registrar will be provided evidence collected as a result of the investigation conducted by the trained abuse handlers. As part of the investigation, if inaccurate or false WHOIS registrant information is detected, the registrar is notified about this. The registrar is the party with a direct relationship with—and a direct contract with—the registrant. The registrar will also have vital information that the registry operator will not, such as:

- Details about the domain purchase, such as the payment method used (credit

card, PayPal, etc.);

- The identity of a proxy-protected registrant;
- The purchaser's IP address;
- Whether there is a reseller involved, and;
- The registrant's past sales history and purchases in other TLDs (insofar as the registrar can determine this).

Registrars do not share the above information with registry operators due to privacy and liability concerns, among others. Because they have more information with which to continue the investigation, and because they have a direct relationship with the registrant, the registrar is in the best position to evaluate alleged abuse. The registrar can determine if the use violates the registrar's legal terms of service or the registry Anti-Abuse Policy, and can decide whether or not to take any action. While the language and terms vary, registrars will be expected to include language in their registrar-registrant contracts that indemnifies the registrar if it takes action, and allows the registrar to suspend or cancel a domain name; this will be in addition to the registry Anti-Abuse Policy. Generally, registrars can act if the registrant violates the registrar's terms of service, or violates ICANN policy, or if illegal activity is involved, or if the use violates the registry's Anti-Abuse Policy.

If a registrar does not take action within a time period indicated by the registry operator (usually 24 hours), the registry operator might then decide to take action itself. At all times, the registry operator reserves the right to act directly and immediately if the potential harm to Internet users seems significant or imminent, with or without notice to the sponsoring registrar.

The registry operator will be prepared to call upon relevant law enforcement bodies as needed. There are certain cases, for example, Illegal pharmacy domains, where the registry operator will contact the Law Enforcement Agencies to share information about these domains, provide all the evidence collected and work closely with them before any action will be taken for suspension. The specific action is often dependent upon the jurisdiction of which the registry operator, although the operator in all cases will adhere to applicable laws and regulations.

When valid court orders or seizure warrants are received from courts or law enforcement agencies of relevant jurisdiction, the registry operator will order execution in an expedited fashion. Compliance with these will be a top priority and will be completed as soon as possible and within the defined timelines of the order. There are certain cases where Law Enforcement Agencies request information about a domain including but not limited to:

- Registration information
- History of a domain, including recent updates made
- Other domains associated with a registrant's account
- Patterns of registrant portfolio

Requests for such information is handled on a priority basis and sent back to the requestor as soon as possible. Afilias sets a goal to respond to such requests within 24 hours.

The registry operator may also engage in proactive screening of its zone for malicious use of the domains in the TLD, and report problems to the sponsoring registrars. The registry operator could take advantage of a combination of the following resources, among others:

- Blocklists of domain names and nameservers published by organizations such as SURBL and Spamhaus.
- Anti-phishing feeds, which will provide URLs of compromised and maliciously registered domains being used for phishing.
- Analysis of registration or DNS query data [DNS query data received by the TLD nameservers.]

The registry operator will keep records and track metrics regarding abuse and

abuse reports. These will include:

- Number of abuse reports received by the registry's abuse point of contact described above;
- Number of cases and domains referred to registrars for resolution;
- Number of cases and domains where the registry took direct action;
- Resolution times;
- Number of domains in the TLD that have been blacklisted by major anti-spam blocklist providers, and;
- Phishing site uptimes in the TLD.

#### Removal of orphan glue records

By definition, orphan glue records used to be glue records. Glue records are related to delegations and are necessary to guide iterative resolvers to delegated nameservers. A glue record becomes an orphan when its parent nameserver record is removed without also removing the corresponding glue record. (Please reference the ICANN SSAC paper SAC048 at: <http://www.icann.org/en/committees/security/sac048.pdf>.) Orphan glue records may be created when a domain (example.tld) is placed on EPP ServerHold or ClientHold status. When placed on Hold, the domain is removed from the zone and will stop resolving. However, any child nameservers (now orphan glue) of that domain (e.g., ns1.example.tld) are left in the zone. It is important to keep these orphan glue records in the zone so that any innocent sites using that nameserver will continue to resolve. This use of Hold status is an essential tool for suspending malicious domains.

Afilias observes the following procedures, which are being followed by other registries and are generally accepted as DNS best practices. These procedures are also in keeping with ICANN SSAC recommendations.

When a request to delete a domain is received from a registrar, the registry first checks for the existence of glue records. If glue records exist, the registry will check to see if other domains in the registry are using the glue records. If other domains in the registry are using the glue records then the request to delete the domain will fail until no other domains are using the glue records. If no other domains in the registry are using the glue records then the glue records will be removed before the request to delete the domain is satisfied. If no glue records exist then the request to delete the domain will be satisfied.

If a registrar cannot delete a domain because of the existence of glue records that are being used by other domains, then the registrar may refer to the zone file or the "weekly domain hosted by nameserver report" to find out which domains are using the nameserver in question and attempt to contact the corresponding registrar to request that they stop using the nameserver in the glue record. The registry operator does not plan on performing mass updates of the associated DNS records.

The registry operator will accept, evaluate, and respond appropriately to complaints that orphan glue is being used maliciously. Such reports should be made in writing to the registry operator, and may be submitted to the registry's abuse point-of-contact. If it is confirmed that an orphan glue record is being used in connection with malicious conduct, the registry operator will have the orphan glue record removed from the zone file. Afilias has the technical ability to execute such requests as needed.

#### Methods to promote WHOIS accuracy

The creation and maintenance of accurate WHOIS records is an important part of registry management. As described in our response to question #26, WHOIS, the registry operator will manage a secure, robust and searchable WHOIS service for this TLD.

#### WHOIS data accuracy

The registry operator will offer a "thick" registry system. In this model, all key contact details for each domain name will be stored in a central location by the registry. This allows better access to domain data, and provides uniformity in storing the information. The registry operator will ensure that the required fields for WHOIS data (as per the defined policies for the TLD) are enforced at the registry level. This ensures that the registrars are providing required domain registration data. Fields defined by the registry policy to be mandatory are documented as such and must be submitted by registrars. The Afiliias registry system verifies formats for relevant individual data fields (e.g. e-mail, and phone/fax numbers). Only valid country codes are allowed as defined by the ISO 3166 code list. The Afiliias WHOIS system is extensible, and is capable of using the VAULT system, described further below.

Similar to the centralized abuse point of contact described above, the registry operator can institute a contact email address which could be utilized by third parties to submit complaints for inaccurate or false WHOIS data detected. This information will be processed by Afiliias' support department and forwarded to the registrars. The registrars can work with the registrants of those domains to address these complaints. Afiliias will audit registrars on a yearly basis to verify whether the complaints being forwarded are being addressed or not. This functionality, available to all registry operators, is activated based on the registry operator's business policy.

Afiliias also incorporates a spot-check verification system where a randomly selected set of domain names are checked periodically for accuracy of WHOIS data. Afiliias' .PRO registry system incorporates such a verification system whereby 1% of total registrations or 100 domains, whichever number is larger, are spot-checked every month to verify the domain name registrant's critical information provided with the domain registration data. With both a highly qualified corps of engineers and a 24x7 staffed support function, Afiliias has the capacity to integrate such spot-check functionality into this TLD, based on the registry operator's business policy. Note: This functionality will not work for proxy protected WHOIS information, where registrars or their resellers have the actual registrant data. The solution to that problem lies with either registry or registrar policy, or a change in the general marketplace practices with respect to proxy registrations.

Finally, Afiliias' registry systems have a sophisticated set of billing and pricing functionality which aids registry operators who decide to provide a set of financial incentives to registrars for maintaining or improving WHOIS accuracy. For instance, it is conceivable that the registry operator may decide to provide a discount for the domain registration or renewal fees for validated registrants, or levy a larger cost for the domain registration or renewal of proxy domain names. The Afiliias system has the capability to support such incentives on a configurable basis, towards the goal of promoting better WHOIS accuracy.

#### Role of registrars

As part of the RRA (Registry Registrar Agreement), the registry operator will require the registrar to be responsible for ensuring the input of accurate WHOIS data by their registrants. The Registrar/Registered Name Holder Agreement will include a specific clause to ensure accuracy of WHOIS data, and to give the registrar rights to cancel or suspend registrations if the Registered Name Holder fails to respond to the registrar's query regarding accuracy of data. ICANN's WHOIS Data Problem Reporting System (WDPRS) will be available to those who wish to file WHOIS inaccuracy reports, as per ICANN policy (<http://wdprs.internic.net/>).

Controls to ensure proper access to domain functions



Several measures are in place in the Afiliias registry system to ensure proper access to domain functions, including authentication provisions in the RRA relative to notification and contact updates via use of AUTH-INFO codes.

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

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

Information about other registry security measures such as encryption and security of registrar channels are confidential to ensure the security of the registry system. The details can be found in the response to question #30b.

#### Validation and abuse mitigation mechanisms

Afiliias has developed advanced validation and abuse mitigation mechanisms. These capabilities and mechanisms are described below. These services and capabilities are discretionary and may be utilized by the registry operator based on their policy and business need.

Afiliias has the ability to analyze the registration data for known patterns at the time of registration. A database of these known patterns is developed from domains and other associated objects (e.g., contact information) which have been previously detected and suspended after being flagged as abusive. Any domains matching the defined criteria can be flagged for investigation. Once analyzed and confirmed by the domain anti-abuse team members, these domains may be suspended. This provides proactive detection of abusive domains.

Provisions are available to enable the registry operator to only allow registrations by pre-authorized and verified contacts. These verified contacts are given a unique code that can be used for registration of new domains.

#### Registrant pre-verification and authentication

One of the systems that could be used for validity and identity authentication is VAULT (Validation and Authentication Universal Lookup). It utilizes information obtained from a series of trusted data sources with access to billions of records containing data about individuals for the purpose of providing independent age and id verification as well as the ability to incorporate additional public or private data sources as required. At present it has the following: US Residential Coverage - 90% of Adult Population and also International Coverage - Varies from Country to Country with a minimum of 80% coverage (24 countries, mostly European).

Various verification elements can be used. Examples might include applicant data such as name, address, phone, etc. Multiple methods could be used for verification include integrated solutions utilizing API (XML Application Programming Interface) or sending batches of requests.

- Verification and Authentication requirements would be based on TLD operator requirements or specific criteria.

- Based on required WHOIS Data; registrant contact details (name, address, phone)
- If address/ZIP can be validated by VAULT, the validation process can continue (North America +25 International countries)
- If in-line processing and registration and EPP/API call would go to the verification clearinghouse and return up to 4 challenge questions.
- If two-step registration is required, then registrants would get a link to complete the verification at a separate time. The link could be specific to a domain registration and pre-populated with data about the registrant.
- If WHOIS data is validated a token would be generated and could be given back to the registrar which registered the domain.
- WHOIS data would reflect the Validated Data or some subset, i.e., fields displayed could be first initial and last name, country of registrant and date validated. Other fields could be generic validation fields much like a "privacy service".
- A "Validation Icon" customized script would be sent to the registrants email address. This could be displayed on the website and would be dynamically generated to avoid unauthorized use of the Icon. When clicked on the Icon would show limited WHOIS details i.e. Registrant: jdoe, Country: USA, Date Validated: March 29, 2011, as well as legal disclaimers.
- Validation would be annually renewed, and validation date displayed in the WHOIS.

#### Abuse prevention resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way. Abuse prevention and detection is a function that is staffed across the various groups inside Afilias, and requires a team effort when abuse is either well hidden or widespread, or both. While all of Afilias' 200+ employees are charged with responsibility to report any detected abuse, the engineering and analysis teams, numbering over 30, provide specific support based on the type of abuse and volume and frequency of analysis required. The Afilias security and support teams have the authority to initiate mitigation.

Afilias has developed advanced validation and abuse mitigation mechanisms. These capabilities and mechanisms are described below. These services and capabilities are discretionary and may be utilized by the registry operator based on their policy and business need.

This TLD's anticipated volume of registrations in the first three years of operations is listed in response #46. Afilias and the registry operator's anti-abuse function anticipates the expected volume and type of registrations, and together will adequately cover the staffing needs for this TLD. The registry operator will maintain an abuse response team, which may be a combination of internal staff and outside specialty contractors, adjusting to the needs of the size and type of TLD. The team structure planned for this TLD is based on several years of experience responding to, mitigating, and managing abuse for TLDs of various sizes. The team will generally consist of abuse handlers (probably internal), a junior analyst, (either internal or external), and a senior security consultant (likely an external resource providing the registry operator with extra expertise as needed). These responders will be specially trained in the investigation of abuse complaints, and will have the latitude to act expeditiously to suspend domain names (or apply other remedies) when called for.

The exact resources required to maintain an abuse response team must change with the size and registration procedures of the TLD. An initial abuse handler is necessary as a point of contact for reports, even if a part-time responsibility. The abuse handlers monitor the abuse email address for complaints and evaluate incoming reports from a variety of sources. A large percentage of abuse reports to the registry operator may be unsolicited commercial email. The designated abuse handlers can identify legitimate reports and then decide what action is appropriate, either to act upon them, escalate to a security analyst for closer investigation, or refer them to registrars as per the above-described procedures. A TLD with rare cases of abuse would conform to this structure.

If multiple cases of abuse within the same week occur regularly, the registry operator will consider staffing internally a security analyst to investigate the complaints as they become more frequent. Training an abuse analyst requires 3-6 months and likely requires the active guidance of an experienced senior security analyst for guidance and verification of assessments and recommendations being made.

If this TLD were to regularly experience multiple cases of abuse within the same day, a full-time senior security analyst would likely be necessary. A senior security analyst capable of fulfilling this role should have several years of experience and able to manage and train the internal abuse response team.

The abuse response team will also maintain subscriptions for several security information services, including the blocklists from organizations like SURBL and Spamhaus and anti-phishing and other domain related abuse (malware, fast-flux etc.) feeds. The pricing structure of these services may depend on the size of the domain and some services will include a number of rapid suspension requests for use as needed.

For a large TLD, regular audits of the registry data are required to maintain control over abusive registrations. When a registrar with a significant number of registrations has been compromised or acted maliciously, the registry operator may need to analyze a set of registration or DNS query data. A scan of all the domains of a registrar is conducted only as needed. Scanning and analysis for a large registrar may require as much as a week of full-time effort for a dedicated machine and team.

## 29. Rights Protection Mechanisms

Rights protection is a core responsibility of the TLD operator, and is supported by a fully-developed plan for rights protection that includes:

- Establishing mechanisms to prevent unqualified registrations (e.g., registrations made in violation of the registry's eligibility restrictions or policies);
- Implementing a robust Sunrise program, utilizing the Trademark Clearinghouse, the services of one of ICANN's approved dispute resolution providers, a trademark validation agent, and drawing upon sunrise policies and rules used successfully in previous gTLD launches;
- Implementing a professional trademark claims program that utilizes the Trademark Clearinghouse, and drawing upon models of similar programs used successfully in previous TLD launches;
- Complying with the URS requirements;
- Complying with the UDRP;
- Complying with the PDDRP, and;
- Including all ICANN-mandated and independently developed rights protection mechanisms ("RPMs") in the registry-registrar agreement entered into by ICANN-accredited registrars authorized to register names in the TLD.

The response below details the rights protection mechanisms at the launch of the TLD (Sunrise and Trademark Claims Service) which comply with rights protection policies (URS, UDRP, PDDRP, and other ICANN RPMs), outlines additional provisions made for rights protection, and provides the resourcing plans.

Safeguards for rights protection at the launch of the TLD

The launch of this TLD will include the operation of a trademark claims service according to the defined ICANN processes for checking a registration request and alerting trademark holders of potential rights infringement.

The Sunrise Period will be an exclusive period of time, prior to the opening of public registration, when trademark and service mark holders will be able to reserve marks that are an identical match in the .WEB domain. Following the Sunrise Period, Schlund Technologies GmbH will open registration to qualified applicants.

The anticipated Rollout Schedule for the Sunrise Period will be approximately as follows:

- Launch of the TLD - Sunrise Period begins for trademark holders and service mark holders to submit registrations for their exact marks in the .WEB domain.
- Quiet Period - The Sunrise Period will close and will be followed by a Quiet Period for testing and evaluation.
- One month after close of Quiet Period - Registration in the .WEB domain will be opened to qualified applicants.

Sunrise Period Requirements & Restrictions

Those wishing to reserve their marks in the .WEB domain during the Sunrise Period must own a current trademark or service mark listed in the Trademark Clearinghouse.

Notice will be provided to all trademark holders in the Clearinghouse if someone is seeking a Sunrise registration. This notice will be provided to holders of marks in the Clearinghouse that are an Identical Match (as defined in the Trademark Clearing House) to the name to be registered during Sunrise.

Each Sunrise registration will require a minimum term, to be determined at a later date.

Schlund Technologies GmbH will establish the following Sunrise eligibility requirements (SERs) as minimum requirements, verified by Clearinghouse data, and incorporate a Sunrise Dispute Resolution Policy (SDRP). The SERs include: (i) ownership of a mark that satisfies the criteria set forth in section 7.2 of the Trademark Clearing House specifications, (ii) description of international class of goods or services covered by registration; (iii) representation that all provided information is true and correct; and (iv) provision of data sufficient to document rights in the trademark.

The SDRP will allow challenges based on the following four grounds: (i) at time the challenged domain name was registered, the registrants did not hold a trademark registration of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; (ii) the domain name is not identical to the mark on which the registrant based its Sunrise registration; (iii) the trademark registration on which the registrant based its Sunrise registration is not of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; or (iv) the trademark registration on which the domain name registrant based its Sunrise registration did not issue on or before the effective date of the

Registry Agreement and was not applied for on or before ICANN announced the applications received.

#### Ongoing rights protection mechanisms

Several mechanisms will be in place to protect rights in this TLD. As described in our responses to questions #27 and #28, measures are in place to ensure domain transfers and updates are only initiated by the appropriate domain holder, and an experienced team is available to respond to legal actions by law enforcement or court orders.

This TLD will conform to all ICANN RPs including URS (defined below), UDRP, PDDRP, and all measures defined in Specification 7 of the new TLD agreement.

#### Uniform Rapid Suspension (URS)

Schlund Technologies GmbH will implement decisions rendered under the URS on an ongoing basis. Per the URS policy posted on ICANN's Web site as of this writing, the registry operator will receive notice of URS actions from the ICANN-approved URS providers. These emails will be directed immediately to the registry operator's support staff, which is on duty 24x7. The support staff will be responsible for creating a ticket for each case, and for executing the directives from the URS provider. All support staff will receive pertinent training.

As per ICANN's URS guidelines, within 24 hours of receipt of the notice of complaint from the URS provider, the registry operator shall "lock" the domain, meaning the registry shall restrict all changes to the registration data, including transfer and deletion of the domain names, but the name will remain in the TLD DNS zone file and will thus continue to resolve. The support staff will "lock" the domain by associating the following EPP statuses with the domain and relevant contact objects:

- ServerUpdateProhibited, with an EPP reason code of "URS"
- ServerDeleteProhibited, with an EPP reason code of "URS"
- ServerTransferProhibited, with an EPP reason code of "URS"
- The registry operator's support staff will then notify the URS provider immediately upon locking the domain name, via email.

The registry operator's support staff will retain all copies of emails from the URS providers, assign them a tracking or ticket number, and will track the status of each opened URS case through to resolution via spreadsheet or database.

The registry operator's support staff will execute further operations upon notice from the URS providers. The URS provider is required to specify the remedy and required actions of the registry operator, with notification to the registrant, the complainant, and the registrar.

As per the URS guidelines, if the complainant prevails, the registry operator shall suspend the domain name, which shall remain suspended for the balance of the registration period and would not resolve to the original web site. The nameservers shall be redirected to an informational web page provided by the URS provider about the URS. The WHOIS for the domain name shall continue to display all of the information of the original registrant except for the redirection of the nameservers. In addition, the WHOIS shall reflect that the domain name will not be able to be transferred, deleted or modified for the life of the registration."

#### Rights protection via the RRA

The following will be memorialized and be made binding via the Registry-Registrar and Registrar-Registrant Agreements:

- The registry may reject a registration request or a reservation request, or may delete, revoke, suspend, cancel, or transfer a registration or reservation

under the following criteria:

- a. to enforce registry policies and ICANN requirements; each as amended from time to time;
- b. that is not accompanied by complete and accurate information as required by ICANN requirements and/or registry policies or where required information is not updated and/or corrected as required by ICANN requirements and/or registry policies;
- c. to protect the integrity and stability of the registry, its operations, and the TLD system;
- d. to comply with any applicable law, regulation, holding, order, or decision issued by a court, administrative authority, or dispute resolution service provider with jurisdiction over the registry;
- e. to establish, assert, or defend the legal rights of the registry or a third party or to avoid any civil or criminal liability on the part of the registry and/or its affiliates, subsidiaries, officers, directors, representatives, employees, contractors, and stockholders;
- f. to correct mistakes made by the registry or any accredited registrar in connection with a registration; or
- g. as otherwise provided in the Registry-Registrar Agreement and/or the Registrar-Registrant Agreement.

Reducing opportunities for behaviors such as phishing or pharming

In our response to question #28, Schlund Technologies GmbH has described its anti-abuse program. Rather than repeating the policies and procedures here, please see our response to question #28 for full details.

In the case of this TLD, Schlund Technologies GmbH will apply an approach that addresses registered domain names (rather than potentially registered domains). This approach will not infringe upon the rights of eligible registrants to register domains, and allows Schlund Technologies GmbH internal controls, as well as community-developed UDRP and URS policies and procedures if needed, to deal with complaints, should there be any.

Afilias is a member of various security fora which provide access to lists of names in each TLD which may be used for malicious purposes. Such identified names will be subject to the TLD anti-abuse policy, including rapid suspensions after due process.

Rights protection resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Supporting RPMs requires several departments within the registry operator as well as within Afilias. The implementation of Sunrise and the Trademark Claims service and on-going RPM activities will pull from the 102 Afilias staff members of the engineering, product management, development, security and policy teams at Afilias, which is on duty 24x7, and the support staff of the registry operator. A trademark validator will also be assigned within the registry operator, whose responsibilities may require as much as 50% of full-time employment if the domains under management were to exceed several million. No additional hardware or software resources are required to support this as Afilias has fully-operational capabilities to manage abuse today.

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

The answer to question #30a is provided by Afiliias, the back-end provider of registry services for this TLD.

Afiliias aggressively and actively protects the registry system from known threats and vulnerabilities, and has deployed an extensive set of security protocols, policies and procedures to thwart compromise. Afiliias' robust and detailed plans are continually updated and tested to ensure new threats are mitigated prior to becoming issues. Afiliias will continue these rigorous security measures, which include:

- Multiple layers of security and access controls throughout registry and support systems;
- 24x7 monitoring of all registry and DNS systems, support systems and facilities;
- Unique, proven registry design that ensures data integrity by granting only authorized access to the registry system, all while meeting performance requirements;
- Detailed incident and problem management processes for rapid review, communications, and problem resolution, and;
- Yearly external audits by independent, industry-leading firms, as well as twice-yearly internal audits.

#### Security policies and protocols

Afiliias has included security in every element of its service, including facilities, hardware, equipment, connectivity, Internet services, systems, computer systems, organizational security, outage prevention, monitoring, disaster mitigation, and escrow/insurance, from the original design, through development, and finally as part of production deployment. Examples of threats and the confidential and proprietary mitigation procedures are detailed in our response to question #30(b).

There are several important aspects of the security policies and procedures to note:

- Afiliias hosts domains in data centers around the world that meet or exceed global best practices.
- Afiliias' DNS infrastructure is massively provisioned as part of its DDoS mitigation strategy, thus ensuring sufficient capacity and redundancy to support new gTLDs.
- Diversity is an integral part of all of our software and hardware stability and robustness plan, thus avoiding any single points of failure in our infrastructure.
- Access to any element of our service (applications, infrastructure and data) is only provided on an as-needed basis to employees and a limited set of others to fulfill their job functions. The principle of least privilege is applied.
- All registry components - critical and non-critical - are monitored 24x7 by staff at our NOCs, and the technical staff has detailed plans and procedures that have stood the test of time for addressing even the smallest anomaly. Well-documented incident management procedures are in place to quickly involve the on-call technical and management staff members to address any issues.

Afiliias follows the guidelines from the ISO 27001 Information Security Standard (Reference:

[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=42103](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103) ) for the management and implementation of its Information Security Management System. Afiliias also utilizes the COBIT IT governance framework to facilitate policy development and enable controls for appropriate management of risk (Reference: <http://www.isaca.org/cobit>). Best practices

defined in ISO 27002 are followed for defining the security controls within the organization. Afiliias continually looks to improve the efficiency and effectiveness of our processes, and follows industry best practices as defined by the IT Infrastructure Library, or ITIL (Reference: <http://www.itil-officialsite.com/>).

The Afiliias registry system is located within secure data centers that implement a multitude of security measures both to minimize any potential points of vulnerability and to limit any damage should there be a breach. The characteristics of these data centers are described fully in our response to question #30(b).

The Afiliias registry system employs a number of multi-layered measures to prevent unauthorized access to its network and internal systems. Before reaching the registry network, all traffic is required to pass through a firewall system. Packets passing to and from the Internet are inspected, and unauthorized or unexpected attempts to connect to the registry servers are both logged and denied. Management processes are in place to ensure each request is tracked and documented, and regular firewall audits are performed to ensure proper operation. 24x7 monitoring is in place and, if potential malicious activity is detected, appropriate personnel are notified immediately.

Afiliias employs a set of security procedures to ensure maximum security on each of its servers, including disabling all unnecessary services and processes and regular application of security-related patches to the operating system and critical system applications. Regular external vulnerability scans are performed to verify that only services intended to be available are accessible.

Regular detailed audits of the server configuration are performed to verify that the configurations comply with current best security practices. Passwords and other access means are changed on a regular schedule and are revoked whenever a staff member's employment is terminated.

#### Access to registry system

Access to all production systems and software is strictly limited to authorized operations staff members. Access to technical support and network operations teams where necessary are read only and limited only to components required to help troubleshoot customer issues and perform routine checks. Strict change control procedures are in place and are followed each time a change is required to the production hardware/application. User rights are kept to a minimum at all times. In the event of a staff member's employment termination, all access is removed immediately.

Afiliias applications use encrypted network communications. Access to the registry server is controlled. Afiliias allows access to an authorized registrar only if each of the authentication factors matches the specific requirements of the requested authorization. These mechanisms are also used to secure any web-based tools that allow authorized registrars to access the registry. Additionally, all write transactions in the registry (whether conducted by authorized registrars or the registry's own personnel) are logged.

EPP connections are encrypted using TLS/SSL, and mutually authenticated using both certificate checks and login/password combinations. Web connections are encrypted using TLS/SSL for an encrypted tunnel to the browser, and authenticated to the EPP server using login/password combinations.

All systems are monitored for security breaches from within the data center and without, using both system-based and network-based testing tools. Operations staff also monitor systems for security-related performance anomalies. Triple-redundant continual monitoring ensures multiple detection paths for any potential incident or problem. Details are provided in our response to questions #30(b) and #42. Network Operations and Security Operations teams perform regular audits in search of any potential vulnerability.



To ensure that registrar hosts configured erroneously or maliciously cannot deny service to other registrars, Afilias uses traffic shaping technologies to prevent attacks from any single registrar account, IP address, or subnet. This additional layer of security reduces the likelihood of performance degradation for all registrars, even in the case of a security compromise at a subset of registrars.

There is a clear accountability policy that defines what behaviors are acceptable and unacceptable on the part of non-staff users, staff users, and management. Periodic audits of policies and procedures are performed to ensure that any weaknesses are discovered and addressed. Aggressive escalation procedures and well-defined Incident Response management procedures ensure that decision makers are involved at early stages of any event.

In short, security is a consideration in every aspect of business at Afilias, and this is evidenced in a track record of a decade of secure, stable and reliable service.

#### Independent assessment

Supporting operational excellence as an example of security practices, Afilias performs a number of internal and external security audits each year of the existing policies, procedures and practices for:

- Access control;
- Security policies;
- Production change control;
- Backups and restores;
- Batch monitoring;
- Intrusion detection, and
- Physical security.

Afilias has an annual Type 2 SSAE 16 audit performed by PricewaterhouseCoopers (PwC). Further, PwC performs testing of the general information technology controls in support of the financial statement audit. A Type 2 report opinion under SSAE 16 covers whether the controls were properly designed, were in place, and operating effectively during the audit period (calendar year). This SSAE 16 audit includes testing of internal controls relevant to Afilias' domain registry system and processes. The report includes testing of key controls related to the following control objectives:

- Controls provide reasonable assurance that registrar account balances and changes to the registrar account balances are authorized, complete, accurate and timely.
- Controls provide reasonable assurance that billable transactions are recorded in the Shared Registry System (SRS) in a complete, accurate and timely manner.
- Controls provide reasonable assurance that revenue is systemically calculated by the Deferred Revenue System (DRS) in a complete, accurate and timely manner.
- Controls provide reasonable assurance that the summary and detail reports, invoices, statements, registrar and registry billing data files, and ICANN transactional reports provided to registry operator(s) are complete, accurate and timely.
- Controls provide reasonable assurance that new applications and changes to existing applications are authorized, tested, approved, properly implemented and documented.
- Controls provide reasonable assurance that changes to existing system software and implementation of new system software are authorized, tested, approved, properly implemented and documented.
- Controls provide reasonable assurance that physical access to data centers is restricted to properly authorized individuals.
- Controls provide reasonable assurance that logical access to system resources is restricted to properly authorized individuals.
- Controls provide reasonable assurance that processing and backups are appropriately authorized and scheduled and that deviations from scheduled processing and backups are identified and resolved.

The last Type 2 report issued was for the year 2010, and it was unqualified, i.e., all systems were evaluated with no material problems found.

During each year, Afilias monitors the key controls related to the SSAE controls. Changes or additions to the control objectives or activities can result due to deployment of new services, software enhancements, infrastructure changes or process enhancements. These are noted and after internal review and approval, adjustments are made for the next review.

In addition to the PricewaterhouseCoopers engagement, Afilias performs internal security audits twice a year. These assessments are constantly being expanded based on risk assessments and changes in business or technology.

Additionally, Afilias engages an independent third-party security organization, PivotPoint Security, to perform external vulnerability assessments and penetration tests on the sites hosting and managing the Registry infrastructure. These assessments are performed with major infrastructure changes, release of new services or major software enhancements. These independent assessments are performed at least annually. A report from a recent assessment is attached with our response to question #30(b).

Afilias has engaged with security companies specializing in application and web security testing to ensure the security of web-based applications offered by Afilias, such as the Web Admin Tool (WAT) for registrars and registry operators.

Finally, Afilias has engaged IBM's Security services division to perform ISO 27002 gap assessment studies so as to review alignment of Afilias' procedures and policies with the ISO 27002 standard. Afilias has since made adjustments to its security procedures and policies based on the recommendations by IBM.

#### Special TLD considerations

Afilias' rigorous security practices are regularly reviewed; if there is a need to alter or augment procedures for this TLD, they will be done so in a planned and deliberate manner.

#### Commitments to registrant protection

With over a decade of experience protecting domain registration data, Afilias understands registrant security concerns. Afilias supports a "thick" registry system in which data for all objects are stored in the registry database that is the centralized authoritative source of information. As an active member of IETF (Internet Engineering Task Force), ICANN's SSAC (Security & Stability Advisory Committee), APWG (Anti-Phishing Working Group), MAAWG (Messaging Anti-Abuse Working Group), USENIX, and ISACA (Information Systems Audits and Controls Association), the Afilias team is highly attuned to the potential threats and leading tools and procedures for mitigating threats. As such, registrants should be confident that:

- Any confidential information stored within the registry will remain confidential;
- The interaction between their registrar and Afilias is secure;
- The Afilias DNS system will be reliable and accessible from any location;
- The registry system will abide by all polices, including those that address registrant data;
- Afilias will not introduce any features or implement technologies that compromise access to the registry system or that compromise registrant security.

Afilias has directly contributed to the development of the documents listed below and we have implemented them where appropriate. All of these have helped

improve registrants' ability to protect their domains name(s) during the domain name lifecycle.

- [SAC049]: SSAC Report on DNS Zone Risk Assessment and Management (03 June 2011)
- [SAC044]: A Registrant's Guide to Protecting Domain Name Registration Accounts (05 November 2010)
- [SAC040]: Measures to Protect Domain Registration Services Against Exploitation or Misuse (19 August 2009)
- [SAC028]: SSAC Advisory on Registrar Impersonation Phishing Attacks (26 May 2008)
- [SAC024]: Report on Domain Name Front Running (February 2008)
- [SAC022]: Domain Name Front Running (SAC022, SAC024) (20 October 2007)
- [SAC011]: Problems caused by the non-renewal of a domain name associated with a DNS Name Server (7 July 2006)
- [SAC010]: Renewal Considerations for Domain Name Registrants (29 June 2006)
- [SAC007]: Domain Name Hijacking Report (SAC007) (12 July 2005)

To protect any unauthorized modification of registrant data, Afilias mandates TLS/SSL transport (per RFC 5246) and authentication methodologies for access to the registry applications. Authorized registrars are required to supply a list of specific individuals (five to ten people) who are authorized to contact the registry. Each such individual is assigned a pass phrase. Any support requests made by an authorized registrar to registry customer service are authenticated by registry customer service. All failed authentications are logged and reviewed regularly for potential malicious activity. This prevents unauthorized changes or access to registrant data by individuals posing to be registrars or their authorized contacts.

These items reflect an understanding of the importance of balancing data privacy and access for registrants, both individually and as a collective, worldwide user base.

The Afilias 24/7 Customer Service Center consists of highly trained staff who collectively are proficient in 15 languages, and who are capable of responding to queries from registrants whose domain name security has been compromised - for example, a victim of domain name hijacking. Afilias provides specialized registrant assistance guides, including specific hand-holding and follow-through in these kinds of commonly occurring circumstances, which can be highly distressing to registrants

Security resourcing plans

Please refer to our response to question #30b for security resourcing plans.

© **Internet Corporation For Assigned Names and Numbers.**



# **Annex 9.**



## **New gTLD Application Submitted to ICANN by: NU DOT CO LLC**

**String: WEB**

**Originally Posted: 13 June 2012**

**Application ID: 1-1296-36138**

### **Applicant Information**

#### **1. Full legal name**

NU DOT CO LLC

#### **2. Address of the principal place of business**

Contact Information Redacted

#### **3. Phone number**

Contact Information Redacted

#### **4. Fax number**

Contact Information Redacted

## 5. If applicable, website or URL

## Primary Contact

### 6(a). Name

Jose Ignacio Rasco

### 6(b). Title

Manager

### 6(c). Address

### 6(d). Phone Number

Contact Information Redacted

### 6(e). Fax Number

### 6(f). Email Address

Contact Information Redacted

## Secondary Contact

### 7(a). Name

Mr. Nicolai Bezsonoff

### 7(b). Title

Manager

**7(c). Address****7(d). Phone Number**

Contact Information Redacted

**7(e). Fax Number****7(f). Email Address**

Contact Information Redacted

**Proof of Legal Establishment****8(a). Legal form of the Applicant**

Limited liability company

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

NU DOTCO LLC is a UNITED STATES entity, registered in the STATE of DELAWARE as a limited liability company.

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

Attachments are not displayed on this form.

**9(a). If applying company is publicly traded, provide the exchange and symbol.****9(b). If the applying entity is a subsidiary, provide the parent company.**



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

## Applicant Background

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

Jose Ignacio Rasco III	Manager
Juan Diego Calle	Manager
Nicolai Bezsonoff	Manager

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

Jose Ignacio Rasco III	CFO
Juan Diego Calle	CEO
Nicolai Bezsonoff	COO

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

Domain Marketing Holdings, LLC	Not Applicable
NUCO LP, LLC	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.**

WEB

**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.**

NU DOTCO, LLC ("NU.CO") foresees no known rendering issues in connection with the proposed .LAW TLD which it is seeking to apply for as a gTLD. This answer is based upon consultation with NU.CO's backend provider, Neustar, which has successfully launched a number of new gTLDs over the last decade. In reaching this determination, the following data points were analyzed:

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

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

## Mission/Purpose

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

18.1 Mission/purpose of .WEB

The mission of .WEB is to provide the internet community at-large with an alternative "home domain" for their online presence. We envision that through strategic marketing campaigns designed to brand the domain, it will become a premium online namespace for a variety of businesses and websites. This general domain will provide new registrants with better, more relevant alternatives to the limited options remaining for current commercial TLD names.

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

18.2 How will .WEB benefit registrants, Internet users, and others?

.WEB seeks to offer registrants and the broader internet community, with a reliable, trusted, and secure top level domain (TLD). Congestion in the current availability of commercial TLD names fundamentally advantages older incumbent players. Providing access to additional high-value second level domain names (i.e. shorter and more memorable) will provide an opportunity for new entrants to compete effectively for internet users' finite attention. The domain's coherent and consistent branding will assist registrants in developing meaningful emotional connection with users, allowing them to further

differentiate themselves as premium destinations. These marketing efforts along with the initial adoption of key industry players, should reinforce the implicit attribution of "cutting-edge" and "innovativeness" upon its registrants. Prospective users benefit from the long-term commitment of a proven executive team that has a track-record of building and successfully marketing affinity TLD's (e.g., .CO targeting innovative businesses and entrepreneurs).

The demand for having an online presence continues to grow worldwide, especially as more people and businesses become active internet users, enjoying the increases in productivity and promotional effectiveness that the internet offers. A clear example of this is the number of worldwide internet users, which has grown at an average 18% annual rate over the past decade, and domain registrations which have experienced similar adoption rates having grown from approximately 25mm in 2000 to over 225mm today.

In particular for small businesses and entrepreneurs, the Internet offers an incredibly useful way to promote themselves to a wider audience, both locally and globally. Moreover, it allows them to cost-effectively offer their products and services directly to consumers, leveling the playing field with larger and more established competitors. A number of new and innovative business models have been established that were not possible prior to the Internet, creating substantial value for society.

However, until a few years ago it was difficult and costly for individuals and small businesses to establish an internet presence. This has changed as prices decreased dramatically and offerings became more accessible and intuitive. This is the result of having many retailers (i.e. registrars or resellers) that compete amongst each other on price, along with product and service differentiation. Differentiation has mainly centered around higher value-add services ancillary to the domain registration itself, such as hosting, web-site builders, SSL, e-mail, etc. The basic product (a domain) has not changed much, and until now, there have been few feasible alternatives to the commercial TLDs. The proposed new TLDs will provide users with more relevant and customized options. Just as ICANN opened up the market for the distribution and registration of domains and created the Registrar industry, which ultimately benefitted hundreds of millions of people and businesses worldwide, we expect that the introduction of new TLDs will yield similar benefits.

The experienced team behind this application initially launched and currently operates the .CO ccTLD. The intention is for .WEB to be added to .CO's product portfolio, where it can benefit from economies of scale along with the firm's experience and expertise in marketing and branding TLD properties. Their successful track record proves that properly branded affinity domains can help sites form deeper emotional connections with their users, providing significant value-add. The .CO re-launch is a great illustration of how a new option in TLDs can address the unmet needs an affinity group (e.g., small businesses and start-ups), and we continue to firmly believe that the new .WEB domain will provide better, more relevant solutions for registrants .

Since its launch, .CO's marketing has primarily focused on developing a worldwide ecosystem of innovative small businesses and entrepreneurs. To date, the .CO registry, .CO Internet S.A.S, has reached close to 1.3 million domains under management, with more than one million individual new Registrations in the first year alone and a renewal rate for domains purchased during launch of nearly 70% and a current average renewal rate of 65%. The renewal rate is one of the highest amongst the industry and especially high considering it has not yet reached the multiple year expiration dates, where it's expected to climb even higher. In addition, .CO has become the standard secondary option to .COM for the leading global registrars, having the most conversions when presented with a non-.COM option. Further, .CO has secured a strong position with the tech startup community by securing such high profile users as Twitter (t.co), Google (g.co), tech influencers like Angel list (angel.co) and 500 Startups (500.co), and entrepreneurship organizations like Startup America (s.co).

.CO has differentiated itself from other existing TLDs by combining innovative branding with the highest standards in trademark protection, unprecedented marketing campaigns, and pro-active security monitoring. We plan to implement a very similar strategy for .WEB in its launch, operation, promotion and growth.

We plan to target a similar community of entrepreneurs, startups, and progressive corporate entities that are looking for an online presence with a suitable domain name. We anticipate the addressable community will continue to grow as traditional businesses choose to launch an online presence for their pre-existing operations and as entrepreneurs launch new start-ups. The domain's marketing strategy will utilize a 3 pillar framework, similar to that used with .CO:

- Awareness: We plan to launch marketing campaigns to both the small businesses and entrepreneurs promoting .WEB via a combination of:

- o Media placements online and offline
- o Social media campaigns
- o Events
- o Sponsorships
- o Endorsements
- o PR efforts
- o Direct marketing
- o Channel marketing

- Usage: We plan to foster the community of users of .WEB via a combination community engagement and outreach, use-case development and direct marketing to base.

- Distribution: The distribution will be done through the existing ICANN accredited registrar channel and will include marketing at the point of sale, packages and bundles, campaigns, etc.

The marketing plans will evolve depending on market conditions, but using .CO as an example, we implemented an awareness and branding strategy that included the creation of a brand identity and logo; mass media placements including 2 super-bowl commercials with one of our partners plus many TV placements; billboards and other outdoors campaigns; several online media campaigns including networks, re-targeting and videos; ongoing Twitter, Facebook engagements; sponsorship and presence in a variety of events for TMs (INTA), Tech startups (SxSW, Web 2.0, Internetweek, etc.), Startups (Task Rabbit TR.co), Community (ICANN, LACTLD, etc.), etc. We also implemented for .CO a strong usage promotion of the domain by creating and fostering a community of .CO users and case studies. We achieved this through a combination of events, sponsorships, and partnerships with different entities like Angel.co, 500.co, Startup America (s.co), founders institute (fi.co), etc. We also cultivated many case studies of successful .CO users, remaining in close contact with them. Finally, we implemented a rigorous channel marketing and sales plan that included marketing placements at the point of purchase plus co-marketing and community outreach.

While we do plan to follow a similar strategy to achieve widespread awareness, usage and distribution, the budget and actual placements for promoting .WEB will be scaled down accordingly, as neither its volume of registrations or revenues is expected to be in line with that of .CO.

By launching the .WEB domain we expect to provide more descriptive/ relevant options for end-users, including access to desirable second level domain names which are unavailable or occupied by current general TLD's. As illustrated with .CO, the rapid growth to 1.3 million domains is evidence of pent up demand in the marketplace for good, descriptive domain names. We expect that our marketing strategies will result in a new branded and available option that will emotionally connect with potential users and allow them to differentiate

themselves through the use of a branded premium domain.

We will also follow the same ICANN rules and distribution methods of major gTLDs thereby ensuring Registrars and Resellers do not have to change their systems to distribute the .WEB domain. As our systems are already integrated with largest registrars in the world and we have implemented industry best practices, the transition to delegation and launch should be seamless to the registrar channel as well as consumers.

We will also implement a thick whois and adopt any ICANN recommendations or requirements in the future. In order to protect the privacy of our users, we will allow the use of Privacy or Proxy registrations by reputable registrars that comply with applicable policies specified by ICANN. We find this service is highly valuable for registrants that want to ensure their information is not available online and would like to maintain a higher level privacy.

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

### 18.3 .WEB operating rules to benefit consumers

We plan to follow all ICANN policies, including the best practices and recommendations for gTLDs. This will allow us to ensure end-users, have an easy way to register/purchase, administer, and use their domains. Adopting these policies will also prevent malicious behavior by third parties and ensure a smooth operation of the domain. The plans for the launch will be similar to the launch process used in .CO, which included:

- Gradual Offering Plan: The .CO launch included a very comprehensive gradual opening plan that both protected trademarks and provided transparency to end users. The launch was lauded by ICANN for its comprehensiveness and management. For the launch of .WEB we will follow ICANN's policies especially as it relates to the Trademark Clearinghouse which was similar to the process we used for .CO:

-

o Sunrise: Provide a period of a few weeks to allow the TM and IP community to register their .WEB domains prior to the opening to the public. Trademark validations will be done by the Trademark Clearinghouse or as specified by ICANN in their policies. If there are multiple validated applications, these would go to auction and allocated based on these results.

o Landrush: Provide a period of a few weeks to allow domain investors and others that are interested in premium domains to apply for these domains. Once the period of the Landrush phase is over, a process to check the applications will determine if these were unique or if there were multiple applicants. If single applicants, then the domain is awarded at that time. If multiple applicants then the domain would go to an auction in which all applicants would be able to participate. For .CO this process included close to 30,000 applications and the resulting auctions were managed by Pool.com. The process was very successful managing to allocate very efficiently domains according to their perceived value by applicants and bidders at the resulting auctions.

- General Availability: For .CO we had 100k registrations in the first 10 minutes and we didn't have a single issue nor service degradation through the launch or afterwards. We achieved this through a combination of strong planning between our partners, especially Neustar our back-end provider; communication with our Registrars prior and during the launch in a very structured way; strong infrastructure planning and provisioning; and effective load, contingency, and disaster recovery planning. We plan to use similar methods for the launch of .WEB.

o First come first serve during GA and afterwards, which we believe is the best mechanism to ensure a fair allocation of domains once the domain has been launched.

- o Use of UDRP and any other best-practices in rights protection mechanisms
- o Highly managed General Availability launch
- Premium Domains: We will keep some domains for premium sales and these will be restricted prior to the Gradual Offering Plan begins, but can be applied for during the Sunrise phase. These premium domains will be brokered or sold via auction directly or through an accredited 3rd party. With .CO we used this mechanism as a way to allocate high value domains and also to promote the usage of the domain by high profile companies including Twitter with t.co, Google with g.co, Startup America with s.co, as well as a myriad of smaller startups and other endorsements.

## 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.

In preparation for answering this question, NU DOTCO, LLC (NU.CO) reviewed the following relevant background material regarding the protection of geographic names in the DNS, including:

- ICANN Board Resolution 01-92 regarding the methodology developed for the reservation and release of country names in the .INFO top-level domain (see <http://www.icann.org/en/minutes/minutes-10sep01.htm>);
- ICANN's Proposed Action Plan on .INFO Country Names (see <http://www.icann.org/en/meetings/montevideo/action-plan-country-names-09oct01.htm>);
- "Report of the Second WIPO Internet Domain Name Process: The Recognition and Rights and the Use of Names in the Internet Domain Name System," Section 6, Geographical Identifiers (see <http://www.wipo.int/amc/en/processes/process2/report/html/report.html>);
- ICANN's Governmental Advisory Committee (GAC) Principles Regarding New gTLDs, (see [https://gacweb.icann.org/download/attachments/1540128/gTLD\\_principles\\_0.pdf?version=1&modificationDate=1312358178000](https://gacweb.icann.org/download/attachments/1540128/gTLD_principles_0.pdf?version=1&modificationDate=1312358178000)); and
- ICANN's Generic Names Supporting Organization (GNSO) Reserved Names Working Group - Final Report (see <http://gns0.icann.org/issues/new-gtlds/final-report-rn-wg-23may07.htm>).

#### Initial Reservation of Country and Territory Names

NU.CO is committed to initially reserving the country and territory names contained in the internationally recognized lists described in Article 5 of Specification 5 attached to the New gTLD Applicant Guidebook at the second level and at all other levels within the .WEB gTLD at which domain name registrations will be provided. Specifically, NU.CO will reserve:

- The short form (in English) of all country and territory names contained on the ISO 3166-1 list, as updated from time to time, including the European Union, which is exceptionally reserved on the ISO 3166-1 list, and its scope extended in August 1999 to any application needing to represent the name European Union (see [http://www.iso.org/iso/support/country\\_codes/iso\\_3166\\_code\\_lists/iso-3166-](http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166-)



1\_decoding\_table.htm#EU);

- The United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World; and
- The list of United Nations member states in six official United Nations languages prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names.

#### Potential Future Release of Two Character Names

While NU.CO foresees no immediate need for plans to make use of these initially reserved country names at the second level within the .WEB namespace, NU.CO recognizes that there has been several successful and non-misleading use of country names by new gTLD operators as evidenced below:

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

UK.COOP - Is operated by Co-operatives UK the national trade body that campaigns for co-operation and works to promote, develop and unite co-operative enterprises within the United Kingdom.

NZ.COOP - Is operated by the New Zealand Cooperatives Association which brings together the country's cooperative mutual business in a not-for-profit incorporated society.

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

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

The more likely request by NU.CO will come in connection with the un-reservation and allocation of two-letter .WEB domain names, e.g. US.WEB, UK.WEB, etc. If NU.CO should decide in the future to attempt and allocate these domain names, it would submit the proper Registry Service Evaluation Processes (RSEP) with ICANN. In evaluating similar RSEP requests that have been submitted to ICANN by other gTLD registry operators, NU.CO believes that its request would be favorably granted.

#### Creation and Updating the Policies

NU.CO is committed to continually reviewing and updating when necessary its policies in this area. Consistent with this commitment, NU.CO intends to remain an active participant in any ongoing ICANN policy discussion regarding the protection of geographic names within the DNS.

## Registry Services

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

### 23.1 Introduction

NU DOTCO LLC has elected to partner with NeuStar, Inc ("Neustar") to provide back-end services for the .WEB registry. In making this decision, NU DOTCO LLC recognized that Neustar already possesses a production-proven registry system that can be quickly deployed and smoothly operated over its robust, flexible, and scalable world-class infrastructure. The existing registry services will be leveraged for the .WEB 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. NU DOTCO LLC will use Neustar's Registry Services platform to deploy the .WEB registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to .WEB):

- 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 .WEB 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

NU DOTCO LLC 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 .WEB. The service provides supports for near real-time dynamic updates. The design and construction is agnostic with regard to data display policy is flexible enough to accommodate any data model. In addition, a searchable WHOIS service that complies with all ICANN requirements will be provided. The following WHOIS options will be provided:

Standard WHOIS (Port 43)  
Standard WHOIS (Web)  
Searchable WHOIS (Web)

#### 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

NU DOTCO LLC 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 .WEB 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

NU DOTCO LLC, 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

NU DOTCO LLC will not be offering services that are unique to .WEB.

#### 23.4 Security or Stability Concerns

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

## Demonstration of Technical & Operational Capability

### 24. Shared Registration System (SRS) Performance

#### 24.1 Introduction

NU DOTCO LLC has partnered with NeuStar, Inc ("Neustar"), an experienced TLD registry operator, for the operation of the .WEB 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 .WEB 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, NU DOTCO LLC 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 initiate a TLS handshake session with the EPP server.
- The registrar's host must provide credentials to determine proper access levels.
- The registrar's IP address must be preregistered in the network firewalls and traffic-shapers.

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

Figure 24-1 attached 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 .WEB 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 .WEB.

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 .WEB 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 attached.

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 .WEB 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 .WEB 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 .WEB registry.

## 25. Extensible Provisioning Protocol (EPP)

### 25.1 Introduction

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

### 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 attached, 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 attached. 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 .WEB 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 attached provides a list of extensions developed for other TLDs. Should the .WEB 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 .WEB registry is attached in the document titled "EPP Schema Files."

#### 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 .WEB registry.

## 26. Whois

### 26.1 Introduction

.WEB 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. .WEB's back-end registry services provider, Neustar, has extensive experience providing ICANN and RFC-compliant WHOIS services for each of the TLDs that it operates both as a Registry Operator for gTLDs, ccTLDs and back-end registry services provider. As one of the first "thick" registry operators in the gTLD space, Neustar's WHOIS service has been designed from the ground up to display as much information as required by a TLD and respond to a very stringent availability and performance requirement.

Some of the key features of .WEB's solution include:

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

## 26.2 Software Components

The WHOIS architecture comprises the following components:

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

## 26.3 Compliance with RFC and Specifications 4 and 10

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

Table 26-1 attached 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.WEB). 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 attached 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%, less than or equal to 60 minutes. Please note that Neustar's current architecture is built towards the stricter SLAs (95%, less than or equal to 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 attached 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 .WEB 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 .WEB registry. The resources are more than adequate to support the WHOIS needs of all the TLDs operated by Neustar, including the .WEB registry.

## 27. Registration Life Cycle

### 27.1 Registration Life Cycle

#### 27.1.1 Introduction

.WEB will follow the lifecycle and business rules found in the majority of gTLDs today. Our back-end operator, Neustar, has over ten years of experience managing numerous TLDs that utilize standard and unique business rules and lifecycles. This section describes the business rules, registration states, and the overall domain lifecycle that will be use for .WEB.

#### 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 .WEB registry per the defined .WEB 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 .WEB 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 .WEB 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 .WEB registry.
- Hold - Removes the domain from the DNS zone.
- UpdateProhibited - Prevents the object from being modified by an Update command.
- TransferProhibited - Prevents the object from being transferred to another Registrar by the Transfer command.
- RenewProhibited - Prevents a domain from being renewed by a Renew command.
- DeleteProhibited - Prevents the object from being deleted by a Delete command.

The lifecycle of a domain begins with the registration of the domain. All registrations must follow the EPP standard. 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 is 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 .WEB 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 .WEB will follow that term restriction. 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 attached 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 27.2 for detailed descriptions 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 serverTransferProhibited 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 with NU DOTCO LLC 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 .WEB 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 .WEB registry.

## 28. Abuse Prevention and Mitigation

### 28.1 Abuse Prevention and Mitigation

Strong abuse prevention of a new gTLD is an important benefit to the internet community. .WEB and its registry operator and back-end registry services provider, Neustar agree that a registry must not only aim for the highest standards of technical and operational competence, but also needs to act as a steward of the space on behalf of the Internet community and ICANN in promoting the public interest. Neustar brings extensive experience establishing and implementing registration policies. This experience will be leveraged to help .WEB 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, NU DOTCO LLC'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 .WEB's registry provider, Neustar is at the forefront of the prevention of such abusive practices and is one of the few registry operators to have actually developed and implemented an active "domain takedown" policy. We also believe that a strong program is essential given that registrants have a reasonable expectation that they are in control of the data associated with their domains, especially its presence in the DNS zone. Because domain names are sometimes used as a mechanism to enable various illegitimate activities on the Internet often the best preventative measure to thwart these attacks is to remove the names completely from the DNS before they can impart harm, not only to the domain name registrant, but also to millions of unsuspecting Internet users.

Removing the domain name from the zone has the effect of shutting down all activity associated with the domain name, including the use of all websites and e-mail. The use of this technique should not be entered into lightly. .WEB has an extensive, defined, and documented process for taking the necessary action of removing a domain from the zone when its presence in the zone poses a threat to the security and stability of the infrastructure of the Internet or the registry.

#### 28.1.2 Abuse Point of Contact

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

.WEB 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 NU DOTCO LLC 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 .WEB.

##### 28.2.1 .WEB Acceptable Use Policy

This Acceptable Use Policy gives the Registry the ability to quickly lock, cancel, transfer or take ownership of any .WEB 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 .WEB'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, .WEB can meet its obligations under Section 2.8 of the Registry Agreement where required to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its TLD. The Registry will respond to legitimate law enforcement inquiries within one business day from receiving the request. Such response shall include, at a minimum, an acknowledgement of receipt of the request, Questions or comments concerning the request, and an outline of the next steps to be taken by .WEB for rapid resolution of the request.

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

#### 28.2.3 Monitoring for Malicious Activity

.WEB's partner, Neustar is at the forefront of the prevention of abusive DNS practices. Neustar is one of only a few registry operators to have actually developed and implemented an active "domain takedown" policy in which the registry itself takes down abusive domain names.

Neustar's approach is quite different from a number of other gTLD Registries and the results have been unmatched. Neustar targets verified abusive domain names and removes them within 12 hours regardless of whether or not there is cooperation from the domain name registrar. This is because Neustar has determined that the interest in removing such threats from the consumer outweighs any potential damage to the registrar/registrant relationship.

Neustar's active prevention policies stem from the notion that registrants in the TLD 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, including malware, bot command and control, pharming, and phishing, the best preventative measure to thwart these attacks is often 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.

##### 28.2.3.1 Rapid Takedown Process

Since implementing the program, Neustar has developed two basic variations of the process. The more common process variation is a light-weight process that is triggered by "typical" notices. The less-common variation is the full process that is triggered by unusual notices. These notices tend to involve the need for accelerated action by the registry in the event that a complaint is received by Neustar which alleges that a domain name is being used to threaten the stability and security of the TLD, or is part of a real-time investigation by law enforcement or security researchers. These processes are described below:

##### 28.2.3.2 Lightweight Process

In addition to having an active Information Security group that, on its own initiatives, seeks out abusive practices in the TLD, Neustar is an active

member in a number of security organizations that have the expertise and experience in receiving and investigating reports of abusive DNS practices, including but not limited to, the Anti-Phishing Working Group, Castle Cops, NSP-SEC, the Registration Infrastructure Safety Group and others. Each of these sources are well-known security organizations that have developed a reputation for the prevention of harmful agents affecting the Internet. Aside from these organizations, Neustar also actively participates in privately run security associations whose basis of trust and anonymity makes it much easier to obtain information regarding abusive DNS activity.

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

Once the complaint has been reviewed and the alleged abusive domain name activity is verified to the best of the ability of the CERT Team, the sponsoring registrar is 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-hNeustar's period (i.e., is unresponsive to the request or refuses to take action), Neustar places 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.

#### 28.2.3.3 Full Process

In the event that Neustar receives a complaint which claims that a domain name is being used to threaten the stability and security of the TLD or is a part of a real-time investigation by law enforcement or security researchers, Neustar follows a slightly different course of action.

Upon initiation of this process, members of the CERT Team are paged and a teleconference bridge is immediately opened up for the CERT Team to assess whether the activity warrants immediate action. If the CERT Team determines the incident is not an immediate threat to the security and the stability of critical internet infrastructure, they provide documentation to the Neustar Network Operations Center to clearly capture the rationale for the decision and either refers the incident to the Lightweight process set forth above. If no abusive practice is discovered, the incident is closed.

However, if the CERT TEAM determines there is a reasonable likelihood that the incident warrants immediate action as described above, a determination is made to immediately remove the domain from the zone. As such, Customer Support contacts the responsible registrar immediately to communicate that there is a domain involved in a security and stability issue. The registrar is provided only the domain name in Question and the broadly stated type of incident. Given the sensitivity of the associated security concerns, it may be important that the registrar not be given explicit or descriptive information in regards to data that has been collected (evidence) or the source of the complaint. The need for security is to fully protect the chain of custody for evidence and the

source of the data that originated the complaint.

#### 28.2.3.3.1 Coordination with Law Enforcement & Industry Groups

One of the reasons for which Neustar was selected to serve as the back-end registry services provider by .WEB is Neustar's extensive experience with its industry-leading abusive domain name and malicious monitoring program and its close working relationship with a number of law enforcement agencies, both in the United States and internationally. For example, in the United States, Neustar is in constant communication with the Federal Bureau of Investigation, US CERT, Homeland Security, the Food and Drug Administration, and the National Center for Missing and Exploited Children.

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

With the assistance of Neustar as its back-end registry services provider, .WEB can meet its obligations under Section 2.8 of the Registry Agreement where required to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its TLD. .WEB and/or Neustar 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 .WEB and/or Neustar for rapid resolution of the request.

In the event such request involves any of the activities which can be validated by .WEB and/or Neustar 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), Neustar places 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 .WEB 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 Measures to Promote WHOIS Accuracy

.WEB acknowledges that ICANN has developed a number of mechanisms over the past decade that are intended to address the issue of inaccurate WHOIS information. Such measures alone have not proven to be sufficient and therefore .WEB will put forth additional efforts to address this by undertaking the following measures:

- 1) A mechanism a procedures to address domain names with inaccurate or incomplete WHOIS data
- 2) Policies and Procedures to ensure compliance including include audits

- Mechanism to address with inaccurate WHOIS data: a procedure whereby third parties can submit complaints directly to the Applicant (as opposed to ICANN or the sponsoring Registrar) about inaccurate or incomplete WHOIS data. Such information shall be forwarded to the sponsoring Registrar, who shall be required to address those complaints with their registrants. Thirty days after forwarding the complaint to the registrar, .WEB will examine the current WHOIS data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or there was some other disposition. If the Registrar has failed to take any action, or it is clear that the Registrant was either unwilling or unable to correct the inaccuracies, Applicant reserves the right to suspend the applicable domain name(s) until such time as the Registrant is able to cure the deficiencies.

- Policies and Procedures to ensure compliance: .WEB shall on its own initiative, no less than twice per year, perform a manual review of a random sampling of .WEB domain names to test the accuracy of the WHOIS information. Although this will not include verifying the actual information in the WHOIS record, .WEB will be examining the WHOIS data for prima facie evidence of inaccuracies. In the event that such evidence exists, it shall be forwarded to the sponsoring Registrar, who shall be required to address those complaints with their registrants. Thirty days after forwarding the complaint to the registrar, the Applicant will examine the current WHOIS data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or there was some other disposition. If the Registrar has failed to take any action, or it is clear that the Registrant was either unwilling or unable to correct the inaccuracies, .WEB reserves the right to suspend the applicable domain name(s) until such time as the Registrant is able to cure the deficiencies.

#### 28.5 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 .WEB registry.

## 29. Rights Protection Mechanisms

### 29.1 Rights Protection Mechanisms

NU DOTCO LLC 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. .WEB 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 .WEB's selection of Neustar 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, .WEB will implement the following rights protection mechanisms in accordance with the Applicant Guidebook as further described below:

- Trademark Clearinghouse: a one-stop shop so that trademark holders can protect their trademarks with a single registration.
- Sunrise and Trademark Claims processes for the TLD.
- Implementation of the Uniform 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, .WEB 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, .WEB's back-end registry services provider is actively participating in the IAG to ensure that the protections afforded by the clearinghouse and associated RPMs are feasible and implementable.

Utilizing the trademark clearinghouse, all operators of new gTLDs must offer: (i) a sunrise registration service for at least 30 days during the pre-launch phase giving eligible trademark owners an early opportunity to register second-level domains in new gTLDs; and (ii) a trademark claims service for at least the first 60 days that second-level registrations are open. The trademark claim service is intended to provide clear notice" to a potential registrant of the rights of a trademark owner whose trademark is registered in the clearinghouse.

.WEB'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 .WEB.

#### 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 .WEB 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. 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 24 hours of receipt of the complaint from the URS Provider to restrict all changes to the registration data, including transfer and deletion of the domain names.

In addition, in the event of a determination in favor of the complainant, the registry is required to suspend the domain name. This suspension remains for the balance of the registration period and would not resolve the original website. Rather, the nameservers would be redirected to an informational web page provided by the URS Provider about the URS. Additionally, the WHOIS reflects that the domain name will not be able to be transferred, deleted, or modified for the life of the registration. Finally,



there is an option for a successful complainant to extend the registration period for one additional year at commercial rates.

.WEB is fully aware of each of these requirements and will have the capability to implement these requirements for new gTLDs. In fact, during the IRT's development of the URS, Neustar began examining the implications of the URS on its registry operations and provided the IRT with feedback on whether the recommendations from the IRT would be feasible for registries to implement.

Although there have been a few changes to the URS since the IRT recommendations, Neustar continued to participate in the development of the URS by providing comments to ICANN, many of which were adopted. As a result, Neustar is committed to supporting the URS for all of the registries that it provides back-end registry services.

#### 29.1.3 Implementation of Thick WHOIS

The .WEB 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, NU DOTCO LLC will implement a number of measures to handle complaints regarding the abusive registration of domain names in its TLD as described in .WEB's 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. .WEB'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

.WEB 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.

### 29.3 Resourcing Plans

The rights protection mechanisms described in the response above involve a wide range of tasks, procedures, and systems. The responsibility for each mechanism varies based on the specific requirements. In general the development of applications such as sunrise and IP claims is the responsibility of the Engineering team, with guidance from the Product Management team. Customer Support and Legal play a critical role in enforcing certain policies such as the rapid suspension process. These teams have years of experience implementing these or similar processes.

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

- Development/Engineering - 19 employees
- Product Management- 4 employees
- Customer Support - 12 employees

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

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

### 30.(a).1 Security Policies

NU DOTCO LLC and our back-end operator, Neustar recognize the vital need to secure the systems and the integrity of the data in commercial solutions. The .WEB 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 CIS (Center for Internet Security). 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 .WEB 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 .WEB
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 .WEB 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 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 .WEB. 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).5 below.

#### 30.(a).5 Commitments and Security Levels

The .WEB 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.(b) 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

© **Internet Corporation For Assigned Names and Numbers.**



# **Annex 10.**






**gTLD RESPONSE TO STRING CONFUSION OBJECTION**

The named Applicant hereby submits the following response to the objection filed by Web.com Group, Inc. for resolution, under the rules of the NEW gTLD Dispute Resolution Procedures. This document and associated submissions were sent to the following addresses : <sup>Contact Information Redacted</sup>, DRfiling@icann.org;  
Contact Information Redacted

As required, USD 2,750 were paid to ICDR on 8 May 2013. Evidence of the payment is attached for information.  
**(Attachment 74)**

**Rules and Procedures:** NEW gTLD Dispute Resolution Procedures/ICDR Supplementary Procedures for String Confusion Objections

**Party Information**

Name of Applicant: Vistaprint Limited	Name of Objector: Web.com Group, Inc.
Address: Contact Information Redacted	Address: Contact Information Redacted
City, State/Province, Country, Postal Code: Contact Information Redacted	City, State/Province, Country, Postal Code: Contact Information Redacted
Telephone: Email Address: Contact Information Redacted	Telephone: Email Address: Contact Information Redacted
Name of Applicant's Attorney or Representative: Flip Petillion	Name of Objector's Attorney or Representative: Steven C. Sereboff
Name of Firm (if applicable): Crowell & Moring	Name of Firm (if applicable): SoCal IP Law Group LLP
Address: Contact Information Redacted	Address: Contact Information Redacted
City, State/Province, Country, Postal Code: Contact Information Redacted	City, State/Province, Country, Postal Code: Contact Information Redacted
Telephone: Email Address: Contact Information Redacted	Telephone: Email Address: Contact Information Redacted
Signature:  Attorney-at-law, 23 May 2013	

## I. The Parties

### A. The Applicant

Through its subsidiary, Webs Inc., the Applicant (also Respondent) provides free website creation tools and hosting services. Additional paid features are offered (Attachment 1).

At present, the Applicant conducts its business using a website that is accessible via the domain name 'webs.com'. The 'webs.com' domain name was registered on April 4, 1995 (Attachment 2).

'Webs' is the mark under which the Applicant brands its products and services.

Webs' clients are predominantly non-US clients (54% non-US, 46% US) (Attachment 3).

### B. The Objector

The Objector primarily provides web site development services to small and medium businesses and conducts its business using a website that is accessible via the domain name 'web.com' (Attachment 4). The 'web.com' domain name was registered on July 2, 1996 (Attachment 5).

The Objector uses the mark 'Web.com' for which it has two U.S. trademark registrations (Attachment 6).

Web.com's clients are primarily US based (Attachment 7).

## II. Factual background

### A. The Objector and the Applicant have co-existed for many years without any problem

#### 1. The WEBS.COM and WEB.COM domain names have been used and coexisting in the market for many years

The 'webs.com' domain name was created on April 5, 1995 (Attachment 2), more than a year before the creation of the 'web.com' domain name on July 2, 1996 (Attachment 5).

Both 'webs.com' and 'web.com' domain names have been used simultaneously for more than 16 years. The two domain names have co-existed, and significant and distinct businesses have thrived under these separate names, with each business possessing its own independent identity and goodwill.

#### 2. The Parties have never initiated any case against each other

Neither the Applicant nor the Objector have ever litigated over the others use of their respective mark and domain name.

**3. The Applicant's use of the WEBS.COM domain name has never been the subject of any lawsuit**

The Applicant's use of the 'webs.com' domain name has never been questioned by a party in court or in a UDRP case.

**4. The Objector's use of the WEB.COM domain name has never been the subject of any law suit**

In so far as the Applicant is aware, the Objector's use of the WEB.COM domain name has never been questioned by a party in court or in a UDRP proceeding.

**B. Both the Applicant and the Objector have filed an application for a new generic Top Level Domain**

The Applicant has applied for the string .WEBS (standard and community application) with a view to consolidating the reputation of the Applicant's website creation tools and hosting services, known under the identifier 'WEBS' and the community it represents. The use of the 'WEBS' identifier is aimed at making it unambiguous that the TLD is related to the Applicant (**Attachments 8 and 9**)

The Objector has applied for the string .WEB (**Attachment 10**).

**C. There are 7 applicants for .WEB**

There are 7 applicants for .WEB. Apart from the Objector, an application for .WEB was filed by DotWeb Inc. (AE), Charleston Road Registry Inc., (US), Afilias Domains No. 3 Limited (IE), Ruby Glen, LLC (US), Schlund Technologies GmbH (DE), and NU DOT CO LLC (US) (**Attachment 11-16**).

No other party applied for .WEBS.

**D. The other applicants for .WEB have not filed a string confusion objection**

None of the other 6 applicants for .WEB has filed an objection against the Applicant. It is fair to deduce from this that these applicants either do not share the grounds for the objection filed by the Objector and/or that they did not deem it appropriate to file such an objection on these or other grounds.

### III. The purpose of ICANN's new gTLD program and the limited grounds for objection

On 12 January 2012, ICANN launched its new Generic Top-Level Domain (gTLD or TLD) program, with the goal of “*enhancing competition[,] consumer choice[,] . . . [and] innovation via the introduction of new gTLDs.*”<sup>1</sup> The Applicant filed its application for the string .WEBS, which it intends to use in connection with its free website creation and hosting business. The applied-for .WEBS gTLD will increase competition and benefit Internet users by providing new and different services within an expanded DNS, and thus enhance the goals of ICANN's new gTLD program.<sup>2</sup>

ICANN designed the objection process to protect certain legitimate rights, while also ensuring that objectors could not prevent the delegation of legitimate TLDs. Objections are only permitted on the four specific grounds enumerated in the Guidebook: string confusion, legal rights, community opposition, and limited public interest.<sup>3</sup> Any objection outside these narrow grounds must fail.

Accordingly, it is important to apply the criteria as written, and not in an overbroad way that unnecessarily interferes with the delegation of the applied-for TLD. The Applicant will show that the Objector seeks to use the string confusion objection to limit competition. Such use of the objection proceedings directly conflicts with the purpose of ICANN's new gTLD program.

The Applicant will also show that the objection is not only contrary to the purpose of ICANN's new gTLD program, but also fails to meet the stringent criteria of a legal rights objection.

### IV. The task of the panel expert

#### A. The relevant criterion

The applicable rule has been provided in the AGB, Section 3.5.1. which reads as follows:

*“A DRSP panel hearing a string confusion objection will consider whether the applied-for gTLD string is likely to result in string confusion. String confusion exists where a string so nearly resembles another that it is likely to deceive or cause confusion. For a likelihood of confusion to exist, it must be probable, not merely possible that confusion will arise in the mind of the average, reasonable Internet user. Mere association, in the sense that the string brings another string to mind, is insufficient to find a likelihood of confusion.” (emphasis added)*

The Applicant wishes to point out that the Objector omitted the last sentence when referring to AGB, Section 3.5.1. (Objection, p. 3). However, as will be demonstrated below, this sentence is quite relevant for this case.

<sup>1</sup> About the Program: ICANN New gTLDs, available at <http://newgtlds.icann.org/en/about/program>.

<sup>2</sup> About the Program: ICANN New gTLDs, available at <http://newgtlds.icann.org/en/about/program> (“The program's goals include enhancing competition and consumer choice, and enabling the benefits of innovation via the introduction of new gTLDs.”).

<sup>3</sup> *Id.*, Module 3.2.1.

## B. Difference with the task of the String Similarity Panel

The evaluation undertaken by the Expert Panel is different from that assigned by ICANN to the String Similarity Panel in the Initial Evaluation.

### 1. The task of the String Similarity Panel

The String Similarity Panel was assigned the task of determining contention sets. The String Similarity Panel was asked to review the entire pool of applied-for strings to determine whether the strings proposed in any two or more applications were so similar that they would create a probability of user confusion if allowed to coexist in the DNS. (AGB, Module 4-3)

The criterion to be used by the String Similarity Panel is defined in the Applicant Guidebook which states:

*“Contention sets are groups of applications containing identical or similar applied-for gTLD strings.”*

[...]

*“‘similar’ means strings so similar that they create a probability of user confusion if more than one of the strings is delegated into the root zone.*

[...]

*The String Similarity Panel will [...] review the entire pool of applied-for strings to determine whether the strings proposed in any two or more applications are so similar that they would create a probability of user confusion if allowed to coexist in the DNS. The panel will make such a determination for each pair of applied-for gTLD strings. The outcome of the String Similarity review described in Module 2 is the identification of contention sets among applications that have direct or indirect contention relationships with one another.*

*Two strings are in direct contention if they are identical or similar to one another.*

[...]

*Two strings are in indirect contention if they are both in direct contention with a third string, but not with one another.” (AGB, Module 4-2, 4-3)*

Module 2 of the Applicant Guidebook also states:

**“Standard for String Confusion** – *String confusion exists where a string so nearly resembles another **visually** that it is likely to deceive or cause confusion. For the likelihood of confusion to exist, it must be probable, not merely possible that confusion will arise in the mind of the average, reasonable Internet user. Mere association, in the sense that the string brings another string to mind, is insufficient to find a likelihood of confusion.” (AGB, Module 2-8)*

## 2. The task of the Expert Panel

The Applicant Guidebook provides in Module 2 that – in contrast with the determination by the String Similarity Panel – a String Confusion Objection brought before an Expert Panel:

“...is **not limited to visual similarity**. Rather, confusion based on any type of similarity (including **visual, aural, or similarity of meaning**) may be claimed by an objector.” (AGB, Module 2-8).

### V. ICANN and its String Similarity Panel do not consider the strings to be confusingly similar

#### A. ICANN’s String Similarity Assessment Tool provides a low similarity rate

In the application period for new gTLDs, ICANN had made accessible a String Similarity Assessment Tool. It is still accessible on <https://icann.sword-group.com/algorithm/Default.aspx>. (Attachment 17)

According to the information published on this website, this tool “*is intended to provide an open, objective, and predictable mechanism for assessing the degree of visual similarity between TLD strings.*”

It allows for the comparison of two strings to each other.

When comparing .WEBS with .WEB, the similarity rate is 72% (Attachment 18) which is much lower than the similarity rate of various TLDs that currently co-exist (Attachments 19-55). E.g., the currently co-existing .LT and .TL strings and .IL and .LI are respectively 93% and 94% similar (Attachments 53-54).

The 72% similarity is also much lower than the 88% similarity between the applied-for .ACCOUNTANTS and .ACCOUNTANT or the 84% similarity between the applied-for .COUPONS and .COUPON (Attachments 56-57). The applicants for these strings did not file a string confusion objection.

Internet users have become used to the existence of TLDs having much more similarity than the claimed similarity between .WEBS and .WEB. For instance, with a similarity rate of 83%, .IO and .JO are considered visually more similar (Attachment 44). Also, in certain languages, from an aural perspective, .IO is virtually identical to .JO. From a conceptual point of view, .IO and .JO are as meaningful, or rather equally meaningless. Nonetheless, this poses no problem for the average Internet user, who is used to small differences between TLDs.

#### B. ICANN has not put the applications for .WEBS and .WEB in a contention set

As mentioned above, in the Initial Evaluation, ICANN assigned a panel called the String Similarity Panel with the task to determine contention sets: The String Similarity Panel was asked to review the entire pool of applied-for strings to determine whether the strings

proposed in any two or more applications were so similar that they would create a probability of user confusion if allowed to coexist in the DNS (AGB, Module 4-3).

The outcome of this assignment was that two contention sets of non-exact matches were created: the set containing .HOTELS and .HOTEIS strings and the set containing the .UNICOM and .UNICORN strings ([Attachment 58](#)).

No other contention sets for non-exact matches in Latin script were created.

This shows that neither the String Similarity Panel nor ICANN (who endorses the determinations by the String Similarity Panel) were of the opinion that the .WEBS and .WEB strings are so similar that they would create a probability of user confusion if allowed to coexist in the DNS.

## VI. The Objector does not consider WEBS and WEB to be confusingly similar

### A. The Objector considers much more similar signs not confusingly similar

Web.com has narrowed the scope of its enforceable trademark rights by entering into a Supplemental Consent to Registration with Verio. The Objector and Verio have agreed that there was no likely confusion between WEB.COM on the one hand, and WEB.COM on the other hand ([Attachment 59](#)).

When entering into the Supplemental Consent, the Objector was of the opinion that “customers understand that you have to use the correct Internet address because a different Internet address will resolve to a different website” and that there is no likelihood of confusion because “[t]he consuming public is sophisticated enough” ([Attachment 59](#)). The Objector also indicated that the parties have enjoyed long coexistence without any known instances of actual confusion.

Therefore, it is impossible to understand how the Objector can agree to coexistence between WEB.COM and WEB.COM and yet object to a coexistence between WEB and WEBS. Indeed:

- The letter ‘S’ is much more distinctive than the symbol ‘.’;
- The dot is placed in the middle of the WEB.COM sign, making it much more likely to be overlooked than the last letter of a word, which (together with the first letter) has been shown to be more significant than the rest of the letters (*infra*);
- The Applicant and the Objector have also enjoyed long coexistence without any known instances of actual trademark relevant confusion.

### B. The Objector never formally challenged the co-existence between the WEBS.COM and WEB.COM domain names

The Objector has never instituted a formal challenge to the WEBS.COM domain name, which co-exists with the Objector’s WEB.COM domain name for years. Whereas the letter ‘S’ in ‘WEBS.COM’ makes ‘WEBS.COM’ clearly differ from ‘WEB.COM’, the difference

between a 'WEBS' TLD and a 'WEB' TLD is even greater. As a TLD will always come at the end of the domain name syntax, the distinctive letter 'S' will always appear at the end, making this last letter more significant .

## VII. There is no overall similarity

The difference between the .WEBS and .WEB strings is grounded in the character 'S' present in the first and not part of the second. In linguistic terms, the character 'S' is manifestly distinct.

The Applicant asked an independent expert to provide his views on the following questions:

- 1) Regardless of the ICANN framework, would you consider both strings to be confusing?
- 2) Given the ICANN framework, would you consider both strings confusing based on any of the following types of similarity: visual, aural or similarity of meaning?

The expert to whom this request was addressed, Professor Piet Desmet, is full professor at the University of Leuven in linguistics and language teaching methodology (Attachment 60).

Professor Desmet from the University of Leuven has made the following findings:

1. Exterior letters serve as visual clues for word recognition. The first and last letters of a word have been shown to be more salient than the rest of the letters and to receive priority in processing. Readers can recognize a word even when its interior letters are scrambled.

Professor Desmet concludes that 'webs' and 'web' are recognized as two radically different words since their last letters are completely different.

2. In the case of 'web' and 'webs', completely regular patterns allow for a one-to-one mapping of spelling to sound. In other words, a word that consists of completely regular patterns is spelled out exactly as it sounds. The sound of the word easily translates into the spelling of the word and *vice versa*. Words consisting of completely regular patterns facilitate word recognition.

Professor Desmet considers that 'webs' and 'web' have completely regular patterns allowing for one-to-one mapping of spelling to sound, which highly facilitates the word recognition of both words.

3. Third, there is an extremely limited number of words that could be generated by changing only one single letter in 'webs' and 'web'. In other words, 'webs' and 'web' have a limited number of orthographic neighbors. Words with a high number of orthographic neighbors are more difficult to recognize and have an inhibitory effect when reading, as evidenced by eye-fixation patterns. Words with fewer orthographic neighbors are more easily recognizable.



Professor Desmet concludes that this results in a higher word recognition for 'webs' and 'web' which have a limited number of orthographic neighbors.

4. Fourth, a reader will first decompose the word 'webs' into meaningful units. 'Webs' is composed of two meaningful units, namely 'web' and the plural marker '-s'. 'Web' only has one meaningful unit.

For professor Desmet, this is an extra factor that enhances the ability to recognize the difference between 'web' and 'webs'.

5. Also, the plural '-s' is a completely regular plural and easily recognizable compared to irregular plurals (e.g. with vowel change such as 'hero'/'heroes') that have been proven to be less easily recognizable.

In conclusion, Professor Desmet considers the 5 elements above reason enough to dismiss the idea of string confusion in the case of 'webs'/'web'.

### VIII. The strings are visually different

The two strings .WEBS and .WEB are visually distinct.

A number of different trademark offices provide guidance on how to interpret confusion. For example, the European Union Trade Mark Office provides guidance on how to interpret confusion. Its *Manual concerning opposition* was used by the GNSO<sup>4</sup> when it suggested language for the Applicant Guidebook of ICANN. The Manual lays down a couple of relevant principles that apply in the case at instance:

*"The visual comparison is based on an analysis of the number and sequence of the letters, the number of words and the structure of the signs." (Attachment 61, p. 10, section 3.2)*

*"The length of a name may influence the effect of differences. The shorter a name, the more easily the public is able to perceive all its single elements. Thus, small differences may frequently lead in short words to a different overall impression. In contrast, the public is less aware of differences between long names." (Attachment 61, p. 22, section 4.2)*

Visually, the 'S' is a clear differentiator because it is positioned at the end of the short word (which gives it priority in the processing of word recognition) and it has the function to indicate the plural, which is a regular plural. This is confirmed by the findings of Professor Desmet mentioned above.

The difference is sufficiently clear not to cause any confusion, mistake or deception, as is made clear by the longstanding coexistence between the domain names WEBS.COM and WEB.COM.

---

<sup>4</sup> ICANN's Generic Names Supporting Organization ; see <http://gns0.icann.org/en/>

### IX. The strings are aurally different

Also aurally, the strings are different. As evidenced by the findings of Professor Desmet, both 'webs' and 'web' consist of completely regular patterns and are spelled out exactly as they sound. In other words, all letters are clearly pronounced in both words, which makes the words clearly recognizable and distinct from one another.

Indeed, the sound of the letter 's' is clearly stressed in 'webs' and is not present in the word 'web'. Individuals are perfectly capable of distinguishing the sound that is generated by adding the letter 's' to a word with similar endings as the word 'web'. *E.g.*, individuals are perfectly capable of distinguishing 'step' from 'steps', 'car' from 'cars' or 'sales rep' from 'sales reps'.

Hence, also from an aural perspective, 'webs' is clearly different and distinguishable from 'web'.

### X. The strings have a different meaning

The strings have a different meaning. 'Web' refers to the world wide web or to a network or silken structure created by a spider (**Attachment 62**), whereas 'webs' has no particular meaning and could be anything. On Wikipedia, 'webs' is used for the Applicant's web hosting services, a radio station and a 2003 sci-fi movie (**Attachment 63**). 'Web' on the other hand has a clear dictionary meaning (**Attachment 64**).

In any event, as mentioned above, the Applicant Guidebook expressly provides that mere association, in the sense that the string brings another string to mind, is insufficient to find a likelihood of confusion (AGB, Section 3.5.1.).

As also explained above, the mission and purpose of the Applicant .WEBS gTLD is to consolidate the reputation of the Applicant's hosting services, known under the identifier 'WEBS' and the community it represents and to ensure that the .WEBS top-level domain will be unambiguous as regards the identity of the Registry Operator.

This purpose is in diametric opposition to the mission and purpose of the Objector's .WEB gTLD, which is to "become the most versatile gTLD on the World Wide Web" and to "quickly become as ubiquitous" and to "serve everyone, from commerce to information to community-building" (**Attachment 10**, response to evaluation question 18).

As a result, the services offered under .WEBS and .WEB will clearly distinguish themselves.

### XI. The real objective of the Objector

During the Objector's first quarter 2013 earnings conference call, the Objector stated that it is certainly interested in getting the .WEB gTLD, but that it's not its core business. The objector said that it will "be perfectly content if anyone gets .web because they are going to distribute it through [the Objector] and it [i]s [their] name and [the Objector is] advertising and building a brand in the marketplace and [is] going to be a great deliverer of .web extensions, whoever gets it; whether it's [the Objector] or someone else" (**Attachment 65**, p. 13). The Objector pointed out that its strategy has always been to cooperate and that they have

looked at the people who have applied for .web and that it is talking to all of them about who would benefit from this and which team would be the best team to provide services.

While the Objector is in contention with multiple applicants for .WEB, the Applicant is not in contention with any other applicant for .WEBS. The Objector has realized that it faces a challenge in obtaining the delegation of the .WEB extension, while the Applicant does not face a similar challenge in dealing with other applicants. With the present objection, the Objector is trying to give the Applicant the same challenge.

The Objector's sole motive in filing the objection is to prevent a potential competitor, who does not have the intention to create goodwill in the Objector's name, from entering the gTLD market. Such intent, to limit competition, is clearly contrary to the purpose of ICANN's new gTLD program.

As mentioned above, no other applicant for .WEB shared the views of the Objector as none of them were of the opinion that there were reasons to file an objection against the Applicant.

## **XII. The Objector's position is incoherent**

The Objector argues that the vast majority of Internet users are non-native English speakers and that non-English speakers commonly confuse plural and singular word forms or omit the plural altogether.

The Objector does not produce any evidence in support of this argument.

Also, how can the Objector (without any evidence) know what a non-native English speaker sees and not, or what he distinguishes and what she does not?

As mentioned above, the first and last letters of a word are in combination visual clues for a word, making words more recognizable. The way individuals recognize words is not related to being a native speaker or not, but is connected to the functioning of the human brain (**Attachment 60**).

## **XIII. The Objector's allegations are unfounded**

### **A. The comparison with UDRP cases is irrelevant for this case**

The UDRP cases referred to by the Objector are all cases between a registrant of a domain name and the holder of a trade mark.

In the present case the question whether one or both of the names is related to a trademark is irrelevant. The present case is not a case about the violation of a trademark. Even if it were, "*the mark .WEB used in relation to Internet registry services is generic and cannot enjoy trademark protection*" (See *Image Online Design, Inc. v ICANN*, Case No. CV 12-08968 DDP (US District Court of California, 7 Feb. 2013), **Attachment 66**, p. 16).

And even if UDRP cases were relevant, UDRP cases relating to generic terms contradict the findings in the cases produced by the Objector. Examples include:

- Mansion (Gibraltar) Limited and Provent Holdings Ltd. v. Agens PSC, WIPO Case No. D2010-0584 (finding that “since “casino” is a well-known generic term, small visual and sound modifications are, in this Panel’s view, very obvious and are more easily remembered by the human mind.”) (**Attachment 67**).

Tire Discounters, Inc. v. TireDiscounter.com, NAF Case No. FA0604000679485 (finding that “[b]ecause the mark is merely descriptive, small differences matter. In the Internet context, consumers are aware that domain names for different websites are often quite similar and that small differences matter. See Entrepreneur Media, Inc. v. Smith, 279 F.3d 1135, 1147 (9<sup>th</sup> Cir. 2002). The omission of the letter “s” from the mark is one of those small differences that matters in this context. Complainant has failed to meet its burden to establish that Respondent’s <tirediscounter.com> domain name is confusingly similar to Complainant’s mark within the meaning of Policy ¶4(a)(i). See Men’s Warehouse, Inc. v. Wick, FA 117861 (Nat. Arb. Forum Sept. 16, 2002).”) (**Attachment 68**)

## B. There is no (Evidence of) Actual Confusion

The evidence of actual confusion to which the Objector points is exceptionally weak given the long history of coexistence of the WEBS.COM and the WEB.COM domain names and between the Objector and the Applicant’s business. Tens of millions websites have been built with Webs and, together, these sites receive 300 million page views each month (**Attachment 1**). The Objector claims to be helping over 3 million customers with its presence on the web (**Attachment 4**).

In light of the large volume of business conducted through both the Applicant’s and Objector’s websites, minimal instances of misdirected consumer communications are “at best *de minimis*,” and the paucity of evidence of actual confusion in fact creates “a presumption against likelihood of confusion in the future.” *Petro Stopping Centers, L.P. v. James River Petroleum, Inc.*, 130 F.3d 88, 96 (4th Cir. 1997) (citations omitted) (**Attachment 69**).

The Objector does not actually provide details of any of the “abundant evidence” of actual confusion that it alleges in the Objection.

The examples of alleged actual confusion that the Objector has provided through links are examples of typographical errors, not actual confusion. The standard for actual consumer confusion requires a mental state of actual confusion as to the source of two products or services. See 3 *McCarthy on Trademarks* § 23:13 (“[E]vidence of actual confusion is the testimony of a ‘reasonably prudent purchaser’ who was in fact confused by defendant’s trademark.”) (emphasis added); *Checkpoint Systems, Inc. v. Check Point Software Technologies, Inc.*, 104 F. Supp. 2d 427, 464 (D.N.J. 2000) (same), *aff’d* 269 F.3d 270 (3d Cir. 2001). Accordingly, courts have routinely rejected typographical errors as evidence of actual confusion. See, e.g., *Heartsprings, Inc. v. HeartSpring, Inc.*, 949 F. Supp. 1539, 1545 n.4 (D. Kan. 1996) (rejecting typographical error in press release as evidence of actual confusion); *Water Pik, Inc. v. Med-Systems, Inc.*, 2012 WL 224447, at \*7 n.7 (D. Colo. Jan. 25, 2012) (rejecting typographical error in blog entry as evidence of actual confusion) (**Attachment 70-73**).

The only examples of alleged confusion for which the Objector provides citations do not evidence actual confusion. Instead, they appear to be typographical errors on the webs.com forum:

- 1) [http://support.webs.com/webs/topics/web\\_com\\_examples](http://support.webs.com/webs/topics/web_com_examples)

The headline for the topic is "[web.com](#) examples" but immediately under this, the question has the correct reference to [webs.com](#): "Is there really no way/place to see examples of real sites created on [webs.com](#)?"

This is obviously a typographical error and not genuine confusion.

- 2) [http://support.webs.com/webs/topics/can\\_dns\\_be\\_hosted\\_elsewhere\\_and\\_still\\_have\\_a\\_site\\_name\\_web\\_com\\_site\\_work](http://support.webs.com/webs/topics/can_dns_be_hosted_elsewhere_and_still_have_a_site_name_web_com_site_work)

Here the headline refers to [web.com](#) but the question underneath correctly refers to [webs.com](#). Headline: "Can DNS be hosted elsewhere, and still have a [site-name.web.com](#) site work?" Question underneath: "I do not want to transfer my domain registration to [webs.com](#) . . . Is there an IP address I can point our DNS to, to make a [webs.com](#) site work?"

This too, is plainly a typographical error, and not actual confusion.

- 3) [http://support.webs.com/webs/topics/my\\_web\\_com\\_site\\_disappeared](http://support.webs.com/webs/topics/my_web_com_site_disappeared)

Here, the customer is complaining about her '[web.com](#)' site disappearing. She is, however, a registered user of the Webs user forum, and responses to the post and subsequent user posts clearly reference Webs.

Again, this post appears to be a typographical error, not actual confusion.

Also, even if the Applicant were to accept that each of the forums that the Objector cites contained examples of individuals who were actually confused as to the source of a product or service (as opposed to someone who made a typographical error), it would underscore the tiny percentage of consumers who would be affected by that confusion.

A final example of alleged confusion is the case in which the Applicant's CEO and co-founder made a typographical error in a press release by PR.com. This typographical error was quickly corrected after discovering the mistake. Does the Objector truly believe that the Applicant's co-founder and CEO was confused about his own company name?

Finally, the fact that the Attorney General of Kentucky and the Attorney General of Arkansas would have sent a letter by mistake to web.com instead of to webs.com does not prove that the Attorneys General were confused. The Attorney General in Arkansas was provided with the incorrect address in the complaint form, filed by a non-customer. With both the Applicant and the Objector having millions of customers, the fact that only two letters were addressed to the wrong party, shows how limited the likelihood of confusion between 'webs.com' and 'web.com' is. The likelihood of confusion between .WEBS and .WEB is even more limited,

given the fact that the last letter in both words is different (which makes the difference more apparent, as shown above).

### CONCLUSION

As explained above there is no risk of confusion in the mind of the average, reasonable Internet user, nor is such risk probable. Accordingly, there is no likelihood of confusion between the strings .WEB and .WEBS such that the strings should be placed in the same contention set.

The Applicant requests that the objection be declared Unsuccessful and that the Applicant and the Objector both move forward in the process without being considered in direct contention with one another.

Respectfully submitted,



Flip Petillion, Advocaat

Authorized Representative of the Respondent

May 23, 2013

### Attachments

1. Company information on the Applicant and its subsidiary
2. Whois records of <webs.com>
3. Overview of US and non-US clients of the Applicant
4. Company information on the Objector
5. Whois records of <web.com>
6. USPTO Reg. Nos. 2521314 and 3666813
7. Objector's most recent annual report
8. Application No. 1-1033-73917 for gTLD '.webs' by the Applicant
9. Application No. 1-1033-22687 for gTLD '.webs' by the Applicant
10. Application No. 1-1009-97005 for gTLD '.web' by the Objector
11. Application for gTLD '.web' by DotWeb Inc. (AE)
12. Application for gTLD '.web' by Charleston Road Registry Inc., (US)
13. Application for gTLD '.web' by Afiliis Domains No. 3 Limited (IE)

14. Application for gTLD '.web' by Ruby Glen, LLC (US)
15. Application for gTLD '.web' by Schlund Technologies GmbH (DE)
16. Application for gTLD '.web' by NU DOT CO LLC (US)
17. Printout of the website where the String Similarity Assessment Tool is accessible via <https://icann.sword-group.com/algorithm/Default.aspx>
18. Printout of the website where the String Similarity Assessment Tool is used to compare '.webs' with '.web'
19. Printout of the website where the String Similarity Assessment Tool is used to compare .BV and .BY
20. Printout of the website where the String Similarity Assessment Tool is used to compare .BA and .BE
21. Printout of the website where the String Similarity Assessment Tool is used to compare .CU and .CV
22. Printout of the website where the String Similarity Assessment Tool is used to compare .FI and .FR
23. Printout of the website where the String Similarity Assessment Tool is used to compare .AC and .AE
24. Printout of the website where the String Similarity Assessment Tool is used to compare .AW and .AU
25. Printout of the website where the String Similarity Assessment Tool is used to compare .CM and .CN
26. Printout of the website where the String Similarity Assessment Tool is used to compare .CU and .CV
27. Printout of the website where the String Similarity Assessment Tool is used to compare .CV and .CY
28. Printout of the website where the String Similarity Assessment Tool is used to compare .GM and .GN
29. Printout of the website where the String Similarity Assessment Tool is used to compare .TL and .TJ
30. Printout of the website where the String Similarity Assessment Tool is used to compare .IL and .IT
31. Printout of the website where the String Similarity Assessment Tool is used to compare .LU and .LV
32. Printout of the website where the String Similarity Assessment Tool is used to compare .LV and .LY
33. Printout of the website where the String Similarity Assessment Tool is used to compare .PK and .PH
34. Printout of the website where the String Similarity Assessment Tool is used to compare .MV and .MW
35. Printout of the website where the String Similarity Assessment Tool is used to compare .EC and .EE
36. Printout of the website where the String Similarity Assessment Tool is used to compare .IT and .TL
37. Printout of the website where the String Similarity Assessment Tool is used to compare .BI and .BJ
38. Printout of the website where the String Similarity Assessment Tool is used to compare .AI and .AL
39. Printout of the website where the String Similarity Assessment Tool is used to compare .GI and .GL
40. Printout of the website where the String Similarity Assessment Tool is used to compare .LT and .IT

41. Printout of the website where the String Similarity Assessment Tool is used to compare .ME and .MF (UC)
42. Printout of the website where the String Similarity Assessment Tool is used to compare .BE and .BF (UC)
43. Printout of the website where the String Similarity Assessment Tool is used to compare .FI and .FJ
44. Printout of the website where the String Similarity Assessment Tool is used to compare .IO and .JO
45. Printout of the website where the String Similarity Assessment Tool is used to compare .IE and .JE
46. Printout of the website where the String Similarity Assessment Tool is used to compare .SI and .SJ
47. Printout of the website where the String Similarity Assessment Tool is used to compare .SL and .LS
48. Printout of the website where the String Similarity Assessment Tool is used to compare .AU and .UA
49. Printout of the website where the String Similarity Assessment Tool is used to compare .ES and .SE
50. Printout of the website where the String Similarity Assessment Tool is used to compare .TP and .PT
51. Printout of the website where the String Similarity Assessment Tool is used to compare .TG and .GT
52. Printout of the website where the String Similarity Assessment Tool is used to compare .IO and .IQ (UC)
53. Printout of the website where the String Similarity Assessment Tool is used to compare .LT and .TL
54. Printout of the website where the String Similarity Assessment Tool is used to compare .IL and .LI
55. List of all currently existing TLDs, as delegated by IANA
56. Printout of the website where the String Similarity Assessment Tool is used to compare .ACCOUNTANTS and .ACCOUNTANT
57. Printout of the website where the String Similarity Assessment Tool is used to compare .COUPONS and .COUPON
58. Printout of the website with ICANN contention sets for exact and non-exact matches
59. Supplemental Consent to Registration of the Objector with Verio
60. Expert opinion by Professor Dr. Piet Desmet
61. OHIM document on confusion
62. Dictionary meaning of 'web'
63. Wikipedia on 'webs'
64. Wikipedia on 'web'
65. Transcript of Q1 2013 Web.com Group Inc. Earnings Conference Call
66. *Image Online Design, Inc. v ICANN*, Case No. CV 12-08968 DDP (US District Court of California, 7 Feb. 2013)
67. *Mansion (Gibraltar) Limited and Provent Holdings Ltd. v. Agens PSC*, WIPO Case No. D2010-0584
68. *Tire Discounters, Inc. v. TireDiscounter.com*, NAF Case No. FA0604000679485
69. *Petro Stopping Centers, L.P. v. James River Petroleum, Inc.*, 130 F.3d 88, 96 (4th Cir. 1997)
70. *Checkpoint Systems, Inc. v. Check Point Software Technologies, Inc.*, 104 F. Supp. 2d 427, 464 (D.N.J. 2000)
71. *Checkpoint Systems, Inc. v. Check Point Software Technologies, Inc.*, 269 F.3d 270 (3d Cir. 2001)



72. *Heartsprings, Inc. v. Heartspring, Inc.*, 949 F. Supp. 1539, 1545 n.4 (D. Kan. 1996)
73. *Water Pik, Inc. v. Med-Systems, Inc.*, 2012 WL 224447, at \*7 n.7 (D. Colo. Jan. 25, 2012)
74. Proof of payment of filing fee.

## Janssen, Jan

---

**From:** Nelissen, Mariet on behalf of Petillion, Flip  
**Sent:** jeudi 23 mai 2013 16:06  
**To:** Tom Simotas  
**Cc:** DRfiling@icann.org; Contact Information Redacted  
**Subject:** 50 504 T 00221 13 - Response (mail 1 of 4)  
**Attachments:** 3109179\_.WEBS (case 50 504 T 00221 13) Response.PDF

Tracking:	Recipient	Delivery	Read
	Tom Simotas		
	DRfiling@icann.org		
	Contact Information Redacted		
	Contact Information Redacted		
	Petillion, Flip	Delivered: 23/05/2013 16:06	Read: 23/05/2013 16:14
	Janssen, Jan	Delivered: 23/05/2013 16:06	Read: 23/05/2013 16:09

Dear Madam,  
Dear Sir,

Please find attached the Response in case number 50 504 T 00221 13. The Annexes will be sent in three separate mails.

Yours sincerely,

Flip Petillion

**Flip Petillion**  
Partner  
Direct: + Contact Information Redacted | Mobile: Contact Information Redacted

**Crowell & Moring LLP** | [www.crowell.com](http://www.crowell.com)

# Contact Information Redacted

[Firm Bio](#) - [LinkedIn](#)

## Janssen, Jan

---

**From:** Tom Simotas Contact Information Redacted  
**To:** Nelissen, Mariet  
**Sent:** jeudi 23 mai 2013 16:06  
**Subject:** Read: 50 504 T 00221 13 - Response (mail 1 of 4)

Your message

To:  
Subject: 50 504 T 00221 13 - Response (mail 1 of 4)  
Sent: Thursday, May 23, 2013 10:06:30 AM (UTC-05:00) Eastern Time (US & Canada)

was read on Thursday, May 23, 2013 10:06:25 AM (UTC-05:00) Eastern Time (US & Canada).




**gTLD RESPONSE TO STRING CONFUSION OBJECTION**

The named Applicant hereby submits the following response to the objection filed by Web.com Group, Inc. for resolution, under the rules of the NEW gTLD Dispute Resolution Procedures. This document and associated submissions were sent to the following addresses : Contact Information Redacted; DRfiling@icann.org;  
Contact Information Redacted

As required, USD 2,750 were paid to ICDR on 8 May 2013. Evidence of the payment is attached for information.  
**(Attachment 74)**

**Rules and Procedures:** NEW gTLD Dispute Resolution Procedures/ICDR Supplementary Procedures for String Confusion Objections

**Party Information**

Name of Applicant:  Vistaprint Limited	Name of Objector:  Web.com Group, Inc.
Address:  Contact Information Redacted	Address:  Contact Information Redacted
City, State/Province, Country, Postal Code:  Contact Information Redacted	City, State/Province, Country, Postal Code:  Contact Information Redacted
Telephone:                      Email Address:  Contact Information Redacted	Telephone:                      Email Address:  Contact Information Redacted
Name of Applicant's Attorney or Representative:  Flip Petillion	Name of Objector's Attorney or Representative:  Steven C. Sereboff
Name of Firm (if applicable):  Crowell & Moring	Name of Firm (if applicable):  SoCal IP Law Group LLP
Address:  Contact Information Redacted	Address:  Contact Information Redacted
City, State/Province, Country, Postal Code:  Contact Information Redacted	City, State/Province, Country, Postal Code:  Contact Information Redacted
Telephone:                      Email Address:  Contact Information Redacted	Telephone:                      Email Address:  Contact Information Redacted
Signature:   Attorney-at-law, 23 May 2013	

## I. The Parties

### A. The Applicant

Through its subsidiary, Webs Inc., the Applicant (also Respondent) provides free website creation tools and hosting services. Additional paid features are offered (Attachment 1).

At present, the Applicant conducts its business using a website that is accessible via the domain name 'webs.com'. The 'webs.com' domain name was registered on April 4, 1995 (Attachment 2).

'Webs' is the mark under which the Applicant brands its products and services.

Webs' clients are predominantly non-US clients (54% non-US, 46% US) (Attachment 3).

### B. The Objector

The Objector primarily provides web site development services to small and medium businesses and conducts its business using a website that is accessible via the domain name 'web.com' (Attachment 4). The 'web.com' domain name was registered on July 2, 1996 (Attachment 5).

The Objector uses the mark 'Web.com' for which it has two U.S. trademark registrations (Attachment 6).

Web.com's clients are primarily US based (Attachment 7).

## II. Factual background

### A. The Objector and the Applicant have co-existed for many years without any problem

#### 1. The WEBS.COM and WEB.COM domain names have been used and coexisting in the market for many years

The 'webs.com' domain name was created on April 5, 1995 (Attachment 2), more than a year before the creation of the 'web.com' domain name on July 2, 1996 (Attachment 5).

Both 'webs.com' and 'web.com' domain names have been used simultaneously for more than 16 years. The two domain names have co-existed, and significant and distinct businesses have thrived under these separate names, with each business possessing its own independent identity and goodwill.

#### 2. The Parties have never initiated any case against each other

Neither the Applicant nor the Objector have ever litigated over the others use of their respective mark and domain name.

**3. The Applicant's use of the WEBS.COM domain name has never been the subject of any lawsuit**

The Applicant's use of the 'webs.com' domain name has never been questioned by a party in court or in a UDRP case.

**4. The Objector's use of the WEB.COM domain name has never been the subject of any law suit**

In so far as the Applicant is aware, the Objector's use of the WEB.COM domain name has never been questioned by a party in court or in a UDRP proceeding.

**B. Both the Applicant and the Objector have filed an application for a new generic Top Level Domain**

The Applicant has applied for the string .WEBS (standard and community application) with a view to consolidating the reputation of the Applicant's website creation tools and hosting services, known under the identifier 'WEBS' and the community it represents. The use of the 'WEBS' identifier is aimed at making it unambiguous that the TLD is related to the Applicant (**Attachments 8 and 9**)

The Objector has applied for the string .WEB (**Attachment 10**).

**C. There are 7 applicants for .WEB**

There are 7 applicants for .WEB. Apart from the Objector, an application for .WEB was filed by DotWeb Inc. (AE), Charleston Road Registry Inc., (US), Afilius Domains No. 3 Limited (IE), Ruby Glen, LLC (US), Schlund Technologies GmbH (DE), and NU DOT CO LLC (US) (**Attachment 11-16**).

No other party applied for .WEBS.

**D. The other applicants for .WEB have not filed a string confusion objection**

None of the other 6 applicants for .WEB has filed an objection against the Applicant. It is fair to deduce from this that these applicants either do not share the grounds for the objection filed by the Objector and/or that they did not deem it appropriate to file such an objection on these or other grounds.

### III. The purpose of ICANN's new gTLD program and the limited grounds for objection

On 12 January 2012, ICANN launched its new Generic Top-Level Domain (gTLD or TLD) program, with the goal of “*enhancing competition[,] consumer choice[,] . . . [and] innovation via the introduction of new gTLDs.*”<sup>1</sup> The Applicant filed its application for the string .WEBS, which it intends to use in connection with its free website creation and hosting business. The applied-for .WEBS gTLD will increase competition and benefit Internet users by providing new and different services within an expanded DNS, and thus enhance the goals of ICANN's new gTLD program.<sup>2</sup>

ICANN designed the objection process to protect certain legitimate rights, while also ensuring that objectors could not prevent the delegation of legitimate TLDs. Objections are only permitted on the four specific grounds enumerated in the Guidebook: string confusion, legal rights, community opposition, and limited public interest.<sup>3</sup> Any objection outside these narrow grounds must fail.

Accordingly, it is important to apply the criteria as written, and not in an overbroad way that unnecessarily interferes with the delegation of the applied-for TLD. The Applicant will show that the Objector seeks to use the string confusion objection to limit competition. Such use of the objection proceedings directly conflicts with the purpose of ICANN's new gTLD program.

The Applicant will also show that the objection is not only contrary to the purpose of ICANN's new gTLD program, but also fails to meet the stringent criteria of a legal rights objection.

### IV. The task of the panel expert

#### A. The relevant criterion

The applicable rule has been provided in the AGB, Section 3.5.1. which reads as follows:

*“A DRSP panel hearing a string confusion objection will consider whether the applied-for gTLD string is likely to result in string confusion. String confusion exists where a string so nearly resembles another that it is likely to deceive or cause confusion. For a likelihood of confusion to exist, it must be probable, not merely possible that confusion will arise in the mind of the average, reasonable Internet user. Mere association, in the sense that the string brings another string to mind, is insufficient to find a likelihood of confusion.” (emphasis added)*

The Applicant wishes to point out that the Objector omitted the last sentence when referring to AGB, Section 3.5.1. (Objection, p. 3). However, as will be demonstrated below, this sentence is quite relevant for this case.

---

<sup>1</sup> About the Program: ICANN New gTLDs, available at <http://newgtlds.icann.org/en/about/program>.

<sup>2</sup> About the Program: ICANN New gTLDs, available at <http://newgtlds.icann.org/en/about/program> (“The program's goals include enhancing competition and consumer choice, and enabling the benefits of innovation via the introduction of new gTLDs.”).

<sup>3</sup> *Id.*, Module 3.2.1.



## B. Difference with the task of the String Similarity Panel

The evaluation undertaken by the Expert Panel is different from that assigned by ICANN to the String Similarity Panel in the Initial Evaluation.

### 1. The task of the String Similarity Panel

The String Similarity Panel was assigned the task of determining contention sets. The String Similarity Panel was asked to review the entire pool of applied-for strings to determine whether the strings proposed in any two or more applications were so similar that they would create a probability of user confusion if allowed to coexist in the DNS. (AGB, Module 4-3)

The criterion to be used by the String Similarity Panel is defined in the Applicant Guidebook which states:

*“Contention sets are groups of applications containing identical or similar applied-for gTLD strings.”*

[...]

*“‘similar’ means strings so similar that they create a probability of user confusion if more than one of the strings is delegated into the root zone.*

[...]

*The String Similarity Panel will [...] review the entire pool of applied-for strings to determine whether the strings proposed in any two or more applications are so similar that they would create a probability of user confusion if allowed to coexist in the DNS. The panel will make such a determination for each pair of applied-for gTLD strings. The outcome of the String Similarity review described in Module 2 is the identification of contention sets among applications that have direct or indirect contention relationships with one another.*

*Two strings are in direct contention if they are identical or similar to one another.*

[...]

*Two strings are in indirect contention if they are both in direct contention with a third string, but not with one another.” (AGB, Module 4-2, 4-3)*

Module 2 of the Applicant Guidebook also states:

**“Standard for String Confusion** – *String confusion exists where a string so nearly resembles another visually that it is likely to deceive or cause confusion. For the likelihood of confusion to exist, it must be probable, not merely possible that confusion will arise in the mind of the average, reasonable Internet user. Mere association, in the sense that the string brings another string to mind, is insufficient to find a likelihood of confusion.” (AGB, Module 2-8)*

## 2. The task of the Expert Panel

The Applicant Guidebook provides in Module 2 that – in contrast with the determination by the String Similarity Panel – a String Confusion Objection brought before an Expert Panel:

“...is **not limited to visual similarity**. Rather, confusion based on any type of similarity (including **visual, aural, or similarity of meaning**) may be claimed by an objector.” (AGB, Module 2-8).

### V. ICANN and its String Similarity Panel do not consider the strings to be confusingly similar

#### A. ICANN's String Similarity Assessment Tool provides a low similarity rate

In the application period for new gTLDs, ICANN had made accessible a String Similarity Assessment Tool. It is still accessible on <https://icann.sword-group.com/algorithm/Default.aspx>. (Attachment 17)

According to the information published on this website, this tool “*is intended to provide an **open, objective, and predictable mechanism** for assessing the degree of **visual similarity** between TLD strings.*”

It allows for the comparison of two strings to each other.

When comparing .WEBS with .WEB, the similarity rate is 72% (Attachment 18) which is much lower than the similarity rate of various TLDs that currently co-exist (Attachments 19-55). *E.g.*, the currently co-existing .LT and .TL strings and .IL and .LI are respectively 93% and 94% similar (Attachments 53-54).

The 72% similarity is also much lower than the 88% similarity between the applied-for .ACCOUNTANTS and .ACCOUNTANT or the 84% similarity between the applied-for .COUPONS and .COUPON (Attachments 56-57). The applicants for these strings did not file a string confusion objection.

Internet users have become used to the existence of TLDs having much more similarity than the claimed similarity between .WEBS and .WEB. For instance, with a similarity rate of 83%, .IO and .JO are considered visually more similar (Attachment 44). Also, in certain languages, from an aural perspective, .IO is virtually identical to .JO. From a conceptual point of view, .IO and .JO are as meaningful, or rather equally meaningless. Nonetheless, this poses no problem for the average Internet user, who is used to small differences between TLDs.

#### B. ICANN has not put the applications for .WEBS and .WEB in a contention set

As mentioned above, in the Initial Evaluation, ICANN assigned a panel called the String Similarity Panel with the task to determine contention sets: The String Similarity Panel was asked to review the entire pool of applied-for strings to determine whether the strings

proposed in any two or more applications were so similar that they would create a probability of user confusion if allowed to coexist in the DNS (AGB, Module 4-3).

The outcome of this assignment was that two contention sets of non-exact matches were created: the set containing .HOTELS and .HOTEIS strings and the set containing the .UNICOM and .UNICORN strings (**Attachment 58**).

No other contention sets for non-exact matches in Latin script were created.

This shows that neither the String Similarity Panel nor ICANN (who endorses the determinations by the String Similarity Panel) were of the opinion that the .WEBS and .WEB strings are so similar that they would create a probability of user confusion if allowed to coexist in the DNS.

## **VI. The Objector does not consider WEBS and WEB to be confusingly similar**

### **A. The Objector considers much more similar signs not confusingly similar**

Web.com has narrowed the scope of its enforceable trademark rights by entering into a Supplemental Consent to Registration with Verio. The Objector and Verio have agreed that there was no likely confusion between WEB.COM on the one hand, and WEBCOM on the other hand (**Attachment 59**).

When entering into the Supplemental Consent, the Objector was of the opinion that “customers understand that you have to use the correct Internet address because a different Internet address will resolve to a different website” and that there is no likelihood of confusion because “[t]he consuming public is sophisticated enough” (**Attachment 59**). The Objector also indicated that the parties have enjoyed long coexistence without any known instances of actual confusion.

Therefore, it is impossible to understand how the Objector can agree to coexistence between WEB.COM and WEBCOM and yet object to a coexistence between WEB and WEBS. Indeed:

- The letter ‘S’ is much more distinctive than the symbol ‘.’;
- The dot is placed in the middle of the WEB.COM sign, making it much more likely to be overlooked than the last letter of a word, which (together with the first letter) has been shown to be more significant than the rest of the letters (*infra*);
- The Applicant and the Objector have also enjoyed long coexistence without any known instances of actual trademark relevant confusion.

### **B. The Objector never formally challenged the co-existence between the WEBS.COM and WEB.COM domain names**

The Objector has never instituted a formal challenge to the WEBS.COM domain name, which co-exists with the Objector’s WEB.COM domain name for years. Whereas the letter ‘S’ in ‘WEBS.COM’ makes ‘WEBS.COM’ clearly differ from ‘WEB.COM’, the difference

between a 'WEBS' TLD and a 'WEB' TLD is even greater. As a TLD will always come at the end of the domain name syntax, the distinctive letter 'S' will always appear at the end, making this last letter more significant .

## VII. There is no overall similarity

The difference between the .WEBS and .WEB strings is grounded in the character 'S' present in the first and not part of the second. In linguistic terms, the character 'S' is manifestly distinct.

The Applicant asked an independent expert to provide his views on the following questions:

- 1) Regardless of the ICANN framework, would you consider both strings to be confusing?
- 2) Given the ICANN framework, would you consider both strings confusing based on any of the following types of similarity: visual, aural or similarity of meaning?

The expert to whom this request was addressed, Professor Piet Desmet, is full professor at the University of Leuven in linguistics and language teaching methodology (**Attachment 60**).

Professor Desmet from the University of Leuven has made the following findings:

1. Exterior letters serve as visual clues for word recognition. The first and last letters of a word have been shown to be more salient than the rest of the letters and to receive priority in processing. Readers can recognize a word even when its interior letters are scrambled.

Professor Desmet concludes that 'webs' and 'web' are recognized as two radically different words since their last letters are completely different.

2. In the case of 'web' and 'webs', completely regular patterns allow for a one-to-one mapping of spelling to sound. In other words, a word that consists of completely regular patterns is spelled out exactly as it sounds. The sound of the word easily translates into the spelling of the word and *vice versa*. Words consisting of completely regular patterns facilitate word recognition.

Professor Desmet considers that 'webs' and 'web' have completely regular patterns allowing for one-to-one mapping of spelling to sound, which highly facilitates the word recognition of both words.

3. Third, there is an extremely limited number of words that could be generated by changing only one single letter in 'webs' and 'web'. In other words, 'webs' and 'web' have a limited number of orthographic neighbors. Words with a high number of orthographic neighbors are more difficult to recognize and have an inhibitory effect when reading, as evidenced by eye-fixation patterns. Words with fewer orthographic neighbors are more easily recognizable.

Professor Desmet concludes that this results in a higher word recognition for 'webs' and 'web' which have a limited number of orthographic neighbors.

4. Fourth, a reader will first decompose the word 'webs' into meaningful units. 'Webs' is composed of two meaningful units, namely 'web' and the plural marker '-s'. 'Web' only has one meaningful unit.

For professor Desmet, this is an extra factor that enhances the ability to recognize the difference between 'web' and 'webs'.

5. Also, the plural '-s' is a completely regular plural and easily recognizable compared to irregular plurals (e.g. with vowel change such as 'hero'/'heroes') that have been proven to be less easily recognizable.

In conclusion, Professor Desmet considers the 5 elements above reason enough to dismiss the idea of string confusion in the case of 'webs'/'web'.

### **VIII. The strings are visually different**

The two strings .WEBS and .WEB are visually distinct.

A number of different trademark offices provide guidance on how to interpret confusion. For example, the European Union Trade Mark Office provides guidance on how to interpret confusion. Its *Manual concerning opposition* was used by the GNSO<sup>4</sup> when it suggested language for the Applicant Guidebook of ICANN. The Manual lays down a couple of relevant principles that apply in the case at instance:

*"The visual comparison is based on an analysis of the number and sequence of the letters, the number of words and the structure of the signs." (Attachment 61, p. 10, section 3.2)*

*"The length of a name may influence the effect of differences. The shorter a name, the more easily the public is able to perceive all its single elements. Thus, small differences may frequently lead in short words to a different overall impression. In contrast, the public is less aware of differences between long names." (Attachment 61, p. 22, section 4.2)*

Visually, the 'S' is a clear differentiator because it is positioned at the end of the short word (which gives it priority in the processing of word recognition) and it has the function to indicate the plural, which is a regular plural. This is confirmed by the findings of Professor Desmet mentioned above.

The difference is sufficiently clear not to cause any confusion, mistake or deception, as is made clear by the longstanding coexistence between the domain names WEBS.COM and WEB.COM.

---

<sup>4</sup> ICANN's Generic Names Supporting Organization ; see <http://gns0.icann.org/en/>

**IX. The strings are aurally different**

Also aurally, the strings are different. As evidenced by the findings of Professor Desmet, both 'webs' and 'web' consist of completely regular patterns and are spelled out exactly as they sound. In other words, all letters are clearly pronounced in both words, which makes the words clearly recognizable and distinct from one another.

Indeed, the sound of the letter 's' is clearly stressed in 'webs' and is not present in the word 'web'. Individuals are perfectly capable of distinguishing the sound that is generated by adding the letter 's' to a word with similar endings as the word 'web'. *E.g.*, individuals are perfectly capable of distinguishing 'step' from 'steps', 'car' from 'cars' or 'sales rep' from 'sales reps'.

Hence, also from an aural perspective, 'webs' is clearly different and distinguishable from 'web'.

**X. The strings have a different meaning**

The strings have a different meaning. 'Web' refers to the world wide web or to a network or silken structure created by a spider (**Attachment 62**), whereas 'webs' has no particular meaning and could be anything. On Wikipedia, 'webs' is used for the Applicant's web hosting services, a radio station and a 2003 sci-fi movie (**Attachment 63**). 'Web' on the other hand has a clear dictionary meaning (**Attachment 64**).

In any event, as mentioned above, the Applicant Guidebook expressly provides that mere association, in the sense that the string brings another string to mind, is insufficient to find a likelihood of confusion (AGB, Section 3.5.1.).

As also explained above, the mission and purpose of the Applicant .WEBS gTLD is to consolidate the reputation of the Applicant's hosting services, known under the identifier 'WEBS' and the community it represents and to ensure that the .WEBS top-level domain will be unambiguous as regards the identity of the Registry Operator.

This purpose is in diametric opposition to the mission and purpose of the Objector's .WEB gTLD, which is to "become the most versatile gTLD on the World Wide Web" and to "quickly become as ubiquitous" and to "serve everyone, from commerce to information to community-building" (**Attachment 10**, response to evaluation question 18).

As a result, the services offered under .WEBS and .WEB will clearly distinguish themselves.

**XI. The real objective of the Objector**

During the Objector's first quarter 2013 earnings conference call, the Objector stated that it is certainly interested in getting the .WEB gTLD, but that it's not its core business. The objector said that it will "*be perfectly content if anyone gets .web because they are going to distribute it through [the Objector] and it [i]s [their] name and [the Objector is] advertising and building a brand in the marketplace and [is] going to be a great deliverer of .web extensions, whoever gets it; whether it's [the Objector] or someone else*" (**Attachment 65**, p. 13). The Objector pointed out that its strategy has always been to cooperate and that they have looked at the people who have applied for .web and that it is talking to all of them about who would benefit from this and which team would be the best team to provide services.

While the Objector is in contention with multiple applicants for .WEB, the Applicant is not in contention with any other applicant for .WEBS. The Objector has realized that it faces a challenge in obtaining the delegation of the .WEB extension, while the Applicant does not face a similar challenge in dealing with other applicants. With the present objection, the Objector is trying to give the Applicant the same challenge.

The Objector's sole motive in filing the objection is to prevent a potential competitor, who does not have the intention to create goodwill in the Objector's name, from entering the gTLD market. Such intent, to limit competition, is clearly contrary to the purpose of ICANN's new gTLD program.

As mentioned above, no other applicant for .WEB shared the views of the Objector as none of them were of the opinion that there were reasons to file an objection against the Applicant.

**XII. The Objector's position is incoherent**

The Objector argues that the vast majority of Internet users are non-native English speakers and that non-English speakers commonly confuse plural and singular word forms or omit the plural altogether.

The Objector does not produce any evidence in support of this argument.

Also, how can the Objector (without any evidence) know what a non-native English speaker sees and not, or what he distinguishes and what she does not?

As mentioned above, the first and last letters of a word are in combination visual clues for a word, making words more recognizable. The way individuals recognize words is not related to being a native speaker or not, but is connected to the functioning of the human brain (**Attachment 60**).

**XIII. The Objector's allegations are unfounded****A. The comparison with UDRP cases is irrelevant for this case**

The UDRP cases referred to by the Objector are all cases between a registrant of a domain name and the holder of a trade mark.

In the present case the question whether one or both of the names is related to a trademark is irrelevant. The present case is not a case about the violation of a trademark. Even if it were, “*the mark .WEB used in relation to Internet registry services is generic and cannot enjoy trademark protection*” (See *Image Online Design, Inc. v ICANN*, Case No. CV 12-08968 DDP (US District Court of California, 7 Feb. 2013), **Attachment 66**, p. 16).

And even if UDRP cases were relevant, UDRP cases relating to generic terms contradict the findings in the cases produced by the Objector. Examples include:

- *Mansion (Gibraltar) Limited and Provent Holdings Ltd. v. Agens PSC*, WIPO Case No. D2010-0584 (finding that “*since “casino” is a well-known generic term, small visual and sound modifications are, in this Panel’s view, very obvious and are more easily remembered by the human mind.*”) (**Attachment 67**).

*Tire Discounters, Inc. v. TireDiscounter.com*, NAF Case No. FA0604000679485 (finding that “[*b*]ecause the mark is merely descriptive, small differences matter. In the Internet context, consumers are aware that domain names for different websites are often quite similar and that small differences matter. See *Entrepreneur Media, Inc. v. Smith*, 279 F.3d 1135, 1147 (9<sup>th</sup> Cir. 2002). The omission of the letter “s” from the mark is one of those small differences that matters in this context. Complainant has failed to meet its burden to establish that Respondent’s **<tirediscounter.com>** domain name is confusingly similar to Complainant’s mark within the meaning of Policy ¶4(a)(i). See *Men’s Warehouse, Inc. v. Wick*, FA 117861 (Nat. Arb. Forum Sept. 16, 2002).”) (**Attachment 68**)

## B. There is no (Evidence of) Actual Confusion

The evidence of actual confusion to which the Objector points is exceptionally weak given the long history of coexistence of the WEBS.COM and the WEB.COM domain names and between the Objector and the Applicant’s business. Tens of millions websites have been built with Webs and, together, these sites receive 300 million page views each month (**Attachment 1**). The Objector claims to be helping over 3 million customers with its presence on the web (**Attachment 4**).

In light of the large volume of business conducted through both the Applicant’s and Objector’s websites, minimal instances of misdirected consumer communications are “at best *de minimis*,” and the paucity of evidence of actual confusion in fact creates “a presumption against likelihood of confusion in the future.” *Petro Stopping Centers, L.P. v. James River Petroleum, Inc.*, 130 F.3d 88, 96 (4th Cir. 1997) (citations omitted) (**Attachment 69**).

The Objector does not actually provide details of any of the “abundant evidence” of actual confusion that it alleges in the Objection.

The examples of alleged actual confusion that the Objector has provided through links are examples of typographical errors, not actual confusion. The standard for actual consumer confusion requires a mental state of actual confusion as to the source of two products or services. See 3 *McCarthy on Trademarks* § 23:13 (“[E]vidence of actual confusion is the testimony of a ‘reasonably prudent purchaser’ who was in fact confused by defendant’s trademark.”) (emphasis added); *Checkpoint Systems, Inc. v. Check Point Software*



*Technologies, Inc.*, 104 F. Supp. 2d 427, 464 (D.N.J. 2000) (same), *aff'd* 269 F.3d 270 (3d Cir. 2001). Accordingly, courts have routinely rejected typographical errors as evidence of actual confusion. See, e.g., *Heartsprings, Inc. v. HeartSpring, Inc.*, 949 F. Supp. 1539, 1545 n.4 (D. Kan. 1996) (rejecting typographical error in press release as evidence of actual confusion); *Water Pik, Inc. v. Med-Systems, Inc.*, 2012 WL 224447, at \*7 n.7 (D. Colo. Jan. 25, 2012) (rejecting typographical error in blog entry as evidence of actual confusion) (**Attachment 70-73**).

The only examples of alleged confusion for which the Objector provides citations do not evidence actual confusion. Instead, they appear to be typographical errors on the webs.com forum:

- 1) [http://support.webs.com/webs/topics/web\\_com\\_examples](http://support.webs.com/webs/topics/web_com_examples)

The headline for the topic is “[web.com](#) examples” but immediately under this, the question has the correct reference to [webs.com](#): “Is there really no way/place to see examples of real sites created on [webs.com](#)?”

This is obviously a typographical error and not genuine confusion.

- 2) [http://support.webs.com/webs/topics/can\\_dns\\_be\\_hosted\\_elsewhere\\_and\\_still\\_have\\_a\\_site\\_name\\_web\\_com\\_site\\_work](http://support.webs.com/webs/topics/can_dns_be_hosted_elsewhere_and_still_have_a_site_name_web_com_site_work)

Here the headline refers to [web.com](#) but the question underneath correctly refers to [webs.com](#). Headline: “Can DNS be hosted elsewhere, and still have a [site-name.web.com](#) site work?” Question underneath: “I do not want to transfer my domain registration to [webs.com](#) . . . Is there an IP address I can point our DNS to, to make a [webs.com](#) site work?”

This too, is plainly a typographical error, and not actual confusion.

- 3) [http://support.webs.com/webs/topics/my\\_web\\_com\\_site\\_disappeared](http://support.webs.com/webs/topics/my_web_com_site_disappeared)

Here, the customer is complaining about her ‘[web.com](#)’ site disappearing. She is, however, a registered user of the Webs user forum, and responses to the post and subsequent user posts clearly reference Webs.

Again, this post appears to be a typographical error, not actual confusion.

Also, even if the Applicant were to accept that each of the forums that the Objector cites contained examples of individuals who were actually confused as to the source of a product or service (as opposed to someone who made a typographical error), it would underscore the tiny percentage of consumers who would be affected by that confusion.

A final example of alleged confusion is the case in which the Applicant’s CEO and co-founder made a typographical error in a press release by PR.com. This typographical error was quickly corrected after discovering the mistake. Does the Objector truly believe that the Applicant’s co-founder and CEO was confused about his own company name?

Finally, the fact that the Attorney General of Kentucky and the Attorney General of Arkansas would have sent a letter by mistake to web.com instead of to webs.com does not prove that the Attorneys General were confused. The Attorney General in Arkansas was provided with the incorrect address in the complaint form, filed by a non-customer. With both the Applicant and the Objector having millions of customers, the fact that only two letters were addressed to the wrong party, shows how limited the likelihood of confusion between 'webs.com' and 'web.com' is. The likelihood of confusion between .WEBS and .WEB is even more limited, given the fact that the last letter in both words is different (which makes the difference more apparent, as shown above).

### CONCLUSION

As explained above there is no risk of confusion in the mind of the average, reasonable Internet user, nor is such risk probable. Accordingly, there is no likelihood of confusion between the strings .WEB and .WEBS such that the strings should be placed in the same contention set.

The Applicant requests that the objection be declared Unsuccessful and that the Applicant and the Objector both move forward in the process without being considered in direct contention with one another.

Respectfully submitted,



Flip Petillion, Advocaat

Authorized Representative of the Respondent

May 23, 2013

### Attachments

1. Company information on the Applicant and its subsidiary
2. Whois records of <webs.com>
3. Overview of US and non-US clients of the Applicant
4. Company information on the Objector
5. Whois records of <web.com>
6. USPTO Reg. Nos. 2521314 and 3666813

7. Objector's most recent annual report
8. Application No. 1-1033-73917 for gTLD '.webs' by the Applicant
9. Application No. 1-1033-22687 for gTLD '.webs' by the Applicant
10. Application No. 1-1009-97005 for gTLD '.web' by the Objector
11. Application for gTLD '.web' by DotWeb Inc. (AE)
12. Application for gTLD '.web' by Charleston Road Registry Inc., (US)
13. Application for gTLD '.web' by Afilias Domains No. 3 Limited (IE)
14. Application for gTLD '.web' by Ruby Glen, LLC (US)
15. Application for gTLD '.web' by Schlund Technologies GmbH (DE)
16. Application for gTLD '.web' by NU DOT CO LLC (US)
17. Printout of the website where the String Similarity Assessment Tool is accessible via <https://icann.sword-group.com/algorithm/Default.aspx>
18. Printout of the website where the String Similarity Assessment Tool is used to compare '.webs' with '.web'
19. Printout of the website where the String Similarity Assessment Tool is used to compare .BV and .BY
20. Printout of the website where the String Similarity Assessment Tool is used to compare .BA and .BE
21. Printout of the website where the String Similarity Assessment Tool is used to compare .CU and .CV
22. Printout of the website where the String Similarity Assessment Tool is used to compare .FI and .FR
23. Printout of the website where the String Similarity Assessment Tool is used to compare .AC and .AE
24. Printout of the website where the String Similarity Assessment Tool is used to compare .AW and .AU
25. Printout of the website where the String Similarity Assessment Tool is used to compare .CM and .CN
26. Printout of the website where the String Similarity Assessment Tool is used to compare .CU and .CV
27. Printout of the website where the String Similarity Assessment Tool is used to compare .CV and .CY
28. Printout of the website where the String Similarity Assessment Tool is used to compare .GM and .GN
29. Printout of the website where the String Similarity Assessment Tool is used to compare .TL and .TJ
30. Printout of the website where the String Similarity Assessment Tool is used to compare .IL and .IT
31. Printout of the website where the String Similarity Assessment Tool is used to compare .LU and .LV
32. Printout of the website where the String Similarity Assessment Tool is used to compare .LV and .LY
33. Printout of the website where the String Similarity Assessment Tool is used to compare .PK and .PH
34. Printout of the website where the String Similarity Assessment Tool is used to compare .MV and .MW
35. Printout of the website where the String Similarity Assessment Tool is used to compare .EC and .EE
36. Printout of the website where the String Similarity Assessment Tool is used to compare .IT and .TL
37. Printout of the website where the String Similarity Assessment Tool is used to compare .Bl and .BJ

38. Printout of the website where the String Similarity Assessment Tool is used to compare .AI and .AL
39. Printout of the website where the String Similarity Assessment Tool is used to compare .GI and .GL
40. Printout of the website where the String Similarity Assessment Tool is used to compare .LT and .IT
41. Printout of the website where the String Similarity Assessment Tool is used to compare .ME and .MF (UC)
42. Printout of the website where the String Similarity Assessment Tool is used to compare .BE and .BF (UC)
43. Printout of the website where the String Similarity Assessment Tool is used to compare .FI and .FJ
44. Printout of the website where the String Similarity Assessment Tool is used to compare .IO and .JO
45. Printout of the website where the String Similarity Assessment Tool is used to compare .IE and .JE
46. Printout of the website where the String Similarity Assessment Tool is used to compare .SI and .SJ
47. Printout of the website where the String Similarity Assessment Tool is used to compare .SL and .LS
48. Printout of the website where the String Similarity Assessment Tool is used to compare .AU and .UA
49. Printout of the website where the String Similarity Assessment Tool is used to compare .ES and .SE
50. Printout of the website where the String Similarity Assessment Tool is used to compare .TP and .PT
51. Printout of the website where the String Similarity Assessment Tool is used to compare .TG and .GT
52. Printout of the website where the String Similarity Assessment Tool is used to compare .IO and .IQ (UC)
53. Printout of the website where the String Similarity Assessment Tool is used to compare .LT and .TL
54. Printout of the website where the String Similarity Assessment Tool is used to compare .IL and .LI
55. List of all currently existing TLDs, as delegated by IANA
56. Printout of the website where the String Similarity Assessment Tool is used to compare .ACCOUNTANTS and .ACCOUNTANT
57. Printout of the website where the String Similarity Assessment Tool is used to compare .COUPONS and .COUPON
58. Printout of the website with ICANN contention sets for exact and non-exact matches
59. Supplemental Consent to Registration of the Objector with Verio
60. Expert opinion by Professor Dr. Piet Desmet
61. OHIM document on confusion
62. Dictionary meaning of 'web'
63. Wikipedia on 'webs'
64. Wikipedia on 'web'
65. Transcript of Q1 2013 Web.com Group Inc. Earnings Conference Call
66. Image Online Design, Inc. v ICANN, *Case No. CV 12-08968 DDP* (US District Court of California, 7 Feb. 2013)
67. Mansion (Gibraltar) Limited and Provent Holdings Ltd. v. Agens PSC, WIPO Case No. D2010-0584
68. Tire Discounters, Inc. v. TireDiscounter.com, NAF Case No. FA0604000679485

69. *Petro Stopping Centers, L.P. v. James River Petroleum, Inc.*, 130 F.3d 88, 96 (4th Cir. 1997)
70. *Checkpoint Systems, Inc. v. Check Point Software Technologies, Inc.*, 104 F. Supp. 2d 427, 464 (D.N.J. 2000)
71. *Checkpoint Systems, Inc. v. Check Point Software Technologies, Inc.*, 269 F.3d 270 (3d Cir. 2001)
72. *Heartsprings, Inc. v. Heartspring, Inc.*, 949 F. Supp. 1539, 1545 n.4 (D. Kan. 1996)
73. *Water Pik, Inc. v. Med-Systems, Inc.*, 2012 WL 224447, at \*7 n.7 (D. Colo. Jan. 25, 2012)
74. Proof of payment of filing fee.

**Janssen, Jan**

---

**From:** Microsoft Outlook  
**To:** Tom Simotas; DRfiling@icann.org; **Contact Information Redacted**  
**Sent:** jeudi 23 mai 2013 16:10  
**Subject:** Relayed: 50 504 T 00246 13 - Response (mail 1 of 4)

**Delivery to these recipients or groups is complete, but no delivery notification was sent by the destination server:**

[Tom Simotas](#) Contact Information Redacted

[DRfiling@icann.org \(DRfiling@icann.org\)](mailto:DRfiling@icann.org)

Contact Information Redacted

Contact Information Redacted

Contact Information Redacted Contact Infor

**Janssen, Jan**

---

**From:** Microsoft Outlook  
**To:** Tom Simotas; DRfiling@icann.org; Contact Information Redacted  
**Sent:** jeudi 23 mai 2013 16:14  
**Subject:** Relayed: 50 504 T 00246 13 - Response (mail 3 of 4)

**Delivery to these recipients or groups is complete, but no delivery notification was sent by the destination server:**

[Tom Simotas](#) Contact Information Redacted

[DRfiling@icann.org \(DRfiling@icann.org\)](mailto:DRfiling@icann.org)

Contact Information Redacted

Contact Information Redacted

Contact Information Redacted

Subject: 50 504 T 00246 13 - Response (mail 3 of 4)