

**IN THE MATTER OF AN INDEPENDENT REVIEW PROCESS
BEFORE THE INTERNATIONAL CENTRE FOR DISPUTE RESOLUTION**

AFILIAS DOMAINS NO. 3 LIMITED,

Claimant

v.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS,

Respondent

ICDR Case No. 01-18-0004-2702

EXHIBIT LIST FOR

WITNESS STATEMENT BY JOSE IGNACIO RASCO III

June 1, 2020

Exhibit No.	Description
A.1	NDC .WEB Application – Public
A.2	NDC .WEB Application – Non-Public <i>Highly Confidential- Attorneys’ Eyes Only</i>
Aa-Ap	Exhibits to NDC .WEB Application <i>Highly Confidential- Attorneys’ Eyes Only</i>
B	Domain Acquisition Agreement Between Verisign and NDC (25 August 2015) <i>Highly Confidential- Attorneys’ Eyes Only</i>
C	Email from O. Mauss (1&1 Internet) to J. Calle (NDC), with attachment <i>Confidential</i>
D	.TECH Application – Original
E	.TECH Application – Revised
F	Radix Press Release- Radix Wins Rights to .TECH (7 November 2014)
G	.TECH Registry Agreement (unsigned)
H	Confirmation of Understandings between Verisign and NDC (26 July 2016) <i>Highly Confidential- Attorneys’ Eyes Only</i>
I	Emails between J. Nevett (Donuts) and J. Rasco (NDC) <i>Confidential</i>
J	Text messages between S. Heflin (Afilias) and J. Calle (NDC) <i>Confidential</i>
K	Text messages between J. Kane (Afilias) and J. Rasco (NDC) <i>Confidential</i>
L	Donuts Complaint to ICANN
M	Emails between J. Erwin (ICANN) and J. Rasco (NDC) <i>Confidential</i>
N	Emails between C. LaHatte (ICANN) and J. Rasco (NDC) <i>Confidential</i>
O	Emails between C. Willett (ICANN) and J. Rasco (NDC) <i>Confidential</i>
P	Letter from C. Willett (ICANN) to .WEB Contention Set (13 July 2016) <i>Confidential</i>
Q	Email from L. Ausubel (Power Auctions) to J. Rasco (NDC)
R	Text message from J. Kane (Afilias) to J. Rasco (NDC) <i>Confidential</i>
S	Email from C. Willett (ICANN) to J. Rasco (NDC) <i>Confidential</i>
T	Emails between J. Rasco (NDC) and ICANN, with attachment <i>Highly Confidential- Attorneys’ Eyes Only</i>

EXHIBIT A.1



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-effective 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); and
- ICANN's Generic Names Supporting Organization (GNSO) Reserved Names Working Group - Final Report (see <http://gnso.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-3166-1_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 as a result the team is intimately familiar with its operations.

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

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

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

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

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

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 components of the SRS. The primary function of the SRS database is to provide highly reliable, persistent storage for all registry information required for domain

registration services. The database is highly secure, with access limited to transactions from authenticated registrars, trusted application-server processes, and highly restricted access by the registry database administrators. A full description of the database can be found in response to Question 33.

Figure 24-1 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 to 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.**

EXHIBIT A.2

**HIGHLY CONFIDENTIAL –
ATTORNEYS' EYES ONLY**

Redacted – Third Party Designated Confidential Information

EXHIBITS Aa-Ap

**HIGHLY CONFIDENTIAL –
ATTORNEYS' EYES ONLY**

Redacted – Third Party Designated Confidential Information

EXHIBIT B

**HIGHLY CONFIDENTIAL –
ATTORNEYS' EYES ONLY**

Redacted – Third Party Designated Confidential Information

EXHIBIT C

CONFIDENTIAL

Redacted – Third Party Designated Confidential Information

EXHIBIT D



New gTLD Application Submitted to ICANN by: Dot Tech LLC

String: tech

Originally Posted: 13 June 2012

Application ID: 1-1670-76346

Applicant Information

1. Full legal name

Dot Tech 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

Tess Pattison-Wade

6(b). Title

Executive Director

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

Shaul Jolles

7(b). Title

CEO

7(c). Address

7(d). Phone Number

Contact Information Redacted

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Limited Liability Company

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

Unites States

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.

Ecyber Solutions Group 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

Christopher Michael Parrott	Director of Finance
Paul Eugene Spurgeon	COO
Scott Adam Schactman	Director of Legal & Policy
Shaul Jolles	CEO

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

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

Ecyber Solutions Group Inc	Not Applicable
----------------------------	----------------

Applied-for gTLD string

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

tech

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.

There are no known operational or rendering issues associated with our applied for string. We are relying on the proven capabilities of Neustar to troubleshoot and quickly eliminate these should they arise.

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 purpose of “.TECH” is to provide a dedicated online environment for the technology industry allowing businesses to create user friendly access to products, services and information instantaneously through accurate search engine classifications.

It is our mission that businesses bearing the “.TECH” gTLD string would become leaders in their market and be instantly differentiated online as tech savvy innovators, product suppliers, or service professionals.

The “.TECH” gTLD would provide a streamlined presentation of businesses primarily related to, or participating in technological advancements, the production of technology, technology support services, or the sale and distribution of technology products.

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

Technology is defined as the application of scientific knowledge for practical purposes, which is often relayed through the making, usage and knowledge of tools, machines, techniques, crafts, systems, or methods of organization in order to solve a problem or perform a specific function. The word technology comes from the combination of two Greek words, which translate to mean the study of art, skill, craft. Technology is a unique term in the sense that it can either be applied generally, or to a specific area such as construction technology, medical technology, or information technology.

Humans began to create technology through the conversion of natural resources to simple tools. Early forms of technology include the wheel, fire, the printing press, and electricity. By today's standards, these life altering inventions seem more industrial than technologically based, but they sparked the creation of global communication, world wide travel, and in general, the ability of humans to control their external environment. When we compare them to the technological advancements in the modern world, we begin to see technology trending away from necessity -based creations and entering the realms of entertainment, leisure, and design.

Technology has impacted basically every aspect of our lives. From televisions to automobiles, coffee makers to cell phones; consumers worldwide employ technology to help them work faster, relax more, and entertain themselves. Additionally, businesses use technology to mainstream production processes, track their client base, and compile records. Hospitals, governments, schools, and homes benefit hourly from growing technology advancements, and society as a whole is increasingly dependent on the luxuries produced by these processes.

According to the National Science Institute, technology- intensive industries play a significant role in the global economy, representing a growing share of many countries' total economic activity. In 2010, tech intensive-industries represented 30% of the world's gross domestic product. While the United States, Europe and Japan comprise the largest conglomerate of world economic growth in the tech industry, we are also able to see significant industry increases in developing economies such as India, China and Russia. Industries related to technology transcend genre and can be identified in every industry sector in the world. While it is easy to equate technology to specific products we must also consider knowledge based tech industries. Information based technology has seen a steady increase in growth from 1995-2010 and currently accounts for trillions of dollars in revenue

worldwide.

When we consider the prevalence of tech related businesses, departments, and information worldwide and the rate at which domain registration has increased in the last ten years (resulting in overcrowding and a general lack of naming availability), we begin to see the need for industry classifications online such as “.TECH”. “.TECH” will not only open the door for increased online naming abilities, it will also allow consumers to easily locate specific products and services through increased search engine classifications. Further, by developing specific industry classifications such as “.TECH” , advertisers will have increased confidence that they are reaching their target markets, thus increasing advertising revenue across the board for online retailers.

With these thoughts in mind, we at DOT Tech, LLC believe that it is essential for the technology industry to become a leader in this Internet transition. On average, Google reports that there are over 45 million searches performed per month which include the word ‘tech’, resulting in a monthly volume of page views totaling well over 3 billion clicks. The opportunity to enhance the consumer experience while driving competition and information distribution in our market is paramount, and we are excited to be apart of this evolution.

In order to achieve our goals and build name recognition, DOT Tech will be implementing a robust marketing initiative, focused on enhancing the value of the “.TECH” gTLD, while positioning “.TECH” to become an industry “must -have” in assisting businesses to gain market share and exposure.

Within six years of the “.TECH” launch, it is our goal to register 70%+ of all tech industry related companies with a minimum of one “.TECH” gTLD. This achievement would solidify our mission statement and serve to differentiate the Internet in a much needed and effective way.

To do so, the following marketing strategies will be put in place:

- 1) Build strong relationships with Registrar services in order to capture new domain registrations applicable to “.TECH”.
- 2) Create a prominent and consistent image representative of our mission and expressed clearly through branding, advertisements, and corporate relationships.
- 3) Secure “key” Registrants through our Founders program (described further in question 29 of this application) that will act as innovative leaders to assist us in appropriately exposing our target audience to the existence of “.TECH”.
- 4) Cultivate relationships with both domestic and global technology and information technology organizations. Partnerships with these organizations and others like them would increase DOT Tech’s knowledge base in regards to efficiently meeting the needs of the technology industry consumers and business owners.
- 5) Partner with global marketing firms to ensure a wide reaching and effective marketing campaign. This process would allow DOT Tech to efficiently structure our marketing processes to reach the desired Registrants.
- 6) Increase exposure for “.TECH” by creating a strong international presence through attendance at conferences appropriate to our visibility in the market.
- 7) Create a consistent presence in all tech-related trade publications and sponsorship of well-attended tech-related events.
- 8) We intend to implement a highly focused/ targeted marketing blitz to the industry sub divisions associated with technology production, support, services, implementation and consumer retail in order to assist them in implementing and utilizing the “.TECH” gTLD.

It is our goal to provide an efficient and secure registration process by minimizing the input required by the Registrant and creating a streamlined application process. In order to do so and uphold the integrity of our mission to provide instant access to members of the technology industry, DOT Tech will implement the following registration guidelines and naming conventions:

- 1) .TECH registrations will be restricted to individuals, businesses, and organizations that are active members of the technology industry. “Active” can be defined, in this context, as any individual, business or organization wishing to provide technology related industry information, services, or products online.
- 2) Registrants will be asked to submit, at minimum, their contact information and to agree to a statement indicating that it is their intention to utilize their “.TECH” domain for the promotion, distribution, or exchange of information, products or services directly connected to the technology industry.

3) Content on all awarded “.TECH” sites is expected to primarily represent the Registrant’s connection to the technology industry. Sites will be randomly selected for review to ensure compliance with this guideline. Should Registrants be found in violation of this guideline, they will be notified in writing of the violation and given a 30 days to order to correct the content deficiencies of their site. If Registrants are unable to comply with this guideline within the 30 - day probationary period, DOT Tech, LLC will revoke the Registrant’s domain name and it will be returned to general availability. Should a Registrant’s domain name be revoked due to their content deficiencies, all funds paid by the Registrant to date will be considered non-refundable. DOT Tech, LLC or it’s designated agent will perform all tasks related to content monitoring in order to not further burden our registrar partners.

4) Should DOT Tech, LLC discover at any point that a Registrant has falsely represented themselves as an individual, business, or organization related to the technology industry, their awarded domain will be immediately revoked and returned to general availability. Should a Registrant’s domain be revoked due their false representation of their industry relationship, all funds paid by the Registrant to date will be considered non-refundable.

5) Registrants should understand that name availability is not guaranteed and that names will be issued on a first come, first served basis. Should a Registrant’s requested name be unavailable, the Registrant will be offered the option of re-wording, changing, or adapting their initial naming request until a suitable solution is found.

6) Registrants will not be allowed to register names that infringe on the legal rights of other individuals or companies, allude to criminal activities, or contain in any part racially offensive language.

7) DOT Tech, LLC reserves the right to deny, cancel, or transfer any registration or transaction (as more fully described in our Abuse Policies in question 28 below), 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 applicable laws, government rules or requirements, or court orders; (3) to avoid any liability, civil or criminal, on the part of DOT Tech, LLC, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) to correct mistakes made by the DOT Tech, LLC, registry services provider, or any Registrar in connection with a domain name registration; (5) during resolution of any dispute regarding the domain; and (6) if a Registrant’s pre authorization or payment fails; or (7) to prevent the bad faith use of a domain name that is identical to a registered trademark and being utilized to confuse users.

8) DOT Tech’s registry services operator will provide thick WHOIS services that are fully compliant with RFC 3912 and with Specifications 4 and 10 of the Registry Agreement. Additionally, DOT Tech, LLC will provide a Web-based WHOIS application, which will be located at www.whois.tech. The WHOIS Web application will be an intuitive and easy to use application. A complete description of these services can be found in Question 26 below.

9) All Registrants awarded a “.TECH” domain will agree to a one year minimum contract, which will need to be renewed on an annual basis. Renewal is the sole responsibility of the Registrant. Registrant’s failing to renew their awarded domains by their expiration dates will be given a 60-day renewal grace period prior to their domain being revoked and returned to general availability.

10) DOT Tech, LLC is not liable or responsible in any way for any errors, omissions or any other actions by any third party (including any Registrar service) arising out of, or related to a given Registrant’s application for, registration of, renewal of, or failure to register or renew a particular domain name.

11) Through the registration process, all Registrants will be expected to designate an administrative contact for their application, which would possess all the rights granted by DOT Tech, LLC or its designated agents to act in respect to the given domain including, but not limited to, managing the domain name or any services associated thereto.

11) DOT Tech, LLC will implement a reserved names policy consisting of both names DOT Tech, LLC wishes to reserve for our own purposes as the registry operator and names protected by ICANN. DOT Tech, LLC will respect all ICANN reserved names including, but not limited to, two letter country codes and existing TLD’s. Additionally, DOT Tech, LLC will seek ICANN approval on any additional names we plan to reserve in order to appropriately secure them prior to the opening of general availability.

DOT Tech, LLC will additionally implement a series of Rights Protection Mechanisms (RPM) included,

but not limited to; support for and interaction with the Trademark Clearinghouse (“Clearinghouse”), use of the Trademark Claims Service, segmented Sunrise Periods allowing for the owners of trademarks listed in the Clearinghouse to register domain names that consist of an identical match of their listed trademarks, subsequent Sunrise Periods to give trademark owners or Registrants that own the rights to a particular name the ability to block the use of such name, stringent take-down services and Uniform Dispute Resolution Policies.

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

DOT Tech, LLC will collect personal information from its Registrants via any of our approved Registrars. In order to maintain the integrity of the “.TECH” gTLD and minimize the negative consequences to consumers and business owners, the following policies will be adhered to:

- a) No information collected from our Registrants will be used for marketing purposes.
- b) Data collected will not be traded or sold.
- c) All data collected on any Registrant will be available to the Registrant free of charge.
- d) Registrants will be allowed to address and correct data inaccuracies as needed.
- e) All data will be kept secure.

DOT Tech, LLC will strictly uphold the rules set forth in their registration guidelines in order to accurately service our Registrants and mitigate any negative consequences to consumers or Internet users.

DOT Tech, LLC does not plan to offer registrations to Registrants directly. Therefore, our pricing commitments will be made within our Registry-Registrar Agreements. It is our intention that these commitments will percolate down to Registrants directly and that the contractual commitments contained within our Registry-Registrar agreements will be reflected in the retail sale process of our gTLD, thus minimizing the negative consequences that might be imposed on Registrants via the retail process.

DOT Tech plans to offer bulk registration benefits to Registrars during the first 6 months of operation. Registrars wishing to purchase bulk registrations of 1,000 names or more would be offered a 5% discount at the time of purchase. Additionally, DOT Tech, through our founders program will provide a 25% discount to founders’ participants as a participation incentive. It is possible that DOT Tech would offer additional pricing benefits from time to time as relative to the market. All future pricing discounts not detailed in this application will be submitted through the appropriate ICANN channels for approval prior to introduction to the market.

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.

DOT Tech, LLC has thoroughly reviewed ISO 3166 1 and ISO 3166 2, relevant UN documents on the standardization of geographic names, GAC correspondence relating to the reservation of geographic names in the .INFO TLD, and understands its obligations under Specification 5 of the draft Registry Agreement. DOT Tech shall implement measures similar to those used to protect geographic names in the .INFO TLD by reserving and registering to itself all the geographic place names found in ISO 3166 and official country names as specified by the UN. DOT Tech has already discussed this proposed measure of protecting geographic names with its registry services provider, Neustar, and has arranged for such reservation to occur as soon after delegation as is technically possible.

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 Applicant then relay this request to

ICANN. At this point, DOT Tech would wait for the approval of 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.

23.1 Introduction

DOT Tech has elected to partner with NeuStar, Inc (Neustar) to provide back end services for the ".TECH" registry. In making this decision, DOT Tech 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 ".TECH" 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. DOT Tech will use Neustar's Registry Services platform to deploy the ".TECH" registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to ".TECH"):

- 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). [Optional should be deleted if not being offered].

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 ".TECH" 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

DOT Tech 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 ".TECH". 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

DOT Tech 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 ".TECH" 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

DOT Tech, 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

DOT Tech will not be offering services that are unique to ".TECH".

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

DOT Tech has partnered with Neustar, Inc ("Neustar"), an experienced TLD registry operator, for the operation of the ".TECH" 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 ".TECH" 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, DOT Tech 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 ".TECH" 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 ".TECH".

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 ".TECH" 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 ".TECH" 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 ".TECH" 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 ".TECH" registry.

25. Extensible Provisioning Protocol (EPP)

25.1 Introduction

DOT Tech'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 DOT Tech is provided with an unparalleled EPP based registry. The following discussion explains the EPP interface which will be used for the ".TECH" 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

[Default Response]

The ".TECH" 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 ".TECH" 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 ".TECH" 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 ".TECH" registry.

26. Whois

DOT Tech, LLC 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 and relevant RFCs.

DOT Tech, LLC'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, the WHOIS service provided by DOT Tech, LLC's registry services operator has been designed from the ground up to display as much information as required by ICANN and respond to a very stringent availability and performance requirement.

Some of the key features of DOT Tech, LLC's WHOIS services will include:

- Fully compliant with all relevant RFCs including 3912;
- Production proven, highly flexible, and scalable (DOT Tech, LLC's back end registry services provider has 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; and
- Search capabilities (e.g., IDN, registrant data) that mitigate potential forms of abuse as discussed below.

DOT Tech, LLC's registry services operator will provide thick WHOIS services that are fully compliant with RFC 3912 and with Specifications 4 and 10 of the Registry Agreement.

DOT Tech, LLC's WHOIS service will support port 43 queries, and will be optimized for speed using an in-memory database and a master-slave architecture between SRS and WHOIS slaves. RFC 3912 is a simple text based protocol over TCP that describes the interaction between the server and client on port 43. DOT Tech, LLC's registry services operator currently processes millions of WHOIS queries per day.

In addition to the WHOIS Service on port 43, DOT Tech, LLC will provide a Web based WHOIS application, which will be located at www.whois.tech. This WHOIS Web application will be an intuitive and easy to use application for the general public to use. The WHOIS Web application provides all of the features available in the port 43 WHOIS. This includes full and partial search on:

- Domain names
- Nameservers

- Registrant, Technical and Administrative Contacts
- Registrars

The WHOIS web application will also provide features not available on the port 43 service. These include:

- Extensive support for international domain names (IDN)
- Ability to perform WHOIS lookups on the actual Unicode IDN
- Display of the actual Unicode IDN in addition to the ACE encoded name
- A Unicode to Punycode and Punycode to Unicode translator
- An extensive FAQ
- A list of upcoming domain deletions

DOT Tech, LLC will also provide a searchable web based WHOIS service in accordance with Specification 4 Section 1.8 The application will enable users to search the WHOIS directory to find exact or partial matches using any one or more of the following fields:

- Domain name
- 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.)
- Registrar ID
- Name server name and IP address
- Internet Protocol addresses
- The system will also allow search using non-Latin character sets which are compliant with IDNA specification

The WHOIS user will be able to 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 and their WHOIS information will quickly be returned to the user.

In order to reduce abuse for this feature, only authorized users will have access to the Whois search features after providing a username and password. DOT Tech, 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, which will make access to the zone files in bulk via FTP to any person or organization that signs and abides by a Zone File Access (ZFA) Agreement with the registry. Contracted gTLD registries will provide this access daily and at no charge.

DOT Tech, LLC will also provide ICANN and any emergency operators with up-to-date Registration Data on a weekly basis (the day to be designated by ICANN). Data will include data committed as of 00:00:00 UTC on the day previous to the one designated for retrieval by ICANN. The file(s) will be made available for download by SFTP, unless ICANN requests other means in the future.

DOT Tech, LLC's Legal Team consisting of 3 dedicated employees, will regularly monitor the registry service provider to ensure that they are providing the services as described above. This will entail random monthly testing of the WHOIS port 43 and Web-based services to ensure that they meet the ICANN Specifications and RFCs as outlined above, if not, to follow up with the registry services provider to ensure that they do. As the relevant WHOIS will only contain DOT Tech, LLC's information, DOT Tech, LLC's WHOIS services will necessarily be in compliance with any applicable privacy laws or policies.

27. Registration Life Cycle

27.1 Registration Life Cycle

27.1.1 Introduction

".TECH" 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 ".TECH".

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 ".TECH" registry per the defined ".TECH" 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 ".TECH" 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 ".TECH" 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 ".TECH" registry.

-Hold Removes the domain from the DNS zone.

UpdateProhibited Prevents the object from being modified by an Update command.

-TransferProhibited Prevents the object from being transferred to another Registrar by the Transfer command.

-RenewProhibited Prevents a domain from being renewed by a Renew command.

-DeleteProhibited Prevents the object from being deleted by a Delete command.

The lifecycle of a domain begins with the registration of the domain. All registrations must follow the EPP standard, as well as the specific business rules described in the response to Question 18 above. Upon registration a domain will either be in an active or inactive state. Domains in an active state are delegated and have their delegation information published to the zone. Inactive domains either have no delegation information or their delegation information 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 ".TECH" registry will implement a standard domain lifecycle found in most gTLD registries today. There are five possible domain states:

- Active
- Inactive
- Locked
- Pending Transfer
- Pending Delete.

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

27.2.2 Active State

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

27.2.3 Inactive State

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

27.2.4 Locked State

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

27.2.5 Pending Transfer State

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

27.2.6 Pending Delete State

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

27.3 Typical Registration Lifecycle Activities

27.3.1 Domain Creation Process

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

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

2. Nameservers are created in the SRS database. Nameservers are not required to complete the

registration process; however any domain with less than 2 name servers will not be resolvable.

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

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

27.3.2 Update Process

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

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

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

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

27.3.4 Renew Process

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

27.3.5 Transfer Process

The EPP Transfer command is used for several domain transfer related operations:

- Initiate a domain transfer
- Cancel a domain transfer
- Approve a domain transfer
- Reject a domain transfer.

To transfer a domain from one Registrar to another the following process is followed:

1. The gaining (new) Registrar submits a Transfer command, which includes the AuthInfo code of the domain name.
2. If the AuthInfo code is valid and the domain is not in a status that does not allow transfers the domain is placed into pendingTransfer status
3. A poll message notifying the losing Registrar of the pending transfer is sent to the Registrar's message queue
4. The domain remains in pendingTransfer status for up to 120 hours, or until the losing (current) Registrar Acks (approves) or Nack (rejects) the transfer request
5. If the losing Registrar has not Acked or Nacked the transfer request within the 120 hour timeframe, the Registry auto approves the transfer
6. The requesting Registrar may cancel the original request up until the transfer has been completed.

A transfer adds an additional year to the term of the domain. In the event that a transfer will cause the domain to exceed the 10 year maximum term, the Registry will add a partial term up to the 10 year limit. Unlike with the Renew operation, the Registry will not reject a transfer operation.

27.3.6 Deletion Process

A domain may be deleted from the SRS using the EPP Delete operation. The Delete operation will result

in either the domain being immediately removed from the database or the domain being placed in pendingDelete status. The outcome is dependent on when the domain is deleted. If the domain is deleted within the first five days (120 hours) of registration, the domain is immediately removed from the database. A deletion at any other time will result in the domain being placed in pendingDelete status and entering the Redemption Grace Period (RGP). Additionally, domains that are deleted within five days (120) hours of any billable (add, renew, transfer) transaction may be deleted for credit.

27.4 Applicable Time Elements

The following section explains the time elements that are involved.

27.4.1 Grace Periods

There are six grace periods:

Add Delete Grace Period (AGP)

-Renew-Delete Grace Period

Transfer Delete Grace Period

-Auto-Renew-Delete Grace Period

Auto Renew Grace Period

-Redemption Grace Period (RGP).

The first four grace periods listed above are designed to provide the Registrar with the ability to cancel a revenue transaction (add, renew, or transfer) within a certain period of time and receive a credit for the original transaction.

The following describes each of these grace periods in detail.

27.4.2 Add-Delete Grace Period

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

27.4.3 Renew-Delete Grace Period

The Renew-Delete Grace Period is associated with the date the Domain was renewed. Domains may be deleted for credit during the 120 hours after a renewal. The grace period is intended to allow

Registrars to correct domains that were mistakenly renewed. It should be noted that domains that are deleted during the renew grace period will be placed into pendingDelete and will enter the RGP (see below).

27.4.4 Transfer Delete Grace Period

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

27.4.5 Auto-Renew-Delete Grace Period

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

27.4.6 Auto-Renew Grace Period

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

27.4.7 Redemption Grace Period

The RGP is a special grace period that enables Registrars to restore domains that have been inadvertently deleted but are still in pendingDelete status within the Redemption Grace Period. All domains enter the RGP except those deleted during the AGP.

The RGP period is 30 days, during which time the domain may be restored using the EPP RenewDomain command as described below. Following the 30day RGP period the domain will remain in pendingDelete status for an additional five days, during which time the domain may NOT be restored. The domain is released from the SRS, at the end of the 5 day non-restore period. A restore fee applies and is detailed in the Billing Section. A renewal fee will be automatically applied for any domain past expiration.

Neustar has created a unique restoration process that uses the EPP Renew transaction to restore the domain and fulfill all the reporting obligations required under ICANN policy. The following describes the restoration process.

27.5 State Diagram

Figure 27 1 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 Applicant to determine the precise rules that meet the requirements of the TLD. Implementation of the lifecycle rules will be the responsibility of Development/Engineering team, with testing performed by the Quality Assurance team. Neustar's SRS implementation is very flexible and configurable, and in many case development is not required to support business rule changes.

The ".TECH" 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 ".TECH" registry.

28. Abuse Prevention and Mitigation

General Statement of Policy

Abuse within the registry will not be tolerated. DOT Tech, LLC will implement very strict policies and procedures to minimize abusive registrations and other activities that have a negative impact on Internet users. DOT Tech, LLC's homepages will provide clear contact information for its Abuse Team, and in accordance with ICANN policy DOT Tech, LLC shall host NIC.TECH, providing access to .TECH's WhoIs services, the Abuse Policy, and contact information for the Abuse Team.

Anti-Abuse Policy

DOT Tech, LLC will implement in its internal policies and its Registry Registrar Agreements (RRAs) that all registered domain names in the TLD will be subject to a Domain Name Anti-Abuse Policy ("Abuse Policy").

The Abuse Policy will provide DOT Tech, LLC with broad power to suspend, cancel, or transfer domain names that violate the Abuse Policy. DOT Tech, LLC will publish the Abuse Policy on its home website at NIC.TECH and clearly provide DOT Tech, LLC's Point of Contact ("Abuse Contact") and its contact information. This information shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of abuse complaints, and a telephone number and mailing address for the primary contact. DOT Tech, LLC will ensure that this information will be kept accurate and up to date and will be provided to ICANN if and when changes are made.

In addition, with respect to inquiries from ICANN-Accredited Registrars, the Abuse Contact shall handle requests related to abusive domain name practices.

Inquiries addressed to the Abuse Contact will be routed to DOT Tech, LLC's Legal Team who will review and if applicable remedy any Complaint regarding an alleged violation of the Abuse Policy as described in more detail below. DOT Tech, LLC will catalog all abuse communications in its CRM software using a ticketing system that maintains records of all abuse complaints indefinitely. Moreover, DOT Tech, LLC 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 state, at a minimum, that DOT Tech, LLC reserves the right to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary to ; (1) to protect the integrity and stability of the registry; (2) to comply with applicable laws, government rules or requirements, or court orders; (3) to avoid any liability, civil or criminal, on the part of DOT Tech, LLC, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) to correct mistakes made by the DOT Tech, LLC, registry services provider, or any Registrar in connection with a domain name registration; (5) during resolution of any dispute regarding the domain; and (6) if a Registrant's pre-authorization or payment fails; or (7) to prevent the bad faith use of a domain name that is identical to a registered trademark and being used to confuse users.

The Abuse Policy will define the abusive use of domain names to include, but not be limited to, the following activities:

- Illegal or fraudulent actions: use of the DOT Tech, LLC's or Registrar's services to violate the laws or regulations of any country, state, or infringe upon the laws of any other jurisdiction, or in a manner that adversely affects the legal rights of any other person;
- Spam: use of electronic messaging systems from email addresses from domains in the TLD 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;
- Trademark and Copyright Infringement: DOT Tech, LLC will take great care to ensure that trademark and copyright infringement does not occur within the .TECH TLD. DOT Tech, LLC will employ notice and takedown procedures based on the provisions of the Digital Millennium Copyright Act (DMCA) ;
- Phishing: use of counterfeit Web pages within the TLD that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data;
- Pharming: redirecting of unknowing users to fraudulent Web sites or services, typically through DNS hijacking or poisoning;
- Willful distribution of malware: 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.
- 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 DOT Tech, LLC;
- 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 denial-of-service attacks (DDoS attacks);
- Distribution of pornography;
- 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);
- Domain Kiting/Tasting: registration of domain names to test their commercial viability before returning them during a Grace Period;
- High Volume Registrations/Surveying: registration of multiple domain names in order to warehouse them for sale or pay-per-click websites in a way that can impede DOT Tech, LLC from offering them to legitimate users or timely services to other subscribers;
- Geographic Name: registering a domain name that is identical to a Geographic Name, as defined by Specification 5 of the Registry Agreement;
- Inadequate Security: registering and using a domain name to host a website that collects

third-party information but does not employ adequate security measures to protect third-party information in accordance with that geographic area's data and financial privacy laws;

- Front Running: Registrars mining their own web and WhoIs traffic to obtain insider information with regard to high-value second-level domains, which the Registrar will then register to itself or an affiliated third party for sale or to generate advertising revenue;
- WhoIs Accuracy: Intentionally inserting false or misleading Registrant information into the TLD's WhoIs database in connection with the bad faith registration and use of the domain in question;
- WhoIs Misuse: abusing access to the WhoIs database by using Registrant information for data mining purposes or other malicious purposes;
- Fake Renewal Notices; misusing WhoIs Registrant information to send bogus renewal notices to Registrants on file with the aim of causing the Registrant to spend unnecessary money or steal or redirect the domain at issue.

Domain Anti-Abuse Procedure

DOT Tech, LLC will provide a domain name anti-abuse procedure modeled after the DMCA's notice-and-takedown procedure.

At all times, DOT Tech, LLC will publish on its home website at NIC.TECH the Abuse Policy and the contact information for the Abuse Contact. Inquiries addressed to the Point of Contact will be addressed to and received by DOT Tech, LLC's Legal Team who will review and if applicable remedy any Complaint regarding an alleged violation of the Abuse Policy. DOT Tech, LLC will catalog all abuse communications and provide them to third parties only under limited circumstances, such as in response to a subpoena or other such court order or demonstrated official need by law enforcement.

Any correspondence ("Complaint") from a complaining party ("Complainant") to the Abuse Contact will be ticketed in DOT Tech, LLC's CRM software and relayed to DOT Tech, LLC's Abuse Team. A member of DOT Tech, LLC's Abuse Team will then send an email to the Complainant within forty-eight (48) hours of receiving the Complaint confirming receipt of the email and that DOT Tech, LLC will notify the Complainant of the results of the Complaint within ten (10) days of receiving the Complaint.

DOT Tech, LLC's Abuse Team will review the Complaint and give it a "quick look" to see if the Complaint reasonably falls within an abusive use as defined by the Abuse Policy. If not, the Contact will write an email to the Complainant within thirty-six (36) hours of sending the confirmation email that the subject of the complaint clearly does not fall within one of the delineated abusive uses as defined by the Abuse Policy and that DOT Tech, LLC considers the matter closed.

If the quick look does not resolve the matter, DOT Tech, LLC's Abuse Team will give the Complaint a full review. Any Registrant that has been determined to be in violation of DOT Tech, LLC policies shall be notified of the violation of such policy and their options to cure the violation.

Such notification shall state:

- 1) the nature of the violation;
- 2) the proposed remedy to the violation;
- 3) the time frame to cure the violation; and
- 4) the Registry's options to take subsequent action if the Registrant does not cure the violation.

If an abusive use is determined DOT Tech, LLC's Abuse Team will alert it's Registry services team to immediately cancel the resolution of the domain name. DOT Tech, LLC's Abuse Team will immediately notify the Registrant of the suspension of the domain name, the nature of the complaint, and provide the Registrant with the option to respond within ten (10) days or the domain will be canceled.

If the Registrant responds within ten (10) business days, it's response will be reviewed by the DOT Tech, LLC's Abuse Team for further review. If DOT Tech, LLC's Abuse Team is satisfied by the Registrant's response that the use is not abusive, DOT Tech, LLC's Abuse Team will submit a request by the registry services provider to reactivate the domain name. DOT Tech, LLC's Abuse Team will then notify the Complainant that its complaint was ultimately denied and provide the reasons for the denial. If the Registrant does not respond within ten (10) business days, DOT Tech, LLC will notify the registry services team to cancel the abusive domain name.

This Anti Abuse Procedure will not prejudice either party's election to pursue another dispute mechanism, such as URS or UDRP.

With the resources of DOT Tech, LLC's registry services personnel, DOT Tech, LLC 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 (1) 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 Application for rapid resolution of the request.

In the event such request involves any of the activities which can be validated by DOT Tech, LLC and involves the type of activity set forth in the Abuse Policy, the sponsoring Registrar is then given forty-eight (48) 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 48 hour period (i.e., is unresponsive to the request or refuses to take action), DOT Tech, LLC will place the domain on "serverHold".

Maintenance of Registration Criteria

- 1) All Registrants awarded a ".TECH" domain will agree to a one year minimum contract, which will need to be renewed on an annual basis. Renewal is the sole responsibility of the Registrant. Registrant's failing to renew their awarded domains by their expiration dates will be given a 60 day renewal grace period prior to their domain being revoked and returned to general availability.
- 2) DOT Tech, LLC is not liable or responsible in any way for any errors, omissions or any other actions by any third party (including any Registrar service) arising out of or related to a given Registrant's application for, registration of, renewal of, or failure to register or renew a particular domain name.
- 3) Through the registration process all Registrants will be expected to designate an administrative contact for their application, which would possess all the rights granted by DOT Tech, LLC or its designated agents to act in respect to the given domain including but not limited to managing the domain name or any services associated thereto. It is the Registrant's responsibility to update and maintain accurate contact information for their registrations.

Orphan Glue Removal

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 supports 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 the DNS. Therefore, when DOT Tech, LLC has written evidence of actual abuse of orphaned glue, DOT Tech, LLC will take action to remove those records from the zone to mitigate such malicious conduct.

DOT Tech, LLC's registry service operator will run a daily audit of entries in its DNS systems and compare 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 DOT Tech, LLC or its registry services operator becomes aware of actual abuse on orphaned glue after receiving written notification by a third party through its Abuse Contact or through its customer support, such glue records will be removed from the zone.

WhoIs Accuracy

DOT Tech, LLC will provide WhoIs accessibility in a reliable, consistent, and predictable fashion in order to promote Whois accuracy. The Registry will adhere to port 43 WhoIs Service Level Agreements (SLAs), which require that port 43 WHOIS service be highly accessible and fast.

DOT Tech, LLC will offer thick WhoIs services, in which all authoritative WhoIs data including contact data-is maintained at the registry. DOT Tech, LLC will maintain timely, unrestricted, and public access to accurate and complete WhoIs information, including all data objects as specified in

Specification 4. Moreover, prior to the release of any domain names, DOT Tech, LLC's Registrar will provide DOT Tech, LLC with an authorization code to verify eligible Registrants provide accurate Registrant contact information.

In order to further promote WhoIs accuracy, DOT Tech, LLC will offer a mechanism whereby third parties can submit complaints directly to the DOT Tech, LLC (as opposed to ICANN or the sponsoring Registrar) about inaccurate or incomplete WhoIs data. Such information shall be forwarded to the Registrar, who shall be required to address those complaints with their Registrants. Thirty days after forwarding the complaint to the Registrar, DOT Tech, LLC 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, DOT Tech, LLC reserves the right to cancel or suspend the applicable domain name(s) should DOT Tech, LLC determine that the domains are being used in a manner contrary to DOT Tech, LLC's abuse policy.

DOT Tech, LLC shall also require authentication and verification of all Registrant data. DOT Tech, LLC shall verify the certificates of incorporation, whether a corporation is in active status, contact information, e mail address, and, to the best of its abilities, determine whether address information supplied is accurate. Second-level domains in the TLD shall not be operational unless two (2) out of three (3) of the above authentication methods have been satisfied.

DOT Tech, LLC will also maintain historical databases of Registrants and associated information which have provided inaccurate WhoIs information. DOT Tech, LLC will endeavor to use this database to uncover patterns of suspicious registrations which DOT Tech, LLC shall then flag for further authentication or for review of the Registrant's use of the domain in question to ensure Registrant's use is consonant with DOT Tech, LLC's abuse policy.

In addition, DOT Tech, LLC's Abuse Team shall on its own initiative, no less than twice per year, perform a manual review of a random sampling of domain names within the applied-for TLD to test the accuracy of the WhoIs information. Although this will not include verifying the actual information in the WHOIS record, DOT Tech, LLC 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 Registrar, who shall be required to address those complaints with their Registrants. Thirty days after forwarding the complaint to the Registrar, the DOT Tech, LLC 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, DOT Tech, LLC reserves the right to suspend the applicable domain name(s) should DOT Tech, LLC determine that the Registrant is using the domain in question in a manner contrary to DOT Tech, LLC's abuse policy. DOT Tech, LLC shall also reserve the right to report such recalcitrant Registrar activities directly to ICANN.

Abuse Prevention and Mitigation - Domain Name Access

All domain name Registrants will have adequate controls to ensure proper access to domain functions.

In addition to the above, all domain name Registrants in the applied-for TLD will be required to name at least two (2) unique points of contact who are authorized to request and/or approve update, transfer, and deletion requests. The points of contact must establish strong passwords with the Registrar that must be authenticated before a point of contact will be allowed to process updates, transfer, and deletion requests. Once a process update, transfer, or deletion request is entered, the points of contact will automatically be notified when a domain has been updated, transferred, or deleted through an automated system run by DOT Tech, LLC's Registrar. Authentication of modified Registrant information shall be accomplished within 72 hours of receipt.

29. Rights Protection Mechanisms

DOT Tech, LLC is committed to implementing strong and integrated Rights Protection Mechanisms (RPM). Use of domain names that infringe upon the legal rights of others in the TLD will not be tolerated.

The nature of such uses creates security and stability issues for the registry, Registrars, and Registrants, as well as for users of the Internet in general. DOT Tech, LLC will protect the legal rights of others by implementing RPMs and anti abuse policies backed by robust responsiveness to complaints and requirements of DOT Tech, LLC's Registrars.

Trademark Clearinghouse

Each new gTLD Registry will be required to implement support for, and interaction with, the Trademark Clearinghouse ("Clearinghouse"). The 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.

Utilizing the 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 Claims 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.

Sunrise A Period

DOT Tech, LLC will offer segmented Sunrise Periods. The initial Sunrise Period will last [minimum 30 days] for owners of trademarks listed in the Clearinghouse to register domain names that consist of an identical match of their listed trademarks. All domain names registered during the Sunrise Period will be subject to DOT Tech, LLC's domain name registration policies. DOT Tech, LLC will assign 3-5 employees to specifically work as the Rights Protection Team, these employees will receive and authenticate all Sunrise Registrations. The DOT Tech, LLC RPM team will specifically deal with trademark protection issues and mitigate or assist in resolving any rights protection issues which arise during the Sunrise processes.

DOT Tech, LLC's Registrar will ensure that all Sunrise Registrants meet sunrise eligibility requirements (SERs), which will be verified by Clearinghouse data. The proposed SERs include: (i) ownership of a mark that is (a) nationally or regionally registered and for which proof of use, such as a declaration and a single specimen of current use was submitted to, and validated by, the 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, (ii) optional registry elected requirements concerning international classes of goods or services covered by registration; (iii) representation that all provided information is true and correct; and (iv) provision of data sufficient to document rights in the trademark.

Upon receipt of the Sunrise application, DOT Tech, LLC will issue a unique tracking number to the Registrar, which will correspond to that particular application. All applications will receive tracking numbers regardless of whether they are complete. Applications received during the Sunrise period will be accepted on a first-come, first-serve basis. Upon submission of all of the required information and documentation, Registrar will forward the information to DOT Tech, LLC's RPM Team for authentication. DOT Tech, LLC's RPM Team will review the information and documentation, verify the trademark information, and notify the potential Registrant of any deficiencies. If a Registrant does not cure any trademark-related deficiencies and/or respond by the means listed within one (1) week, DOT Tech, LLC will notify its Registrar and the domain name will be released for registration. DOT Tech, LLC 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 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, DOT Tech, LLC's RPM Team will review the Complaint to see if the Complaint reasonably asserts a legitimate challenge as defined by the SDRP. If not, DOT Tech, LLC's RPM Team will send an email to the Complainant within thirty-six (36) hours of sending the

confirmation email that the subject of the complaint clearly does not fall within one of the delineated grounds as defined by the SDRP and that DOT Tech, LLC considers the matter closed.

If the domain name is not found to have adequately met the SERs, DOT Tech, LLC RPM Team will alert the Registrar and registry services provider to immediately suspend the resolution of the domain name. Thereafter, DOT Tech, LLC's RPM Team will immediately notify the Sunrise Registrant of the suspension of the domain name, the nature of the complaint, and provide the Registrant with the option to respond within ten (10) days to cure the SER deficiencies or the domain name will be canceled.

If the Registrant responds within ten (10) business days, its response will be reviewed by DOT Tech, LLC's RPM Team to determine if the SERs are met. If DOT Tech, LLC's RPM Team is satisfied by the Registrant's response, DOT Tech, LLC's RPM Team will submit a request to the Registrar and the registry services provider to un-suspend the domain name. DOT Tech, LLC's RPM Team will then notify the Complainant that its complaint was ultimately denied and provide the reasons for the denial.

Names secured as described through the Sunrise AT/AD processes will result in the registration of resolving domain names at the registry. Names reserved through the Sunrise B process will not result in resolving domain name at DOT Tech, LLC. Rather, these names will be reserved and blocked from live use. The applied for string will resolve to an informational page informing visitors that the name is unavailable for registration and reserved from use.

Applications that fit the following criteria will be considered during the Sunrise A period: DOT Tech, LLC owns and operates an existing domain name in another gTLD or ccTLD, in connection with eligible commerce and satisfies the registration requirements described in Section 1.

Sunrise B

Applications that fit the following criteria will be considered during the Sunrise B period:

- a) Applicant holds valid trademark registrations or owns rights to a particular name and wishes to block the use of such name.
- b) The Applicant must seek to block a name that corresponds to the entire text of its trademark or the complete textual component of a graphical or compound trademark. Certain variances are permitted for trademarks containing spaces or special characters that are not available for domain names.

Founder's Program

Applications for the Founder's Program will be accepted after the close of the Sunrise Periods. Potential Registrants should understand that certain expectations, as described herein will accompany the issuance of a domain name under the Founder's Program and all registrations resulting from this program will be required to follow the below listed guidelines, which will be further described in their Program Agreement:

- a) Registrants awarded a domain through the Founder's Program must use their best efforts to launch a ".TECH" website within 30 days of signing the Program Agreement.
- b) In addition, each Registrant will be required to issue a press release announcing the launch of their ".TECH" Founder Website, concurrent with the launch of their ".TECH" Founder Website, said press release must be approved by DOT Tech, LLC;
- c) Founders are expected to proactively market and promote ".TECH" gTLD in a manner that is likely to produce widespread awareness of the unique advantages gained through the ".TECH" string.
- d) Founders will allow DOT Tech, LLC to use in good faith Founder's name, likeness, trademarks, logos, and Application contents (other than Confidential Information,) as well as other Founder information and content as may be mutually agreed, in DOT Tech, LLC's marketing, promotional and communications materials.

DOT Tech, LLC will randomly verify compliance of the above listed expectations and have the right to revoke any Founder's site, should they be deemed non-compliant. Additionally, DOT Tech, LLC may suspend or delete a Founder's site without prior notice to the Registrar or Registrant if the Founder's site is deemed in violation of any of DOT Tech's registration guidelines or policies. Registrants participating in the Founders program will receive 25% discounted registration, renewal pricing and term extensions (not to exceed 5 years) from DOT Tech's Registrars as recognition for their participation in the Founders Program.

Landrush

Landrush is a limited time opportunity for companies that want to secure a high value ".TECH" name for a small fee (above the basic registration cost). The landrush period will last 30 days.

Applications will be accepted and evaluated to determine if they meet the requirements for registration. At the end of the Landrush period domain names with only one application will be awarded directly to the Applicant. Domain names with two or more applications will proceed to a closed mini auction, between the respective Applicants, where the highest bidder wins.

General Availability Period

Applicant must meet all registration requirements.

Names will be awarded on a first-come, first serve basis which is determined as of the time of the

initial request, not when authentication occurs.

Domain Name Contentions

Name contentions will arise when both a Sunrise A and Sunrise B application are submitted for the same name, the following actions will be taken to resolve the contention.

- a) Both Applicants will be notified of the contention and the Sunrise A Applicant will be given first right to either register their requested domain or withdraw their application. A domain applied for under Sunrise A will, all else being equal, receive priority over the identical domain applied for under Sunrise B. Sunrise A names get priority over Sunrise B names.
- b) If the Sunrise Applicant chooses to register their name regardless of the contention, then the Sunrise B Applicant may choose to pursue further action independently of DOT Tech, LLC to contest the name. These processes may include UDRP or Civil Court and are not connected to DOT Tech's sunrise policies.
- c) If two Sunrise A Applicants apply for the same domain name (i.e., Delta Airlines and Delta Faucet both seek to be awarded the use of DELTA.TECH) then DOT Tech, LLC will notify both Applicants of the contention and proceed to an auction process as described in Section 9.
- d) If two Sunrise B Applicants apply for the same domain name (i.e., Delta Airlines and Delta Faucet, both seek to block the use of DELTA.UNO), then DOT Tech, LLC will accept both applications as valid and block the use of the indicated domain.

Appeal of Rejected Sunrise Applications

An Applicant can file a request for reconsideration within 10 days of the notification of DOT Tech, LLC's rejection. Reconsideration can be requested by completing a reconsideration form and filing a reconsideration fee with DOT Tech, LLC. Forms, fee information, and process documentation will be available on the DOT Tech, LLC website. Upon receipt of the reconsideration form and the corresponding fee, DOT Tech, LLC or its Agents will re-examine the application, and notify the Registrant of all findings or additional information needed. The Request for Reconsideration must be submitted through the Registrant's Registrar, and a reconsideration fee must be paid to DOT Tech, LLC.

Auctions

Sunrise A names found to be in contention as described above will result in Auction. DOT Tech, LLC plans to have a qualified third party conduct our auction processes, therefore the rules contained in this document are subject to change based on the selection of an auctioneer:

- a) All auction participants are expected to keep their account information current, throughout the auction process.
- b) Auction participants will receive up to date communication from the auctioneer as the auction progresses, bidding status changes, or issues arise.

Bidding

- a) Auctions will follow a standard process flow: scheduled (upcoming), open and closed.
- b) You will receive an "Auction Scheduled" notice at least ten (10) days prior to the scheduled auction start date. You will receive an "Auction Start" notice on the auction start date, which will indicate that you may begin placing bids through the interface. Once closed, the auction is complete and if you are the winning bidder, you will proceed to the payment process.
- c) If you choose to bid for a particular domain and you are the highest bidder at the end of an auction, you are obligated to complete the transaction and pay the Auctioneer the amount of your winning bid. Carefully consider your bids prior to placing them - bids are not retractable under any circumstances.
- d) If no bids are placed on a particular domain, the Registry will register the domain on behalf of the first customer (in the respective phase) to submit an application through a Registrar.

Extensions

- a) A normal auction period is anticipated to last a minimum of 7 (seven) days. However, in the event of significant auction activity, an auction close may extend during the last twenty-four (24) hours of scheduled operation to better need the volume of the auction.
- b) Auction extensions are meant to provide a mechanism that is fair for bidders in all time zones to respond to being outbid.
- c) An auction extension will occur whenever the auction lead changes in the last twenty-four (24) hours of the schedule of an auction. The close will be revised to reflect a new closing time set at twenty-four (24) hours after the change in auction lead occurred. Essentially, this means that a winning maximum bid has to remain unchallenged for a period of twenty-four (24) hours before the auction will close.
- d) It is important to note that extensions are not simply based on the auction value changing since this could occur as a result of proxy bidding where the same bidder retains their lead. In this case, the maximum bid has not changed, the leader has not changed and therefore no extension will occur.

Payment Default

In the event that you as the winning bidder decide not to honor your payment obligations (or in the event of a reversal of payment or a charge back by a credit card company or other payment provider)

on any outstanding balance, the Registry has the right to cancel any/all of your winning registrations for any .INC domain name, regardless of whether they have been paid for or not. You do not have the right to "pick and choose" the names you wish to keep or not keep. Winning an auction creates an obligation to remit payment. Failure to remit payment is a breach of your agreement.. You will lose any previously won domains and will no longer be allowed to bid on any current or future auctions sponsored by DOT Tech, LLC. Participants are encouraged therefore to consider carefully each bid submitted as any bid could be a winning bid.

Trademark Claims Service

DOT Tech, LLC will offer a Trademark Claims Service to provide maximum protection and value to rights holders. The Trademark Claims Service will be monitored and operated by DOT Tech, LLC's RPM Team that will receive all communications regarding the Trademark Claims Service and catalog them. DOT Tech, LLC's Registrar will review all domain name requests to determine if they are an identical match of a trademark filed with the Trademark Clearinghouse. 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 spaces, hyphens or underscores. Domain names that are plural forms of a mark, or that merely contain a mark, will not qualify as an identical match.

If the Registrar determines that a prospective domain name registration is identical to a mark registered in the Trademark Clearinghouse, the Registrar will be required to email a "Trademark Claims Notice" (Notice) in English to the prospective Registrant of the domain name and copy DOT Tech, LLC's RPM Team. The Notice will provide the prospective Registrant information regarding the trademark referenced in the Trademark Claims Notice to enhance understanding of the Trademark rights being claimed by the trademark holder. The Notice will be provided in real time without cost to the prospective Registrant.

After receiving the notice, the Registrar will provide the prospective Registrant five (5) days to reply to the Trademark Claims Service with a signed document that specifically warrants that: (i) the prospective Registrant has received notification that the mark 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. If the warranty document satisfies these requirements, the Registrar will effectuate the registration and notify DOT Tech, LLC's RPM Team.

After the effectuation of a registration that is identical to a mark listed in the Trademark Clearinghouse, the Registrar will provide clear notice to the trademark owner consisting of the domain name that has been registered and copy DOT Tech, LLC's RPM Team. The trademark owner then has the option of filing a Complaint under the Uniform Domain Name Dispute Resolution Policy (UDRP) or the Uniform Rapid Suspension System (URS).

Uniform Rapid Suspension System (URS)

DOT Tech, LLC will specify in the Registry Agreement, all RRAs, and all Registration Agreements used in connection with the TLD that it and its Registrars will abide by all decisions made by panels in accordance with the Uniform Rapid Suspension System (URS). DOT Tech, LLC's RPM Team will receive all URS Complaints and decisions, and will notify its Registrar to suspend all registrations determined by a URS panel to be infringing within a commercially reasonable time of receiving the decision. DOT Tech, LLC's RPM Team will catalog all abuse communications, but only provide them 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.

Uniform Domain Name Dispute Resolution Policy (UDRP)

DOT Tech, LLC will specify in the Registry Agreement, all Registry-Registrar Agreements, and Registration Agreements used in connection with the TLD that it will promptly abide by all decisions made by panels in accordance with the Uniform Domain Name Dispute Resolution Policy (UDRP). DOT Tech, LLC's RPM Team will receive all UDRP Complaints and decisions, and will notify its Registrar to cancel or transfer all registrations determined to be infringing within ten (10) business days of receiving the decision. DOT Tech, LLC's RPM Team will catalog all abuse communications, but only provide them 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.

Proven Registrars

In order to reduce abusive registrations and other activities that affect the legal rights of others, DOT Tech, LLC will only contract with ICANN-accredited Registrars. The Registrar, according to the RRA, will not be able to register any domain names, thus eliminating the possibility of front-running.

Pre-Authorization and Authentication

Registrant authentication shall occur in accordance with the registration eligibility criteria and the Anti-Abuse Policy for “.TECH” as set forth in Question 28.

The verification process is designed to prevent a prospective Registrant from providing inaccurate or incomplete data, such that, if necessary, the Registrant can be readily contacted regarding an infringing use of its site; indeed, the process (including verification of a Registrant’s certificate of incorporation) is designed to ensure that only qualified members of the community are permitted to register in the TLD.

Thick WhoIs

DOT Tech, LLC 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.

Takedown Procedure

DOT Tech, LLC will provide a Takedown Procedure modeled after the Digital Millennium Copyright Act’s notice and takedown procedure.

At all times, DOT Tech, LLC will publish on its home website at NIC.TECH contact information for receiving rights protection complaints (Complaint) from rights holders, including but not limited to trademark and copyright Complaints. Complaints will be addressed to and received by DOT Tech, LLC’s RPM Team who will catalogue and ticket in DOT Tech, LLC’s CRM software and review as outlined herein. DOT Tech, LLC will catalog all rights protection communications and only provide them 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.

Any Complaint from a rights holder will be relayed to DOT Tech, LLC’s RPM Team. A member of DOT Tech, LLC’s RPM Team will then send an email to the Complainant within forty-eight (48) hours of receiving the Complaint confirming receipt of the email, and that DOT Tech, LLC will notify the Complainant of the results of the Complaint within (10) days of receiving the Complaint.

After sending the confirmation email, DOT Tech, LLC’s RPM Team will review the Complaint. If DOT Tech, LLC or its Registrar determines that the registration was in bad faith, DOT Tech, LLC or its Registrar may cancel or suspend the resolution of the domain name. Bad faith registration includes, but is not limited to, the registration of a domain identical to a registered trademark where the Registrant has proceeded with registration after receipt of a Clearinghouse notice, as described above.

If the Registrant responds within ten (10) business days, its response will be reviewed by the DOT Tech, LLC’s RPM Team. If DOT Tech, LLC’s RPM Team is satisfied by the Registrant’s response that the content has been taken down or is not infringing, DOT Tech, LLC’s RPM Team will un suspend the domain name. DOT Tech, LLC’s RPM Team will then notify the Complainant that its complaint was ultimately denied and provide the reasons for the denial. If the Registrant does not respond within ten (10) business days, DOT Tech, LLC or its Registrar may cancel or suspend the resolution of the domain name.

This Takedown Procedure will not prejudice any party’s election to pursue another dispute mechanism, such as URS or UDRP, as set forth in DOT Tech, LLC’s response to Question 28.

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

30.(a).1 Security Policies

DOT Tech and our back-end operator, Neustar recognize the vital need to secure the systems and the integrity of the data in commercial solutions. The ".TECH" 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 ".TECH" 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 ".TECH"
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 ".TECH" 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 ".TECH". 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 ".TECH" 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.*

EXHIBIT E



New gTLD Application Submitted to ICANN by: Dot Tech LLC

Application Downloaded On: 23 Oct 2014

String tech

Application ID: 1-1670-76346

Applicant Information

1. Full legal name

[Dot Tech 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

<http://www.radixregistry.comc>

Primary Contact

6(a). Name

[Brijesh 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

Namit 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

Limited Liability Company

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

Unites States

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

Name	Position

Name	Position
Brijesh Joshi	Director & GM

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

Name	Position
Bhavin Turakhia	Founder
Brijesh Joshi	Director & GM
Namit Merchant	General Manager
Vishal Manjalani	Director & VP

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

Name	Position
Radix FZC	Not Applicable

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

Name	Position
Radix FZC	Not Applicable

Applied-for gTLD string

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

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

14B 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.

14C1. If an IDN, provide the language of the label (in English).

14C2 If an IDN, provide the language of the label (as referenced by ISO 639 1)

14D1. If an IDN, provide the script of the label (in English).

14D2. If an IDN, provide the script of the label (as referenced by ISO 15924).

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

15A. If an IDN, upload IDN tables for the proposed registry. An IDN table must include:

1. the applied-for gTLD string relevant to the tables,
2. the script or language designator (as defined in BCP 47),
3. table version number,
4. effective date (DD Month YYYY), and
5. contact name, email address, and phone number.

Submission of IDN tables in a standards-based format is encouraged.

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

15C. List any variants 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.

There are no known operational or rendering issues associated with our applied for string. We are relying on the proven capabilities of Neustar to troubleshoot and quickly eliminate these should they arise.

17. OPTIONAL.

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

18A. Describe the mission/purpose of your proposed gTLD.

The purpose of “.TECH” is to provide a dedicated online environment for the technology industry allowing businesses to create user friendly access to products, services and information instantaneously through accurate search engine classifications.

It is our mission that businesses bearing the “.TECH” gTLD string would become leaders in their market and be instantly differentiated online as tech savvy innovators, product suppliers, or service professionals.

The “.TECH” gTLD would provide a streamlined presentation of businesses primarily related to, or participating in technological advancements, the production of technology, technology support services, or the sale and distribution of technology products.

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

Technology is defined as the application of scientific knowledge for practical purposes, which is often relayed through the making, usage and knowledge of tools, machines, techniques, crafts, systems, or methods of organization in order to solve a problem or perform a specific function. The word technology comes from the combination of two Greek words, which translate to mean the study of art, skill, craft. Technology is a unique term in the sense that it can either be applied generally, or to a specific area such as construction technology, medical technology, or information technology.

Humans began to create technology through the conversion of natural resources to simple tools. Early forms of technology include the wheel, fire, the printing press, and electricity. By today's standards, these life altering inventions seem more industrial than technologically based, but they sparked the creation of global communication, world wide travel, and in general, the ability of humans to control their external environment. When we compare them to the technological advancements in the modern world, we begin to see technology trending away from necessity -based creations and entering the realms of entertainment, leisure, and design.

Technology has impacted basically every aspect of our lives. From televisions to automobiles, coffee makers to cell phones; consumers worldwide employ technology to help them work faster, relax more, and entertain themselves. Additionally, businesses use technology to mainstream production processes, track their client base, and compile records. Hospitals, governments, schools, and homes benefit hourly from growing technology advancements, and society as a whole is increasingly dependent on the luxuries produced by these processes.

According to the National Science Institute, technology- intensive industries play a significant role in the global economy, representing a growing share of many countries' total economic activity. In 2010, tech intensive-industries represented 30% of the world's gross domestic product. While the United States, Europe and Japan comprise the largest conglomerate of world economic growth in the tech industry, we are also able to see significant industry increases in developing economies such as India, China and Russia. Industries related to technology transcend genre and can be identified in every industry sector in the world. While it is easy to equate technology to specific products we must also consider knowledge based tech industries. Information based technology has seen a steady increase in growth from 1995-2010 and currently accounts for trillions of dollars in revenue worldwide.

When we consider the prevalence of tech related businesses, departments, and information worldwide and the rate at which domain registration has increased in the last ten years (resulting in overcrowding and a general lack of naming availability), we begin to see the need for industry classifications online such as “.TECH”. “.TECH” will not only open the door for increased online naming abilities, it will also allow consumers to easily locate specific products and services through increased search engine classifications. Further, by developing specific industry classifications such as “.TECH” , advertisers will have increased confidence that they are reaching their target markets, thus increasing advertising revenue across the board for online retailers.

With these thoughts in mind, we at DOT Tech, LLC believe that it is essential for the technology industry to become a leader in this Internet transition. On average, Google reports that there

are over 45 million searches performed per month which include the word 'tech', resulting in a monthly volume of page views totaling well over 3 billion clicks. The opportunity to enhance the consumer experience while driving competition and information distribution in our market is paramount, and we are excited to be apart of this evolution.

In order to achieve our goals and build name recognition, DOT Tech will be implementing a robust marketing initiative, focused on enhancing the value of the “.TECH” gTLD, while positioning “.TECH” to become an industry “must -have” in assisting businesses to gain market share and exposure.

Within six years of the “.TECH” launch, it is our goal to register 70%+ of all tech industry related companies with a minimum of one “.TECH” gTLD. This achievement would solidify our mission statement and serve to differentiate the Internet in a much needed and effective way.

To do so, the following marketing strategies will be put in place:

- 1) Build strong relationships with Registrar services in order to capture new domain registrations applicable to “.TECH”.
- 2) Create a prominent and consistent image representative of our mission and expressed clearly through branding, advertisements, and corporate relationships.
- 3) Secure “key” Registrants through our Founders program (described further in question 29 of this application) that will act as innovative leaders to assist us in appropriately exposing our target audience to the existence of “.TECH”.
- 4) Cultivate relationships with both domestic and global technology and information technology organizations. Partnerships with these organizations and others like them would increase DOT Tech’s knowledge base in regards to efficiently meeting the needs of the technology industry consumers and business owners.
- 5) Partner with global marketing firms to ensure a wide reaching and effective marketing campaign. This process would allow DOT Tech to efficiently structure our marketing processes to reach the desired Registrants.
- 6) Increase exposure for “.TECH” by creating a strong international presence through attendance at conferences appropriate to our visibility in the market.
- 7) Create a consistent presence in all tech-related trade publications and sponsorship of well-attended tech-related events.
- 8) We intend to implement a highly focused/ targeted marketing blitz to the industry sub divisions associated with technology production, support, services, implementation and consumer retail in order to assist them in implementing and utilizing the “.TECH” gTLD.

It is our goal to provide an efficient and secure registration process by minimizing the input required by the Registrant and creating a streamlined application process. In order to do so and uphold the integrity of our mission to provide instant access to members of the technology industry, DOT Tech will implement the following registration guidelines and naming conventions:

- 1) .TECH registrations will be restricted to individuals, businesses, and organizations that are active members of the technology industry. “Active” can be defined, in this context, as any individual, business or organization wishing to provide technology related industry information, services, or products online.
- 2) Registrants will be asked to submit, at minimum, their contact information and to agree to a statement indicating that it is their intention to utilize their “.TECH” domain for the promotion, distribution, or exchange of information, products or services directly connected to the technology industry.
- 3) Content on all awarded “.TECH” sites is expected to primarily represent the Registrant’s connection to the technology industry. Sites will be randomly selected for review to ensure compliance with this guideline. Should Registrants be found in violation of this guideline, they will be notified in writing of the violation and given a 30 days to order to correct the content deficiencies of their site. If Registrants are unable to comply with this guideline within the 30 day probationary period, DOT Tech, LLC will revoke the Registrant’s domain name and it will be returned to general availability. Should a Registrant’s domain name be revoked due to their content deficiencies, all funds paid by the Registrant to date will be considered non-refundable. DOT Tech, LLC or it’s designated agent will perform all tasks related to content monitoring in order to not further burden our registrar partners.
- 4) Should DOT Tech, LLC discover at any point that a Registrant has falsely represented

themselves as an individual, business, or organization related to the technology industry, their awarded domain will be immediately revoked and returned to general availability. Should a Registrant's domain be revoked due their false representation of their industry relationship, all funds paid by the Registrant to date will be considered non-refundable.

5) Registrants should understand that name availability is not guaranteed and that names will be issued on a first come, first served basis. Should a Registrant's requested name be unavailable, the Registrant will be offered the option of re-wording, changing, or adapting their initial naming request until a suitable solution is found.

6) Registrants will not be allowed to register names that infringe on the legal rights of other individuals or companies, allude to criminal activities, or contain in any part racially offensive language.

7) DOT Tech, LLC reserves the right to deny, cancel, or transfer any registration or transaction (as more fully described in our Abuse Policies in question 28 below), 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 applicable laws, government rules or requirements, or court orders; (3) to avoid any liability, civil or criminal, on the part of DOT Tech, LLC, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) to correct mistakes made by the DOT Tech, LLC, registry services provider, or any Registrar in connection with a domain name registration; (5) during resolution of any dispute regarding the domain; and (6) if a Registrant's pre authorization or payment fails; or (7) to prevent the bad faith use of a domain name that is identical to a registered trademark and being utilized to confuse users.

8) DOT Tech's registry services operator will provide thick WHOIS services that are fully compliant with RFC 3912 and with Specifications 4 and 10 of the Registry Agreement. Additionally, DOT Tech, LLC will provide a Web-based WHOIS application, which will be located at www.whois.tech. The WHOIS Web application will be an intuitive and easy to use application. A complete description of these services can be found in Question 26 below.

9) All Registrants awarded a ".TECH" domain will agree to a one year minimum contract, which will need to be renewed on an annual basis. Renewal is the sole responsibility of the Registrant. Registrant's failing to renew their awarded domains by their expiration dates will be given a 60-day renewal grace period prior to their domain being revoked and returned to general availability.

10) DOT Tech, LLC is not liable or responsible in any way for any errors, omissions or any other actions by any third party (including any Registrar service) arising out of, or related to a given Registrant's application for, registration of, renewal of, or failure to register or renew a particular domain name.

11) Through the registration process, all Registrants will be expected to designate an administrative contact for their application, which would possess all the rights granted by DOT Tech, LLC or its designated agents to act in respect to the given domain including, but not limited to, managing the domain name or any services associated thereto.

11) DOT Tech, LLC will implement a reserved names policy consisting of both names DOT Tech, LLC wishes to reserve for our own purposes as the registry operator and names protected by ICANN. DOT Tech, LLC will respect all ICANN reserved names including, but not limited to, two letter country codes and existing TLD's. Additionally, DOT Tech, LLC will seek ICANN approval on any additional names we plan to reserve in order to appropriately secure them prior to the opening of general availability.

DOT Tech, LLC will additionally implement a series of Rights Protection Mechanisms (RPM) included, but not limited to; support for and interaction with the Trademark Clearinghouse ("Clearinghouse"), use of the Trademark Claims Service, segmented Sunrise Periods allowing for the owners of trademarks listed in the Clearinghouse to register domain names that consist of an identical match of their listed trademarks, subsequent Sunrise Periods to give trademark owners or Registrants that own the rights to a particular name the ability to block the use of such name, stringent take-down services and Uniform Dispute Resolution Policies.

18C. What operating rules will you adopt to eliminate or minimize social costs (e.g., time or financial resource costs, as well as various types of consumer vulnerabilities)? What other steps

will you take to minimize negative consequences/costs imposed upon consumers?

DOT Tech, LLC will collect personal information from its Registrants via any of our approved Registrars. In order to maintain the integrity of the “.TECH” gTLD and minimize the negative consequences to consumers and business owners, the following policies will be adhered to:

- a) No information collected from our Registrants will be used for marketing purposes.
- b) Data collected will not be traded or sold.
- c) All data collected on any Registrant will be available to the Registrant free of charge.
- d) Registrants will be allowed to address and correct data inaccuracies as needed.
- e) All data will be kept secure.

DOT Tech, LLC will strictly uphold the rules set forth in their registration guidelines in order to accurately service our Registrants and mitigate any negative consequences to consumers or Internet users.

DOT Tech, LLC does not plan to offer registrations to Registrants directly. Therefore, our pricing commitments will be made within our Registry Registrar Agreements. It is our intention that these commitments will percolate down to Registrants directly and that the contractual commitments contained within our Registry-Registrar agreements will be reflected in the retail sale process of our gTLD, thus minimizing the negative consequences that might be imposed on Registrants via the retail process.

DOT Tech plans to offer bulk registration benefits to Registrars during the first 6 months of operation. Registrars wishing to purchase bulk registrations of 1,000 names or more would be offered a 5% discount at the time of purchase. Additionally, DOT Tech, through our founders program will provide a 25% discount to founders’ participants as a participation incentive. It is possible that DOT Tech would offer additional pricing benefits from time to time as relative to the market. All future pricing discounts not detailed in this application will be submitted through the appropriate ICANN channels for approval prior to introduction to the market.

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

No

20A. Provide the name and full description of the community that the applicant is committing to serve. In the event that this application is included in a community priority evaluation, it will be scored based on the community identified in response to this question. The name of the community does not have to be formally adopted for the application to be designated as community based

20B. Explain the applicant’s relationship to the community identified in 20(a).

20C. Provide a description of the community-based purpose of the applied-for gTLD.

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

20E. Provide a complete description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD. Policies and enforcement mechanisms are expected to constitute a coherent set.

20F Attach any written endorsements for the application from established institutions representative of the community identified in 20(a). An applicant may submit written endorsements by multiple institutions, if relevant to the community

21A. Is the application for a geographic name?

No

22. Describe proposed measures for protection of geographic names at the second and other levels in the applied for gTLD This should include any applicable rules and procedures for reservation and/or release of such names.

DOT Tech, LLC has thoroughly reviewed ISO 3166-1 and ISO 3166-2, relevant UN documents on the standardization of geographic names, GAC correspondence relating to the reservation of geographic names in the .INFO TLD, and understands its obligations under Specification 5 of the draft Registry Agreement. DOT Tech shall implement measures similar to those used to protect geographic names in the .INFO TLD by reserving and registering to itself all the geographic place names found in ISO 3166 and official country names as specified by the UN. DOT Tech has already discussed this proposed measure of protecting geographic names with its registry services provider, Neustar, and has arranged for such reservation to occur as soon after delegation as is technically possible.

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 Applicant then relay this request to ICANN. At this point, DOT Tech would wait for the approval of the GAC and of ICANN before proceeding to delegate the domain at issue.

23. Provide name and full description of all the Registry Services to be provided. Descriptions should include both technical and business components of each proposed service, and address any potential security or stability concerns.

The following registry services are customary services offered by a registry operator:

- A. Receipt of data from registrars concerning registration of domain names and name servers.
- B. Dissemination of TLD zone files.
- C. Dissemination of contact or other information concerning domain name registrations (e.g., port-43 WHOIS, Web- based Whois, RESTful Whois service).
- D. Internationalized Domain Names, where offered.
- E. DNS Security Extensions (DNSSEC). The applicant must describe whether any of these registry services are intended to be offered in a manner unique to the TLD.

Additional proposed registry services that are unique to the registry must also be described.

23.1 Introduction

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

- 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). [Optional should be deleted if not being offered].

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 ".TECH" 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

DOT Tech 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 ".TECH". 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

DOT Tech 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 ".TECH" 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

DOT Tech, 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

DOT Tech will not be offering services that are unique to ".TECH".

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.

24. Shared Registration System (SRS) Performance: describe

- the plan for operation of a robust and reliable SRS. SRS is a critical registry function for enabling multiple registrars to provide domain name registration services in the TLD. SRS must include the EPP interface to the registry, as well as any other interfaces intended to be provided, if they are critical to the functioning of the registry. Please refer to the requirements in Specification 6 (section 1.2) and Specification 10 (SLA Matrix) attached to the Registry Agreement; and
 - resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).A complete answer should include, but is not limited to:
 - A high-level SRS system description;

- Representative network diagram(s);
- Number of servers;
- Description of interconnectivity with other registry systems;
- Frequency of synchronization between servers; and
- Synchronization scheme (e.g., hot standby, cold standby).

24.1 Introduction

DOT Tech has partnered with Neustar, Inc ("Neustar"), an experienced TLD registry operator, for the operation of the ".TECH" 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 ".TECH" 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, DOT Tech 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 as a result the team is intimately familiar with its operations.

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

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

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

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

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

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

Figure 24-1 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 ".TECH" 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 ".TECH".

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 ".TECH" 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, RDNS (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 ".TECH" 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 ".TECH" 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 ".TECH" registry.

25. Extensible Provisioning Protocol (EPP): provide a detailed description of the interface with registrars, including how the applicant will comply with EPP in RFCs 3735 (if applicable), and 5730-5734.

If intending to provide proprietary EPP extensions, provide documentation consistent with RFC 3735, including the EPP templates and schemas that will be used.

Describe resourcing plans (number and description of personnel roles allocated to this area).

A complete answer is expected to be no more than 5 pages. If there are proprietary EPP extensions, a complete answer is also expected to be no more than 5 pages per EPP extension.

25.1 Introduction

DOT Tech'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 DOT Tech is provided with an unparalleled EPP based registry. The following discussion explains the EPP interface which will be used for the ".TECH" 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

[Default Response]

The ".TECH" 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 ".TECH" 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 ".TECH" 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 ".TECH" registry.

26. Whois: describe

- how the applicant will comply with Whois specifications for data objects, bulk access, and lookups as defined in Specifications 4 and 10 to the Registry Agreement;
- how the Applicant's Whois service will comply with RFC 3912; and
- resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

A complete answer should include, but is not limited to:

- A high-level Whois system description;
- Relevant network diagram(s);
- IT and infrastructure resources (e.g., servers, switches, routers and other components);
- Description of interconnectivity with other registry systems; and

Frequency of synchronization between servers.

To be eligible for a score of 2, answers must also include:

- Provision for Searchable Whois capabilities; and
- A description of potential forms of abuse of this feature, how these risks will be mitigated, and the basis for these descriptions

A complete answer is expected to be no more than 5 pages

DOT Tech, LLC 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 and relevant RFCs.

DOT Tech, LLC'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, the WHOIS service provided by DOT Tech, LLC's registry services operator has been designed from the ground up to display as much information as required by ICANN and respond to a very stringent availability and performance requirement.

Some of the key features of DOT Tech, LLC's WHOIS services will include:

- Fully compliant with all relevant RFCs including 3912;
- Production proven, highly flexible, and scalable (DOT Tech, LLC's back-end registry services provider has 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; and
- Search capabilities (e.g., IDN, registrant data) that mitigate potential forms of abuse as discussed below.

DOT Tech, LLC's registry services operator will provide thick WHOIS services that are fully compliant with RFC 3912 and with Specifications 4 and 10 of the Registry Agreement.

DOT Tech, LLC's WHOIS service will support port 43 queries, and will be optimized for speed using an in memory database and a master slave architecture between SRS and WHOIS slaves. RFC 3912 is a simple text based protocol over TCP that describes the interaction between the server and client on port 43. DOT Tech, LLC's registry services operator currently processes millions of WHOIS queries per day.

In addition to the WHOIS Service on port 43, DOT Tech, LLC will provide a Web-based WHOIS application, which will be located at www.whois.tech. This WHOIS Web application will be an intuitive and easy to use application for the general public to use. The WHOIS Web application provides all of the features available in the port 43 WHOIS. This includes full and partial search on:

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

The WHOIS web application will also provide features not available on the port 43 service. These include:

- Extensive support for international domain names (IDN)
- Ability to perform WHOIS lookups on the actual Unicode IDN
- Display of the actual Unicode IDN in addition to the ACE-encoded name
- A Unicode to Punycode and Punycode to Unicode translator
- An extensive FAQ
- A list of upcoming domain deletions

DOT Tech, LLC will also provide a searchable web-based WHOIS service in accordance with Specification 4 Section 1.8 The application will enable users to search the WHOIS directory to find exact or partial matches using any one or more of the following fields:

- Domain name
- 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.)
- Registrar ID
- Name server name and IP address
- Internet Protocol addresses
- The system will also allow search using non Latin character sets which are compliant with IDNA specification

The WHOIS user will be able to 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 and their WHOIS information will quickly be returned to the user.

In order to reduce abuse for this feature, only authorized users will have access to the Whois search features after providing a username and password. DOT Tech, 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, which will make access to the zone files in bulk via FTP to any person or organization that signs and abides by a Zone File Access (ZFA) Agreement with the registry. Contracted gTLD registries will provide this access daily and at no charge.

DOT Tech, LLC will also provide ICANN and any emergency operators with up to date Registration Data on a weekly basis (the day to be designated by ICANN). Data will include data committed as of 00:00:00 UTC on the day previous to the one designated for retrieval by ICANN. The file(s) will be made available for download by SFTP, unless ICANN requests other means in the future. DOT Tech, LLC's Legal Team consisting of 3 dedicated employees, will regularly monitor the registry service provider to ensure that they are providing the services as described above. This will entail random monthly testing of the WHOIS port 43 and Web-based services to ensure that they meet the ICANN Specifications and RFCs as outlined above, if not, to follow up with the registry services provider to ensure that they do. As the relevant WHOIS will only contain DOT Tech, LLC's information, DOT Tech, LLC's WHOIS services will necessarily be in compliance with any applicable privacy laws or policies.

27 Registration Life Cycle provide a detailed description of the proposed registration lifecycle for domain names in the proposed gTLD. The description must:

- explain the various registration states as well as the criteria and procedures that are used to change state;
- describe the typical registration lifecycle of create/update/delete and all intervening steps such as pending, locked, expired, and transferred that may apply;
- clearly explain any time elements that are involved for instance details of add grace or redemption grace periods, or notice periods for renewals or transfers; and
- describe resourcing plans for this aspect of the criteria (number and description of personnel roles allocated to this area).

The description of the registration lifecycle should be supplemented by the inclusion of a state diagram, which captures definitions, explanations of trigger points, and transitions from state to state

If applicable, provide definitions for aspects of the registration lifecycle that are not covered by standard EPP RFCs

A complete answer is expected to be no more than 5 pages.

27.1 Registration Life Cycle

27.1.1 Introduction

".TECH" 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 ".TECH".

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 ".TECH" registry per the defined ".TECH" 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 ".TECH" 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 ".TECH" 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 ".TECH" registry.

Hold Removes the domain from the DNS zone.

-UpdateProhibited Prevents the object from being modified by an Update command.

TransferProhibited Prevents the object from being transferred to another Registrar by the Transfer command.

-RenewProhibited Prevents a domain from being renewed by a Renew command.

-DeleteProhibited Prevents the object from being deleted by a Delete command.

The lifecycle of a domain begins with the registration of the domain. All registrations must follow the EPP standard, as well as the specific business rules described in the response to Question 18 above. Upon registration a domain will either be in an active or inactive state. Domains in an active state are delegated and have their delegation information published to the zone. Inactive domains either have no delegation information or their delegation information 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 ".TECH" registry will implement a standard domain lifecycle found in most gTLD registries today. There are five possible domain states:

-Active

Inactive

-Locked

Pending Transfer

-Pending Delete.

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

27.2.2 Active State

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

27.2.3 Inactive State

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

27.2.4 Locked State

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

27.2.5 Pending Transfer State

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

27.2.6 Pending Delete State

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

27.3 Typical Registration Lifecycle Activities

27.3.1 Domain Creation Process

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

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

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

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

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

27.3.2 Update Process

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

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

-Domain statuses

Registrant ID

-Administrative Contact ID

Billing Contact ID

-Technical Contact ID

Nameservers

-AuthInfo

Additional Registrar provided fields.

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

27.3.4 Renew Process

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

27.3.5 Transfer Process

The EPP Transfer command is used for several domain transfer related operations:

- Initiate a domain transfer
- Cancel a domain transfer
- Approve a domain transfer
- Reject a domain transfer.

To transfer a domain from one Registrar to another the following process is followed:

1. The gaining (new) Registrar submits a Transfer command, which includes the AuthInfo code of the domain name.
2. If the AuthInfo code is valid and the domain is not in a status that does not allow transfers the domain is placed into pendingTransfer status
3. A poll message notifying the losing Registrar of the pending transfer is sent to the Registrar's message queue
4. The domain remains in pendingTransfer status for up to 120 hours, or until the losing (current) Registrar Ack (approves) or Nack (rejects) the transfer request
5. If the losing Registrar has not Acker or Nacker 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 Applicant to determine the precise rules that meet the requirements of the TLD. Implementation of the lifecycle rules will be the responsibility of Development/Engineering team, with testing performed by the Quality Assurance team. Neustar's SRS implementation is very flexible and configurable, and in many case development is not required to support business rule changes.

The ".TECH" 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 ".TECH" registry.

28. Abuse Prevention and Mitigation: Applicants should describe the proposed policies and procedures to minimize abusive registrations and other activities that have a negative impact on Internet users. A complete answer should include, but is not limited to:

- An implementation plan to establish and publish on its website a single abuse point of contact responsible for addressing matters requiring expedited attention and providing a timely response to abuse complaints concerning all names registered in the TLD through all registrars of record, including those involving a reseller;
- Policies for handling complaints regarding abuse;
- Proposed measures for removal of orphan glue records for names removed from the zone when provided with evidence in written form that the glue is present in connection with malicious conduct (see Specification 6); and
- Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

To be eligible for a score of 2, answers must include measures to promote Whois accuracy as well as measures from one other area as described below.

- Measures to promote Whois accuracy (can be undertaken by the registry directly or by registrars via requirements in the Registry-Registrar Agreement (RRA)) may include, but are not limited to
 - Authentication of registrant information as complete and accurate at time of registration. Measures to accomplish this could include performing background checks, verifying all contact information of principals mentioned in registration data, reviewing proof of establishment documentation, and other means
 - Regular monitoring of registration data for accuracy and completeness, employing authentication methods, and establishing policies and procedures to address domain names with inaccurate or incomplete Whois data; and
 - If relying on registrars to enforce measures, establishing policies and procedures to ensure compliance, which may include audits, financial incentives, penalties, or other means. Note that the requirements of the RAA will continue to apply to all ICANN accredited registrars.
- A description of policies and procedures that define malicious or abusive behavior, capture metrics, and establish Service Level Requirements for resolution, including service levels for responding to law enforcement requests. This may include rapid takedown or suspension systems and sharing information regarding malicious or abusive behavior with industry partners;
- Adequate controls to ensure proper access to domain functions (can be undertaken by the registry directly or by registrars via requirements in the Registry Registrar Agreement (RRA)) may include, but are not limited to:
 - Requiring multi factor authentication (i.e., strong passwords, tokens, one time passwords) from registrants to process update, transfers, and deletion requests;
 - Requiring multiple, unique points of contact to request and/or approve update, transfer, and deletion requests; and
 - Requiring the notification of multiple, unique points of contact when a domain has been updated, transferred, or deleted.

A complete answer is expected to be no more than 20 pages

General Statement of Policy

Abuse within the registry will not be tolerated. DOT Tech, LLC will implement very strict policies and procedures to minimize abusive registrations and other activities that have a negative impact on Internet users. DOT Tech, LLC's homepages will provide clear contact information for its Abuse Team, and in accordance with ICANN policy DOT Tech, LLC shall host NIC.TECH, providing access to .TECH's WhoIs services, the Abuse Policy, and contact information for the Abuse Team.

Anti-Abuse Policy

DOT Tech, LLC will implement in its internal policies and its Registry Registrar Agreements (RRAs) that all registered domain names in the TLD will be subject to a Domain Name Anti-Abuse Policy ("Abuse Policy").

The Abuse Policy will provide DOT Tech, LLC with broad power to suspend, cancel, or transfer domain names that violate the Abuse Policy. DOT Tech, LLC will publish the Abuse Policy on its home website at NIC.TECH and clearly provide DOT Tech, LLC's Point of Contact ("Abuse Contact") and its contact information. This information shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of abuse complaints, and a telephone number and mailing address for the primary contact. DOT Tech, LLC will ensure that this information will be kept accurate and up to date and will be provided to ICANN if and when changes are made.

In addition, with respect to inquiries from ICANN Accredited Registrars, the Abuse Contact shall handle requests related to abusive domain name practices.

Inquiries addressed to the Abuse Contact will be routed to DOT Tech, LLC's Legal Team who will

review and if applicable remedy any Complaint regarding an alleged violation of the Abuse Policy as described in more detail below. DOT Tech, LLC will catalog all abuse communications in its CRM software using a ticketing system that maintains records of all abuse complaints indefinitely. Moreover, DOT Tech, LLC 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 state, at a minimum, that DOT Tech, LLC reserves the right to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary to ; (1) to protect the integrity and stability of the registry; (2) to comply with applicable laws, government rules or requirements, or court orders; (3) to avoid any liability, civil or criminal, on the part of DOT Tech, LLC, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) to correct mistakes made by the DOT Tech, LLC, registry services provider, or any Registrar in connection with a domain name registration; (5) during resolution of any dispute regarding the domain; and (6) if a Registrant's pre-authorization or payment fails; or (7) to prevent the bad faith use of a domain name that is identical to a registered trademark and being used to confuse users.

The Abuse Policy will define the abusive use of domain names to include, but not be limited to, the following activities:

- Illegal or fraudulent actions: use of the DOT Tech, LLC's or Registrar's services to violate the laws or regulations of any country, state, or infringe upon the laws of any other jurisdiction, or in a manner that adversely affects the legal rights of any other person;
- Spam: use of electronic messaging systems from email addresses from domains in the TLD 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;
- Trademark and Copyright Infringement: DOT Tech, LLC will take great care to ensure that trademark and copyright infringement does not occur within the .TECH TLD. DOT Tech, LLC will employ notice and takedown procedures based on the provisions of the Digital Millennium Copyright Act (DMCA) ;
- Phishing: use of counterfeit Web pages within the TLD that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data;
- Pharming: redirecting of unknowing users to fraudulent Web sites or services, typically through DNS hijacking or poisoning;
- Willful distribution of malware: 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.
- 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 DOT Tech, LLC;
- 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 denial-of-service attacks (DDoS attacks);
- Distribution of pornography;
- 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);
- Domain Kiting/Tasting: registration of domain names to test their commercial viability before returning them during a Grace Period;
- High Volume Registrations/Surveying: registration of multiple domain names in order to warehouse them for sale or pay-per-click websites in a way that can impede DOT Tech, LLC from offering them to legitimate users or timely services to other subscribers;
- Geographic Name: registering a domain name that is identical to a Geographic Name, as defined by Specification 5 of the Registry Agreement;
- Inadequate Security: registering and using a domain name to host a website that collects third-party information but does not employ adequate security measures to protect third-party information in accordance with that geographic area's data and financial privacy laws;
- Front Running: Registrars mining their own web and WhoIs traffic to obtain insider information with regard to high-value second-level domains, which the Registrar will then register to itself or an affiliated third party for sale or to generate advertising revenue;

- WhoIs Accuracy: Intentionally inserting false or misleading Registrant information into the TLD's WhoIs database in connection with the bad faith registration and use of the domain in question;
- WhoIs Misuse: abusing access to the WhoIs database by using Registrant information for data mining purposes or other malicious purposes;
- Fake Renewal Notices; misusing WhoIs Registrant information to send bogus renewal notices to Registrants on file with the aim of causing the Registrant to spend unnecessary money or steal or redirect the domain at issue.

Domain Anti-Abuse Procedure

DOT Tech, LLC will provide a domain name anti-abuse procedure modeled after the DMCA's notice-and-takedown procedure.

At all times, DOT Tech, LLC will publish on its home website at NIC.TECH the Abuse Policy and the contact information for the Abuse Contact. Inquiries addressed to the Point of Contact will be addressed to and received by DOT Tech, LLC's Legal Team who will review and if applicable remedy any Complaint regarding an alleged violation of the Abuse Policy. DOT Tech, LLC will catalog all abuse communications and provide them to third parties only under limited circumstances, such as in response to a subpoena or other such court order or demonstrated official need by law enforcement.

Any correspondence ("Complaint") from a complaining party ("Complainant") to the Abuse Contact will be ticketed in DOT Tech, LLC's CRM software and relayed to DOT Tech, LLC's Abuse Team. A member of DOT Tech, LLC's Abuse Team will then send an email to the Complainant within forty-eight (48) hours of receiving the Complaint confirming receipt of the email and that DOT Tech, LLC will notify the Complainant of the results of the Complaint within ten (10) days of receiving the Complaint.

DOT Tech, LLC's Abuse Team will review the Complaint and give it a "quick look" to see if the Complaint reasonably falls within an abusive use as defined by the Abuse Policy. If not, the Contact will write an email to the Complainant within thirty-six (36) hours of sending the confirmation email that the subject of the complaint clearly does not fall within one of the delineated abusive uses as defined by the Abuse Policy and that DOT Tech, LLC considers the matter closed.

If the quick look does not resolve the matter, DOT Tech, LLC's Abuse Team will give the Complaint a full review. Any Registrant that has been determined to be in violation of DOT Tech, LLC policies shall be notified of the violation of such policy and their options to cure the violation.

Such notification shall state:

- 1) the nature of the violation;
- 2) the proposed remedy to the violation;
- 3) the time frame to cure the violation; and
- 4) the Registry's options to take subsequent action if the Registrant does not cure the violation.

If an abusive use is determined DOT Tech, LLC's Abuse Team will alert it's Registry services team to immediately cancel the resolution of the domain name. DOT Tech, LLC's Abuse Team will immediately notify the Registrant of the suspension of the domain name, the nature of the complaint, and provide the Registrant with the option to respond within ten (10) days or the domain will be canceled.

If the Registrant responds within ten (10) business days, it's response will be reviewed by the DOT Tech, LLC's Abuse Team for further review. If DOT Tech, LLC's Abuse Team is satisfied by the Registrant's response that the use is not abusive, DOT Tech, LLC's Abuse Team will submit a request by the registry services provider to reactivate the domain name. DOT Tech, LLC's Abuse Team will then notify the Complainant that its complaint was ultimately denied and provide the reasons for the denial. If the Registrant does not respond within ten (10) business days, DOT Tech, LLC will notify the registry services team to cancel the abusive domain name.

This Anti-Abuse Procedure will not prejudice either party's election to pursue another dispute mechanism, such as URS or UDRP.

With the resources of DOT Tech, LLC's registry services personnel, DOT Tech, LLC 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 (1) 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 Application for rapid resolution of the request.

In the event such request involves any of the activities which can be validated by DOT Tech, LLC and involves the type of activity set forth in the Abuse Policy, the sponsoring Registrar is then given forty-eight (48) 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 48-hour period (i.e., is unresponsive to the request or refuses to take action), DOT Tech, LLC will place the domain on "serverHold".

Maintenance of Registration Criteria

1) All Registrants awarded a ".TECH" domain will agree to a one year minimum contract, which will need to be renewed on an annual basis. Renewal is the sole responsibility of the Registrant. Registrant's failing to renew their awarded domains by their expiration dates will be given a 60 day renewal grace period prior to their domain being revoked and returned to general availability.

2) DOT Tech, LLC is not liable or responsible in any way for any errors, omissions or any other actions by any third party (including any Registrar service) arising out of or related to a given Registrant's application for, registration of, renewal of, or failure to register or renew a particular domain name.

3) Through the registration process all Registrants will be expected to designate an administrative contact for their application, which would possess all the rights granted by DOT Tech, LLC or its designated agents to act in respect to the given domain including but not limited to managing the domain name or any services associated thereto. It is the Registrant's responsibility to update and maintain accurate contact information for their registrations.

Orphan Glue Removal

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 supports 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 the DNS. Therefore, when DOT Tech, LLC has written evidence of actual abuse of orphaned glue, DOT Tech, LLC will take action to remove those records from the zone to mitigate such malicious conduct.

DOT Tech, LLC's registry service operator will run a daily audit of entries in its DNS systems and compare 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 DOT Tech, LLC or its registry services operator becomes aware of actual abuse on orphaned glue after receiving written notification by a third party through its Abuse Contact or through its customer support, such glue records will be removed from the zone.

WhoIs Accuracy

DOT Tech, LLC will provide WhoIs accessibility in a reliable, consistent, and predictable fashion in order to promote Whois accuracy. The Registry will adhere to port 43 WhoIs Service Level Agreements (SLAs), which require that port 43 WHOIS service be highly accessible and fast.

DOT Tech, LLC will offer thick WhoIs services, in which all authoritative WhoIs data—including

contact data—is maintained at the registry. DOT Tech, LLC will maintain timely, unrestricted, and public access to accurate and complete WhoIs information, including all data objects as specified in Specification 4. Moreover, prior to the release of any domain names, DOT Tech, LLC's Registrar will provide DOT Tech, LLC with an authorization code to verify eligible Registrants provide accurate Registrant contact information.

In order to further promote WhoIs accuracy, DOT Tech, LLC will offer a mechanism whereby third parties can submit complaints directly to the DOT Tech, LLC (as opposed to ICANN or the sponsoring Registrar) about inaccurate or incomplete WhoIs data. Such information shall be forwarded to the Registrar, who shall be required to address those complaints with their Registrants. Thirty days after forwarding the complaint to the Registrar, DOT Tech, LLC 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, DOT Tech, LLC reserves the right to cancel or suspend the applicable domain name(s) should DOT Tech, LLC determine that the domains are being used in a manner contrary to DOT Tech, LLC's abuse policy.

DOT Tech, LLC shall also require authentication and verification of all Registrant data. DOT Tech, LLC shall verify the certificates of incorporation, whether a corporation is in active status, contact information, e-mail address, and, to the best of its abilities, determine whether address information supplied is accurate. Second-level domains in the TLD shall not be operational unless two (2) out of three (3) of the above authentication methods have been satisfied.

DOT Tech, LLC will also maintain historical databases of Registrants and associated information which have provided inaccurate WhoIs information. DOT Tech, LLC will endeavor to use this database to uncover patterns of suspicious registrations which DOT Tech, LLC shall then flag for further authentication or for review of the Registrant's use of the domain in question to ensure Registrant's use is consonant with DOT Tech, LLC's abuse policy.

In addition, DOT Tech, LLC's Abuse Team shall on its own initiative, no less than twice per year, perform a manual review of a random sampling of domain names within the applied-for TLD to test the accuracy of the WhoIs information. Although this will not include verifying the actual information in the WHOIS record, DOT Tech, LLC 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 Registrar, who shall be required to address those complaints with their Registrants. Thirty days after forwarding the complaint to the Registrar, the DOT Tech, LLC 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, DOT Tech, LLC reserves the right to suspend the applicable domain name(s) should DOT Tech, LLC determine that the Registrant is using the domain in question in a manner contrary to DOT Tech, LLC's abuse policy. DOT Tech, LLC shall also reserve the right to report such recalcitrant Registrar activities directly to ICANN.

Abuse Prevention and Mitigation Domain Name Access

All domain name Registrants will have adequate controls to ensure proper access to domain functions.

In addition to the above, all domain name Registrants in the applied-for TLD will be required to name at least two (2) unique points of contact who are authorized to request and/or approve update, transfer, and deletion requests. The points of contact must establish strong passwords with the Registrar that must be authenticated before a point of contact will be allowed to process updates, transfer, and deletion requests. Once a process update, transfer, or deletion request is entered, the points of contact will automatically be notified when a domain has been updated, transferred, or deleted through an automated system run by DOT Tech, LLC's Registrar. Authentication of modified Registrant information shall be accomplished within 72 hours of receipt.

29 Rights Protection Mechanisms Applicants must describe how their registry will comply with policies and practices that minimize abusive registrations and other activities that affect the legal rights of others, such as the Uniform Domain Name Dispute Resolution Policy (UDRP), Uniform Rapid Suspension (URS) system, and Trademark Claims and Sunrise services at startup. A complete answer should include

- A description of how the registry operator will implement safeguards against allowing unqualified registrations (e.g., registrations made in violation of the registry's eligibility restrictions or policies), and reduce opportunities for behaviors such as phishing or pharming. At a minimum, the registry operator must offer a Sunrise period and a Trademark Claims service during the required time periods, and implement decisions rendered under the URS on an ongoing basis; and
- A description of resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

To be eligible for a score of 2, answers must also include additional measures specific to rights protection, such as abusive use policies, takedown procedures, registrant pre-verification, or authentication procedures, or other covenants

A complete answer is expected to be no more than 10 pages.

DOT Tech, LLC is committed to implementing strong and integrated Rights Protection Mechanisms (RPM). Use of domain names that infringe upon the legal rights of others in the TLD will not be tolerated. The nature of such uses creates security and stability issues for the registry, Registrars, and Registrants, as well as for users of the Internet in general. DOT Tech, LLC will protect the legal rights of others by implementing RPMs and anti abuse policies backed by robust responsiveness to complaints and requirements of DOT Tech, LLC's Registrars.

Trademark Clearinghouse

Each new gTLD Registry will be required to implement support for, and interaction with, the Trademark Clearinghouse ("Clearinghouse"). The 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.

Utilizing the 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 Claims 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.

Sunrise A Period

DOT Tech, LLC will offer segmented Sunrise Periods. The initial Sunrise Period will last [minimum 30 days] for owners of trademarks listed in the Clearinghouse to register domain names that consist of an identical match of their listed trademarks. All domain names registered during the Sunrise Period will be subject to DOT Tech, LLC's domain name registration policies. DOT Tech, LLC will assign 3-5 employees to specifically work as the Rights Protection Team, these employees will receive and authenticate all Sunrise Registrations. The DOT Tech, LLC RPM team will specifically deal with trademark protection issues and mitigate or assist in resolving any rights protection issues which arise during the Sunrise processes.

DOT Tech, LLC's Registrar will ensure that all Sunrise Registrants meet sunrise eligibility requirements (SERs), which will be verified by Clearinghouse data. The proposed SERs include: (i) ownership of a mark that is (a) nationally or regionally registered and for which proof of use, such as a declaration and a single specimen of current use was submitted to, and validated by, the 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, (ii) optional registry elected requirements concerning international classes of goods or services covered by registration; (iii) representation that all provided information is true and correct; and (iv) provision of data sufficient to document rights in the trademark.

Upon receipt of the Sunrise application, DOT Tech, LLC will issue a unique tracking number to the Registrar, which will correspond to that particular application. All applications will receive tracking numbers regardless of whether they are complete. Applications received during the Sunrise period will be accepted on a first-come, first-serve basis. Upon submission of all of the required information and documentation, Registrar will forward the information to DOT Tech, LLC's RPM Team for authentication. DOT Tech, LLC's RPM Team will review the information and documentation, verify the trademark information, and notify the potential Registrant of any deficiencies. If a Registrant does not cure any trademark-related deficiencies and/or respond by the means listed within one (1) week, DOT Tech, LLC will notify its Registrar and the domain name will be released for registration.

DOT Tech, LLC 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 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, DOT Tech, LLC's RPM Team will review the Complaint to see if the Complaint reasonably asserts a legitimate challenge as defined by the SDRP. If not, DOT Tech, LLC's RPM Team will send an email to the Complainant within thirty-six (36) hours of sending the confirmation email that the subject of the complaint clearly does not fall within one of the delineated grounds as defined by the SDRP and that DOT Tech, LLC considers the matter closed.

If the domain name is not found to have adequately met the SERs, DOT Tech, LLC RPM Team will alert the Registrar and registry services provider to immediately suspend the resolution of the domain name. Thereafter, DOT Tech, LLC's RPM Team will immediately notify the Sunrise Registrant of the suspension of the domain name, the nature of the complaint, and provide the Registrant with the option to respond within ten (10) days to cure the SER deficiencies or the domain name will be canceled.

If the Registrant responds within ten (10) business days, its response will be reviewed by DOT Tech, LLC's RPM Team to determine if the SERs are met. If DOT Tech, LLC's RPM Team is satisfied by the Registrant's response, DOT Tech, LLC's RPM Team will submit a request to the Registrar and the registry services provider to un suspend the domain name. DOT Tech, LLC's RPM Team will then notify the Complainant that its complaint was ultimately denied and provide the reasons for the denial.

Names secured as described through the Sunrise AT/AD processes will result in the registration of resolving domain names at the registry. Names reserved through the Sunrise B process will not result in resolving domain name at DOT Tech, LLC. Rather, these names will be reserved and blocked from live use. The applied for string will resolve to an informational page informing visitors that the name is unavailable for registration and reserved from use.

Applications that fit the following criteria will be considered during the Sunrise A period: DOT Tech, LLC owns and operates an existing domain name in another gTLD or ccTLD, in connection with eligible commerce and satisfies the registration requirements described in Section 1.

Sunrise B

Applications that fit the following criteria will be considered during the Sunrise B period:

- a) Applicant holds valid trademark registrations or owns rights to a particular name and wishes to block the use of such name.
- b) The Applicant must seek to block a name that corresponds to the entire text of its trademark or the complete textual component of a graphical or compound trademark. Certain variances are permitted for trademarks containing spaces or special characters that are not available for domain names.

Founder's Program

Applications for the Founder's Program will be accepted after the close of the Sunrise Periods. Potential Registrants should understand that certain expectations, as described herein will

accompany the issuance of a domain name under the Founder's Program and all registrations resulting from this program will be required to follow the below listed guidelines, which will be further described in their Program Agreement:

- a) Registrants awarded a domain through the Founder's Program must use their best efforts to launch a ".TECH" website within 30 days of signing the Program Agreement.
 - b) In addition, each Registrant will be required to issue a press release announcing the launch of their ".TECH" Founder Website, concurrent with the launch of their ".TECH" Founder Website, said press release must be approved by DOT Tech, LLC;
 - c) Founders are expected to proactively market and promote ".TECH" gTLD in a manner that is likely to produce widespread awareness of the unique advantages gained through the ".TECH" string.
 - d) Founders will allow DOT Tech, LLC to use in good faith Founder's name, likeness, trademarks, logos, and Application contents (other than Confidential Information,) as well as other Founder information and content as may be mutually agreed, in DOT Tech, LLC's marketing, promotional and communications materials.
- DOT Tech, LLC will randomly verify compliance of the above listed expectations and have the right to revoke any Founder's site, should they be deemed non-compliant. Additionally, DOT Tech, LLC may suspend or delete a Founder's site without prior notice to the Registrar or Registrant if the Founder's site is deemed in violation of any of DOT Tech's registration guidelines or policies. Registrants participating in the Founders program will receive 25% discounted registration, renewal pricing and term extensions (not to exceed 5 years) from DOT Tech's Registrars as recognition for their participation in the Founders Program.

Landrush

Landrush is a limited time opportunity for companies that want to secure a high value ".TECH" name for a small fee (above the basic registration cost). The landrush period will last 30 days. Applications will be accepted and evaluated to determine if they meet the requirements for registration. At the end of the Landrush period domain names with only one application will be awarded directly to the Applicant. Domain names with two or more applications will proceed to a closed mini auction, between the respective Applicants, where the highest bidder wins.

General Availability Period

Applicant must meet all registration requirements.

Names will be awarded on a first come, first serve basis which is determined as of the time of the initial request, not when authentication occurs.

Domain Name Contentions

Name contentions will arise when both a Sunrise A and Sunrise B application are submitted for the same name, the following actions will be taken to resolve the contention.

- a) Both Applicants will be notified of the contention and the Sunrise A Applicant will be given first right to either register their requested domain or withdraw their application. A domain applied for under Sunrise A will, all else being equal, receive priority over the identical domain applied for under Sunrise B. Sunrise A names get priority over Sunrise B names.
- b) If the Sunrise Applicant chooses to register their name regardless of the contention, then the Sunrise B Applicant may choose to pursue further action independently of DOT Tech, LLC to contest the name. These processes may include UDRP or Civil Court and are not connected to DOT Tech's sunrise policies.
- c) If two Sunrise A Applicants apply for the same domain name (i.e., Delta Airlines and Delta Faucet both seek to be awarded the use of DELTA.TECH) then DOT Tech, LLC will notify both Applicants of the contention and proceed to an auction process as described in Section 9.
- d) If two Sunrise B Applicants apply for the same domain name (i.e., Delta Airlines and Delta Faucet, both seek to block the use of DELTA.UNO), then DOT Tech, LLC will accept both applications as valid and block the use of the indicated domain.

Appeal of Rejected Sunrise Applications

An Applicant can file a request for reconsideration within 10 days of the notification of DOT Tech, LLC's rejection. Reconsideration can be requested by completing a reconsideration form and filing a reconsideration fee with DOT Tech, LLC. Forms, fee information, and process documentation will be available on the DOT Tech, LLC website. Upon receipt of the reconsideration form and the corresponding fee, DOT Tech, LLC or its Agents will re examine the application, and notify the Registrant of all findings or additional information needed. The Request for Reconsideration must be submitted through the Registrant's Registrar, and a reconsideration fee must be paid to DOT Tech, LLC.

Auctions

Sunrise A names found to be in contention as described above will result in Auction. DOT Tech, LLC plans to have a qualified third party conduct our auction processes, therefore the rules contained in this document are subject to change based on the selection of an auctioneer:

- a) All auction participants are expected to keep their account information current, throughout the auction process.
- b) Auction participants will receive up to date communication from the auctioneer as the

auction progresses, bidding status changes, or issues arise.

Bidding

- a) Auctions will follow a standard process flow: scheduled (upcoming), open and closed.
- b) You will receive an "Auction Scheduled" notice at least ten (10) days prior to the scheduled auction start date. You will receive an "Auction Start" notice on the auction start date, which will indicate that you may begin placing bids through the interface. Once closed, the auction is complete and if you are the winning bidder, you will proceed to the payment process.
- c) If you choose to bid for a particular domain and you are the highest bidder at the end of an auction, you are obligated to complete the transaction and pay the Auctioneer the amount of your winning bid. Carefully consider your bids prior to placing them - bids are not retractable under any circumstances.
- d) If no bids are placed on a particular domain, the Registry will register the domain on behalf of the first customer (in the respective phase) to submit an application through a Registrar.

Extensions

- a) A normal auction period is anticipated to last a minimum of 7 (seven) days. However, in the event of significant auction activity, an auction close may extend during the last twenty-four (24) hours of scheduled operation to better need the volume of the auction.
- b) Auction extensions are meant to provide a mechanism that is fair for bidders in all time zones to respond to being outbid.
- c) An auction extension will occur whenever the auction lead changes in the last twenty-four (24) hours of the schedule of an auction. The close will be revised to reflect a new closing time set at twenty-four (24) hours after the change in auction lead occurred. Essentially, this means that a winning maximum bid has to remain unchallenged for a period of twenty-four (24) hours before the auction will close.
- d) It is important to note that extensions are not simply based on the auction value changing since this could occur as a result of proxy bidding where the same bidder retains their lead. In this case, the maximum bid has not changed, the leader has not changed and therefore no extension will occur.

Payment Default

In the event that you as the winning bidder decide not to honor your payment obligations (or in the event of a reversal of payment or a charge back by a credit card company or other payment provider) on any outstanding balance, the Registry has the right to cancel any/all of your winning registrations for any .INC domain name, regardless of whether they have been paid for or not. You do not have the right to "pick and choose" the names you wish to keep or not keep. Winning an auction creates an obligation to remit payment. Failure to remit payment is a breach of your agreement.. You will lose any previously won domains and will no longer be allowed to bid on any current or future auctions sponsored by DOT Tech, LLC. Participants are encouraged therefore to consider carefully each bid submitted as any bid could be a winning bid.

Trademark Claims Service

DOT Tech, LLC will offer a Trademark Claims Service to provide maximum protection and value to rights holders. The Trademark Claims Service will be monitored and operated by DOT Tech, LLC's RPM Team that will receive all communications regarding the Trademark Claims Service and catalog them. DOT Tech, LLC's Registrar will review all domain name requests to determine if they are an identical match of a trademark filed with the Trademark Clearinghouse. 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 spaces, hyphens or underscores. Domain names that are plural forms of a mark, or that merely contain a mark, will not qualify as an identical match.

If the Registrar determines that a prospective domain name registration is identical to a mark registered in the Trademark Clearinghouse, the Registrar will be required to email a "Trademark Claims Notice" (Notice) in English to the protective Registrant of the domain name and copy DOT Tech, LLC's RPM Team. The Notice will provide the prospective Registrant information regarding the trademark referenced in the Trademark Claims Notice to enhance understanding of the Trademark rights being claimed by the trademark holder. The Notice will be provided in real time without cost to the prospective Registrant.

After receiving the notice, the Registrar will provide the prospective Registrant five (5) days to reply to the Trademark Claims Service with a signed document that specifically warrants that: (i) the prospective Registrant has received notification that the mark 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. If the warranty document satisfies these requirements, the Registrar will effectuate the registration and notify DOT Tech, LLC's RPM Team.

After the effectuation of a registration that is identical to a mark listed in the Trademark Clearinghouse, the Registrar will provide clear notice to the trademark owner consisting of the domain name that has been registered and copy DOT Tech, LLC's RPM Team. The trademark owner then has the option of filing a Complaint under the Uniform Domain Name Dispute Resolution Policy (UDRP) or the Uniform Rapid Suspension System (URS).

Uniform Rapid Suspension System (URS)

DOT Tech, LLC will specify in the Registry Agreement, all RRAs, and all Registration Agreements used in connection with the TLD that it and its Registrars will abide by all decisions made by panels in accordance with the Uniform Rapid Suspension System (URS). DOT Tech, LLC's RPM Team will receive all URS Complaints and decisions, and will notify its Registrar to suspend all registrations determined by a URS panel to be infringing within a commercially reasonable time of receiving the decision. DOT Tech, LLC's RPM Team will catalog all abuse communications, but only provide them 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.

Uniform Domain Name Dispute Resolution Policy (UDRP)

DOT Tech, LLC will specify in the Registry Agreement, all Registry-Registrar Agreements, and Registration Agreements used in connection with the TLD that it will promptly abide by all decisions made by panels in accordance with the Uniform Domain Name Dispute Resolution Policy (UDRP). DOT Tech, LLC's RPM Team will receive all UDRP Complaints and decisions, and will notify its Registrar to cancel or transfer all registrations determined to be infringing within ten (10) business days of receiving the decision. DOT Tech, LLC's RPM Team will catalog all abuse communications, but only provide them 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.

Proven Registrars

In order to reduce abusive registrations and other activities that affect the legal rights of others, DOT Tech, LLC will only contract with ICANN-accredited Registrars. The Registrar, according to the RRA, will not be able to register any domain names, thus eliminating the possibility of front-running.

Pre-Authorization and Authentication

Registrant authentication shall occur in accordance with the registration eligibility criteria and the Anti-Abuse Policy for ".TECH" as set forth in Question 28.

The verification process is designed to prevent a prospective Registrant from providing inaccurate or incomplete data, such that, if necessary, the Registrant can be readily contacted regarding an infringing use of its site; indeed, the process (including verification of a Registrant's certificate of incorporation) is designed to ensure that only qualified members of the community are permitted to register in the TLD.

Thick WhoIs

DOT Tech, LLC 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.

Takedown Procedure

DOT Tech, LLC will provide a Takedown Procedure modeled after the Digital Millennium Copyright Act's notice-and-takedown procedure.

At all times, DOT Tech, LLC will publish on its home website at NIC.TECH contact information for receiving rights protection complaints (Complaint) from rights holders, including but not limited to trademark and copyright Complaints. Complaints will be addressed to and received by DOT Tech, LLC's RPM Team who will catalogue and ticket in DOT Tech, LLC's CRM software and review as outlined herein. DOT Tech, LLC will catalog all rights protection communications and only provide them 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.

Any Complaint from a rights holder will be relayed to DOT Tech, LLC's RPM Team. A member of DOT Tech, LLC's RPM Team will then send an email to the Complainant within forty-eight (48) hours of receiving the Complaint confirming receipt of the email, and that DOT Tech, LLC will notify the Complainant of the results of the Complaint within (10) days of receiving the Complaint.

After sending the confirmation email, DOT Tech, LLC's RPM Team will review the Complaint. If DOT Tech, LLC or its Registrar determines that the registration was in bad faith, DOT Tech, LLC or its Registrar may cancel or suspend the resolution of the domain name. Bad faith registration includes, but is not limited to, the registration of a domain identical to a registered trademark where the Registrant has proceeded with registration after receipt of a Clearinghouse notice, as described above.

If the Registrant responds within ten (10) business days, its response will be reviewed by the DOT Tech, LLC's RPM Team. If DOT Tech, LLC's RPM Team is satisfied by the Registrant's response that the content has been taken down or is not infringing, DOT Tech, LLC's RPM Team will un-suspend the domain name. DOT Tech, LLC's RPM Team will then notify the Complainant that its complaint was ultimately denied and provide the reasons for the denial. If the Registrant does not respond within ten (10) business days, DOT Tech, LLC or its Registrar may cancel or suspend the resolution of the domain name.

This Takedown Procedure will not prejudice any party's election to pursue another dispute mechanism, such as URS or UDRP, as set forth in DOT Tech, LLC's response to Question 28.

30A. Security Policy: provide a summary of the security policy for the proposed registry, including but not limited to:

- indication of any independent assessment reports demonstrating security capabilities, and provisions for periodic independent assessment reports to test security capabilities;
- description of any augmented security levels or capabilities commensurate with the nature of the applied for gTLD string, including the identification of any existing international or industry relevant security standards the applicant commits to following (reference site must be provided);
- list of commitments made to registrants concerning security levels.

To be eligible for a score of 2, answers must also include:

- Evidence of an independent assessment report demonstrating effective security controls (e.g., ISO 27001).

A summary of the above should be no more than 20 pages. Note that the complete security policy for the registry is required to be submitted in accordance with 30(b).

30.(a).1 Security Policies

DOT Tech and our back-end operator, Neustar recognize the vital need to secure the systems and the integrity of the data in commercial solutions. The ".TECH" 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 ".TECH" 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 ".TECH"
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 ".TECH" 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 ".TECH". 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 ".TECH" 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.*

EXHIBIT F

Radix Wins Rights to .TECH, Defeating Google and Other Global Players

NEWS PROVIDED BY

Radix →

07 Nov, 2014, 13:21 GMT

MUMBAI, November 7, 2014 /PRNewswire/

Technology Companies Including Startups can Soon Get yourbrand.tech Website Addresses

Radix, founded by Indian serial entrepreneur Bhavin Turakhia, with over \$30 million in committed funding, has won the global perpetual rights to run the .TECH Top Level Domain (TLD) extension in an auction held by ICANN. Radix made the winning bid of \$6.7 million for rights to .TECH, competing with Google, Donuts, and other industry players. With this victory, Radix now owns the rights to operate .TECH along with 4 other extensions it owns rights to viz. .website, .space, .press and .host.

*"We are delighted to add .TECH to our TLD portfolio. This new extension will represent the ever growing community of users who truly understand the power of the Internet, and appreciate the value of a powerful identity online. As a techie at heart, this is an extension that I can personally relate and connect with the most," says **Bhavin Turakhia, CEO, Radix.***

A Top Level Domain extension is simply the part of the website address that follows the dot, for e g yourwebsite.tech .TECH is a part of the launch of new domain extensions by ICANN (an agency which manages the global supply of Internet addresses) to address depleting pool of names in domain extensions like com, net org and in Consumers found that old extensions

like .com have run out of short, meaningful domain names. This called for new domain extensions like .web, .law, .press and .shop, .music etc., which aim to be contextual to the purposes that websites fulfil while also providing a fresh pool of domain names.

Radix will soon launch TECH enabling tech companies worldwide to get premium desired domain names ending in the TECH extension. Once launched, technology oriented companies, communities and individuals will have the ability to register shorter and more memorable website addresses ending with TECH.

An industry specific domain name like .TECH is an important tool in this direction and is especially significant for India due to the importance of the technology sector in the country. Employing over 3.1 million software engineers, the 15000 firms in IT sector form the largest private sector employer in the country. Statistics by Evans Data Corp., say that by 2017, India will overtake USA in the number of software developers and by 2018, India is projected to have 20% of the global software developer population.

"India has an exciting budding startup culture," added Bhavin. "With the proliferation of successful startups in India and support from the government like the 'Make in India' campaign, these initiatives are going to grow further. A .TECH domain name can help establish strong brand credibility for these startups which often aim at an international market." According to NASSCOM, there are already over 16,000 startups in the country.

Slated for a Q1 2015 launch, .TECH domain names will be made available through all major domain name retailers world-wide. Radix has successfully launched three of its extensions - .website, .press and .host - and is in the process of launching .space.

About Radix

Radix is an active participant in ICANN's process to expand the Internet naming system and introduce new, meaningful Internet addresses. Radix is Asia's largest new gTLD applicant under this program with applications to operate 20 suffixes including .web, .music, .blog, and .shop. The company has invested over \$30 million so far with additional funding lined up, in securing licenses to operate these new extensions and expects to play a large role in the global diversification of the internet namespace.

Learn more about Radix at <http://www.radixregistry.com>

Media Contact: Prateek Pant, prateek.pant@text100.co.in +91-9920-025-254, Text100

SOURCE Radix

EXHIBIT G

REGISTRY AGREEMENT

This REGISTRY AGREEMENT (this “Agreement”) is entered into as of _____ (the “Effective Date”) between Internet Corporation for Assigned Names and Numbers, a California nonprofit public benefit corporation (“ICANN”), and Dot Tech LLC, a Kansas limited liability company (“Registry Operator”).

ARTICLE 1.

DELEGATION AND OPERATION OF TOP-LEVEL DOMAIN; REPRESENTATIONS AND WARRANTIES

1.1 Domain and Designation. The Top-Level Domain to which this Agreement applies is **.tech** (the “TLD”). Upon the Effective Date and until the earlier of the expiration of the Term (as defined in Section 4.1) or the termination of this Agreement pursuant to Article 4, ICANN designates Registry Operator as the registry operator for the TLD, subject to the requirements and necessary approvals for delegation of the TLD and entry into the root-zone.

1.2 Technical Feasibility of String. While ICANN has encouraged and will continue to encourage universal acceptance of all top-level domain strings across the Internet, certain top-level domain strings may encounter difficulty in acceptance by ISPs and webhosters and/or validation by web applications. Registry Operator shall be responsible for ensuring to its satisfaction the technical feasibility of the TLD string prior to entering into this Agreement.

1.3 Representations and Warranties.

(a) Registry Operator represents and warrants to ICANN as follows:

(i) all material information provided and statements made in the registry TLD application, and statements made in writing during the negotiation of this Agreement, were true and correct in all material respects at the time made, and such information or statements continue to be true and correct in all material respects as of the Effective Date except as otherwise previously disclosed in writing by Registry Operator to ICANN;

(ii) Registry Operator is duly organized, validly existing and in good standing under the laws of the jurisdiction set forth in the preamble hereto, and Registry Operator has all requisite power and authority and has obtained all necessary approvals to enter into and duly execute and deliver this Agreement; and

(iii) Registry Operator has delivered to ICANN a duly executed instrument that secures the funds required to perform registry functions for the TLD in the event of the termination or expiration of this Agreement (the “Continued Operations Instrument”), and such instrument is a binding

obligation of the parties thereto, enforceable against the parties thereto in accordance with its terms.

(b) ICANN represents and warrants to Registry Operator that ICANN is a nonprofit public benefit corporation duly organized, validly existing and in good standing under the laws of the State of California, United States of America. ICANN has all requisite power and authority and has obtained all necessary corporate approvals to enter into and duly execute and deliver this Agreement.

ARTICLE 2.

COVENANTS OF REGISTRY OPERATOR

Registry Operator covenants and agrees with ICANN as follows:

2.1 Approved Services; Additional Services. Registry Operator shall be entitled to provide the Registry Services described in clauses (a) and (b) of the first paragraph of Section 2.1 in the Specification 6 attached hereto ("Specification 6") and such other Registry Services set forth on Exhibit A (collectively, the "Approved Services"). If Registry Operator desires to provide any Registry Service that is not an Approved Service or is a material modification to an Approved Service (each, an "Additional Service"), Registry Operator shall submit a request for approval of such Additional Service pursuant to the Registry Services Evaluation Policy at <http://www.icann.org/en/registries/rsep/rsep.html>, as such policy may be amended from time to time in accordance with the bylaws of ICANN (as amended from time to time, the "ICANN Bylaws") applicable to Consensus Policies (the "RSEP"). Registry Operator may offer Additional Services only with the written approval of ICANN, and, upon any such approval, such Additional Services shall be deemed Registry Services under this Agreement. In its reasonable discretion, ICANN may require an amendment to this Agreement reflecting the provision of any Additional Service which is approved pursuant to the RSEP, which amendment shall be in a form reasonably acceptable to the parties.

2.2 Compliance with Consensus Policies and Temporary Policies. Registry Operator shall comply with and implement all Consensus Policies and Temporary Policies found at <http://www.icann.org/general/consensus-policies.htm>, as of the Effective Date and as may in the future be developed and adopted in accordance with the ICANN Bylaws, provided such future Consensus Policies and Temporary Policies are adopted in accordance with the procedure and relate to those topics and subject to those limitations set forth in Specification 1 attached hereto ("Specification 1").

2.3 Data Escrow. Registry Operator shall comply with the registry data escrow procedures set forth in Specification 2 attached hereto ("Specification 2").

2.4 Monthly Reporting. Within twenty (20) calendar days following the end of each calendar month, Registry Operator shall deliver to ICANN reports in the format set forth in Specification 3 attached hereto ("Specification 3").

2.5 Publication of Registration Data. Registry Operator shall provide public access to registration data in accordance with Specification 4 attached hereto (“Specification 4”).

2.6 Reserved Names. Except to the extent that ICANN otherwise expressly authorizes in writing, Registry Operator shall comply with the requirements set forth in Specification 5 attached hereto (“Specification 5”). Registry Operator may at any time establish or modify policies concerning Registry Operator’s ability to reserve (i.e., withhold from registration or allocate to Registry Operator, but not register to third parties, delegate, use, activate in the DNS or otherwise make available) or block additional character strings within the TLD at its discretion. Except as specified in Specification 5, if Registry Operator is the registrant for any domain names in the registry TLD, such registrations must be through an ICANN accredited registrar, and will be considered Transactions (as defined in Section 6.1) for purposes of calculating the Registry-level transaction fee to be paid to ICANN by Registry Operator pursuant to Section 6.1.

2.7 Registry Interoperability and Continuity. Registry Operator shall comply with the Registry Interoperability and Continuity Specifications as set forth in Specification 6 attached hereto (“Specification 6”).

2.8 Protection of Legal Rights of Third Parties. Registry Operator must specify, and comply with, the processes and procedures for launch of the TLD and initial registration-related and ongoing protection of the legal rights of third parties as set forth Specification 7 attached hereto (“Specification 7”). Registry Operator may, at its election, implement additional protections of the legal rights of third parties. Any changes or modifications to the process and procedures required by Specification 7 following the Effective Date must be approved in advance by ICANN in writing. Registry Operator must comply with all remedies imposed by ICANN pursuant to Section 2 of Specification 7, subject to Registry Operator’s right to challenge such remedies as set forth in the applicable procedure described therein. Registry Operator shall take reasonable steps to investigate and respond to any reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD. In responding to such reports, Registry Operator will not be required to take any action in contravention of applicable law.

2.9 Registrars.

(a) All domain name registrations in the TLD must be registered through an ICANN accredited registrar; provided, that Registry Operator need not use a registrar if it registers names in its own name in order to withhold such names from delegation or use in accordance with Section 2.6. Subject to the requirements of Specification 11, Registry Operator must provide non-discriminatory access to Registry Services to all ICANN accredited registrars that enter into and are in compliance with the registry-registrar agreement for the TLD; provided that Registry Operator may establish non-discriminatory criteria for qualification to register names in the TLD that are reasonably related to the proper functioning of the TLD. Registry Operator must use a uniform non-discriminatory

agreement with all registrars authorized to register names in the TLD (the “Registry-Registrar Agreement”). Registry Operator may amend the Registry-Registrar Agreement from time to time; provided, however, that any material revisions thereto must be approved by ICANN before any such revisions become effective and binding on any registrar. Registry Operator will provide ICANN and all registrars authorized to register names in the TLD at least fifteen (15) calendar days written notice of any revisions to the Registry-Registrar Agreement before any such revisions become effective and binding on any registrar. During such period, ICANN will determine whether such proposed revisions are immaterial, potentially material or material in nature. If ICANN has not provided Registry Operator with notice of its determination within such fifteen (15) calendar-day period, ICANN shall be deemed to have determined that such proposed revisions are immaterial in nature. If ICANN determines, or is deemed to have determined under this Section 2.9(a), that such revisions are immaterial, then Registry Operator may adopt and implement such revisions. If ICANN determines such revisions are either material or potentially material, ICANN will thereafter follow its procedure regarding review and approval of changes to Registry-Registrar Agreements at <http://www.icann.org/en/resources/registries/rra-amendment-procedure>, and such revisions may not be adopted and implemented until approved by ICANN.

(b) If Registry Operator (i) becomes an Affiliate or reseller of an ICANN accredited registrar, or (ii) subcontracts the provision of any Registry Services to an ICANN accredited registrar, registrar reseller or any of their respective Affiliates, then, in either such case of (i) or (ii) above, Registry Operator will give ICANN prompt notice of the contract, transaction or other arrangement that resulted in such affiliation, reseller relationship or subcontract, as applicable, including, if requested by ICANN, copies of any contract relating thereto; provided, that ICANN will treat such contract or related documents that are appropriately marked as confidential (as required by Section 7.15) as Confidential Information of Registry Operator in accordance with Section 7.15 (except that ICANN may disclose such contract and related documents to relevant competition authorities). ICANN reserves the right, but not the obligation, to refer any such contract, related documents, transaction or other arrangement to relevant competition authorities in the event that ICANN determines that such contract, related documents, transaction or other arrangement might raise significant competition issues under applicable law. If feasible and appropriate under the circumstances, ICANN will give Registry Operator advance notice prior to making any such referral to a competition authority.

(c) For the purposes of this Agreement: (i) “Affiliate” means a person or entity that, directly or indirectly, through one or more intermediaries, or in combination with one or more other persons or entities, controls, is controlled by, or is under common control with, the person or entity specified, and (ii) “control” (including the terms “controlled by” and “under common control with”) means the possession, directly or indirectly, of the power to direct or cause the direction of the management or policies of a person or entity, whether through the ownership of securities, as trustee or executor, by serving as an employee or a member of a board of directors or equivalent governing body, by contract, by credit arrangement or otherwise.

2.10 Pricing for Registry Services.

(a) With respect to initial domain name registrations, Registry Operator shall provide ICANN and each ICANN accredited registrar that has executed the registry-registrar agreement for the TLD advance written notice of any price increase (including as a result of the elimination of any refunds, rebates, discounts, product tying or other programs which had the effect of reducing the price charged to registrars, unless such refunds, rebates, discounts, product tying or other programs are of a limited duration that is clearly and conspicuously disclosed to the registrar when offered) of no less than thirty (30) calendar days. Registry Operator shall offer registrars the option to obtain initial domain name registrations for periods of one (1) to ten (10) years at the discretion of the registrar, but no greater than ten (10) years.

(b) With respect to renewal of domain name registrations, Registry Operator shall provide ICANN and each ICANN accredited registrar that has executed the registry-registrar agreement for the TLD advance written notice of any price increase (including as a result of the elimination of any refunds, rebates, discounts, product tying, Qualified Marketing Programs or other programs which had the effect of reducing the price charged to registrars) of no less than one hundred eighty (180) calendar days. Notwithstanding the foregoing sentence, with respect to renewal of domain name registrations: (i) Registry Operator need only provide thirty (30) calendar days notice of any price increase if the resulting price is less than or equal to (A) for the period beginning on the Effective Date and ending twelve (12) months following the Effective Date, the initial price charged for registrations in the TLD, or (B) for subsequent periods, a price for which Registry Operator provided a notice pursuant to the first sentence of this Section 2.10(b) within the twelve (12) month period preceding the effective date of the proposed price increase; and (ii) Registry Operator need not provide notice of any price increase for the imposition of the Variable Registry-Level Fee set forth in Section 6.3. Registry Operator shall offer registrars the option to obtain domain name registration renewals at the current price (i.e., the price in place prior to any noticed increase) for periods of one (1) to ten (10) years at the discretion of the registrar, but no greater than ten (10) years.

(c) In addition, Registry Operator must have uniform pricing for renewals of domain name registrations ("Renewal Pricing"). For the purposes of determining Renewal Pricing, the price for each domain registration renewal must be identical to the price of all other domain name registration renewals in place at the time of such renewal, and such price must take into account universal application of any refunds, rebates, discounts, product tying or other programs in place at the time of renewal. The foregoing requirements of this Section 2.10(c) shall not apply for (i) purposes of determining Renewal Pricing if the registrar has provided Registry Operator with documentation that demonstrates that the applicable registrant expressly agreed in its registration agreement with registrar to higher Renewal Pricing at the time of the initial registration of the domain name following clear and conspicuous disclosure of such Renewal Pricing to such registrant, and (ii) discounted Renewal Pricing pursuant to a Qualified Marketing Program (as defined below). The parties acknowledge that the purpose of this Section 2.10(c) is to prohibit abusive and/or discriminatory Renewal Pricing practices imposed by Registry

Operator without the written consent of the applicable registrant at the time of the initial registration of the domain and this Section 2.10(c) will be interpreted broadly to prohibit such practices. For purposes of this Section 2.10(c), a “Qualified Marketing Program” is a marketing program pursuant to which Registry Operator offers discounted Renewal Pricing, provided that each of the following criteria is satisfied: (i) the program and related discounts are offered for a period of time not to exceed one hundred eighty (180) calendar days (with consecutive substantially similar programs aggregated for purposes of determining the number of calendar days of the program), (ii) all ICANN accredited registrars are provided the same opportunity to qualify for such discounted Renewal Pricing; and (iii) the intent or effect of the program is not to exclude any particular class(es) of registrations (e.g., registrations held by large corporations) or increase the renewal price of any particular class(es) of registrations. Nothing in this Section 2.10(c) shall limit Registry Operator’s obligations pursuant to Section 2.10(b).

(d) Registry Operator shall provide public query-based DNS lookup service for the TLD (that is, operate the Registry TLD zone servers) at its sole expense.

2.11 Contractual and Operational Compliance Audits.

(a) ICANN may from time to time (not to exceed twice per calendar year) conduct, or engage a third party to conduct, contractual compliance audits to assess compliance by Registry Operator with its representations and warranties contained in Article 1 of this Agreement and its covenants contained in Article 2 of this Agreement. Such audits shall be tailored to achieve the purpose of assessing compliance, and ICANN will (a) give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested by ICANN, and (b) use commercially reasonable efforts to conduct such audit during regular business hours and in such a manner as to not unreasonably disrupt the operations of Registry Operator. As part of such audit and upon request by ICANN, Registry Operator shall timely provide all responsive documents, data and any other information reasonably necessary to demonstrate Registry Operator’s compliance with this Agreement. Upon no less than ten (10) calendar days notice (unless otherwise agreed to by Registry Operator), ICANN may, as part of any contractual compliance audit, conduct site visits during regular business hours to assess compliance by Registry Operator with its representations and warranties contained in Article 1 of this Agreement and its covenants contained in Article 2 of this Agreement. ICANN will treat any information obtained in connection with such audits that is appropriately marked as confidential (as required by Section 7.15) as Confidential Information of Registry Operator in accordance with Section 7.15.

(b) Any audit conducted pursuant to Section 2.11(a) will be at ICANN’s expense, unless (i) Registry Operator (A) controls, is controlled by, is under common control or is otherwise Affiliated with, any ICANN accredited registrar or registrar reseller or any of their respective Affiliates, or (B) has subcontracted the provision of Registry Services to an ICANN accredited registrar or registrar reseller or any of their respective Affiliates, and, in either case of (A) or (B) above, the audit relates to Registry Operator’s compliance with Section 2.14, in which case Registry Operator shall reimburse ICANN for

all reasonable costs and expenses associated with the portion of the audit related to Registry Operator's compliance with Section 2.14, or (ii) the audit is related to a discrepancy in the fees paid by Registry Operator hereunder in excess of 5% in a given quarter to ICANN's detriment, in which case Registry Operator shall reimburse ICANN for all reasonable costs and expenses associated with the entirety of such audit. In either such case of (i) or (ii) above, such reimbursement will be paid together with the next Registry-Level Fee payment due following the date of transmittal of the cost statement for such audit.

(c) Notwithstanding Section 2.11(a), if Registry Operator is found not to be in compliance with its representations and warranties contained in Article 1 of this Agreement or its covenants contained in Article 2 of this Agreement in two consecutive audits conducted pursuant to this Section 2.11, ICANN may increase the number of such audits to one per calendar quarter.

(d) Registry Operator will give ICANN immediate notice of Registry Operator's knowledge of the commencement of any of the proceedings referenced in Section 4.3(d) or the occurrence of any of the matters specified in Section 4.3(f).

2.12 Continued Operations Instrument. Registry Operator shall comply with the terms and conditions relating to the Continued Operations Instrument set forth in Specification 8 attached hereto ("Specification 8").

2.13 Emergency Transition. Registry Operator agrees that, in the event that any of the emergency thresholds for registry functions set forth in Section 6 of Specification 10 is reached, ICANN may designate an emergency interim registry operator of the registry for the TLD (an "Emergency Operator") in accordance with ICANN's registry transition process (available at <<http://www.icann.org/en/resources/registries/transition-processes>>) (as the same may be amended from time to time, the "Registry Transition Process") until such time as Registry Operator has demonstrated to ICANN's reasonable satisfaction that it can resume operation of the registry for the TLD without the reoccurrence of such failure. Following such demonstration, Registry Operator may transition back into operation of the registry for the TLD pursuant to the procedures set out in the Registry Transition Process, provided that Registry Operator pays all reasonable costs incurred (i) by ICANN as a result of the designation of the Emergency Operator and (ii) by the Emergency Operator in connection with the operation of the registry for the TLD, which costs shall be documented in reasonable detail in records that shall be made available to Registry Operator. In the event ICANN designates an Emergency Operator pursuant to this Section 2.13 and the Registry Transition Process, Registry Operator shall provide ICANN or any such Emergency Operator with all data (including the data escrowed in accordance with Section 2.3) regarding operations of the registry for the TLD necessary to maintain operations and registry functions that may be reasonably requested by ICANN or such Emergency Operator. Registry Operator agrees that ICANN may make any changes it deems necessary to the IANA database for DNS and WHOIS records with respect to the TLD in the event that an Emergency Operator is designated pursuant to this Section 2.13. In addition, in the

event of such failure, ICANN shall retain and may enforce its rights under the Continued Operations Instrument.

2.14 Registry Code of Conduct. In connection with the operation of the registry for the TLD, Registry Operator shall comply with the Registry Code of Conduct as set forth in Specification 9 attached hereto (“Specification 9”).

2.15 Cooperation with Economic Studies. If ICANN initiates or commissions an economic study on the impact or functioning of new generic top-level domains on the Internet, the DNS or related matters, Registry Operator shall reasonably cooperate with such study, including by delivering to ICANN or its designee conducting such study all data related to the operation of the TLD reasonably necessary for the purposes of such study requested by ICANN or its designee, provided, that Registry Operator may withhold (a) any internal analyses or evaluations prepared by Registry Operator with respect to such data and (b) any data to the extent that the delivery of such data would be in violation of applicable law. Any data delivered to ICANN or its designee pursuant to this Section 2.15 that is appropriately marked as confidential (as required by Section 7.15) shall be treated as Confidential Information of Registry Operator in accordance with Section 7.15, provided that, if ICANN aggregates and makes anonymous such data, ICANN or its designee may disclose such data to any third party. Following completion of an economic study for which Registry Operator has provided data, ICANN will destroy all data provided by Registry Operator that has not been aggregated and made anonymous.

2.16 Registry Performance Specifications. Registry Performance Specifications for operation of the TLD will be as set forth in Specification 10 attached hereto (“Specification 10”). Registry Operator shall comply with such Performance Specifications and, for a period of at least one (1) year, shall keep technical and operational records sufficient to evidence compliance with such specifications for each calendar year during the Term.

2.17 Additional Public Interest Commitments. Registry Operator shall comply with the public interest commitments set forth in Specification 11 attached hereto (“Specification 11”).

2.18 Personal Data. Registry Operator shall (i) notify each ICANN-accredited registrar that is a party to the registry-registrar agreement for the TLD of the purposes for which data about any identified or identifiable natural person (“Personal Data”) submitted to Registry Operator by such registrar is collected and used under this Agreement or otherwise and the intended recipients (or categories of recipients) of such Personal Data, and (ii) require such registrar to obtain the consent of each registrant in the TLD for such collection and use of Personal Data. Registry Operator shall take reasonable steps to protect Personal Data collected from such registrar from loss, misuse, unauthorized disclosure, alteration or destruction. Registry Operator shall not use or authorize the use of Personal Data in a way that is incompatible with the notice provided to registrars.

ARTICLE 3.

COVENANTS OF ICANN

ICANN covenants and agrees with Registry Operator as follows:

3.1 Open and Transparent. Consistent with ICANN's expressed mission and core values, ICANN shall operate in an open and transparent manner.

3.2 Equitable Treatment. ICANN shall not apply standards, policies, procedures or practices arbitrarily, unjustifiably, or inequitably and shall not single out Registry Operator for disparate treatment unless justified by substantial and reasonable cause.

3.3 TLD Nameservers. ICANN will use commercially reasonable efforts to ensure that any changes to the TLD nameserver designations submitted to ICANN by Registry Operator (in a format and with required technical elements specified by ICANN at <http://www.iana.org/domains/root/> will be implemented by ICANN within seven (7) calendar days or as promptly as feasible following technical verifications.

3.4 Root-zone Information Publication. ICANN's publication of root-zone contact information for the TLD will include Registry Operator and its administrative and technical contacts. Any request to modify the contact information for the Registry Operator must be made in the format specified from time to time by ICANN at <http://www.iana.org/domains/root/>.

3.5 Authoritative Root Database. To the extent that ICANN is authorized to set policy with regard to an authoritative root server system (the "Authoritative Root Server System"), ICANN shall use commercially reasonable efforts to (a) ensure that the authoritative root will point to the top-level domain nameservers designated by Registry Operator for the TLD, (b) maintain a stable, secure, and authoritative publicly available database of relevant information about the TLD, in accordance with ICANN publicly available policies and procedures, and (c) coordinate the Authoritative Root Server System so that it is operated and maintained in a stable and secure manner; provided, that ICANN shall not be in breach of this Agreement and ICANN shall have no liability in the event that any third party (including any governmental entity or internet service provider) blocks or restricts access to the TLD in any jurisdiction.

ARTICLE 4.

TERM AND TERMINATION

4.1 Term. The term of this Agreement will be ten (10) years from the Effective Date (as such term may be extended pursuant to Section 4.2, the "Term").

4.2 Renewal.

(a) This Agreement will be renewed for successive periods of ten (10) years upon the expiration of the initial Term set forth in Section 4.1 and each successive Term, unless:

(i) Following notice by ICANN to Registry Operator of a fundamental and material breach of Registry Operator's covenants set forth in Article 2 or breach of its payment obligations under Article 6 of this Agreement, which notice shall include with specificity the details of the alleged breach, and such breach has not been cured within thirty (30) calendar days of such notice, (A) an arbitrator or court of competent jurisdiction has finally determined that Registry Operator has been in fundamental and material breach of such covenant(s) or in breach of its payment obligations, and (B) Registry Operator has failed to comply with such determination and cure such breach within ten (10) calendar days or such other time period as may be determined by the arbitrator or court of competent jurisdiction; or

(ii) During the then current Term, Registry Operator shall have been found by an arbitrator (pursuant to Section 5.2 of this Agreement) or a court of competent jurisdiction on at least three (3) separate occasions to have been in (A) fundamental and material breach (whether or not cured) of Registry Operator's covenants set forth in Article 2 or (B) breach of its payment obligations under Article 6 of this Agreement.

(b) Upon the occurrence of the events set forth in Section 4.2(a) (i) or (ii), the Agreement shall terminate at the expiration of the then-current Term.

4.3 Termination by ICANN.

(a) ICANN may, upon notice to Registry Operator, terminate this Agreement if: (i) Registry Operator fails to cure (A) any fundamental and material breach of Registry Operator's representations and warranties set forth in Article 1 or covenants set forth in Article 2, or (B) any breach of Registry Operator's payment obligations set forth in Article 6 of this Agreement, each within thirty (30) calendar days after ICANN gives Registry Operator notice of such breach, which notice will include with specificity the details of the alleged breach, (ii) an arbitrator or court of competent jurisdiction has finally determined that Registry Operator is in fundamental and material breach of such covenant(s) or in breach of its payment obligations, and (iii) Registry Operator fails to comply with such determination and cure such breach within ten (10) calendar days or such other time period as may be determined by the arbitrator or court of competent jurisdiction.

(b) ICANN may, upon notice to Registry Operator, terminate this Agreement if Registry Operator fails to complete all testing and procedures (identified by ICANN in writing to Registry Operator prior to the date hereof) for delegation of the TLD

into the root zone within twelve (12) months of the Effective Date. Registry Operator may request an extension for up to additional twelve (12) months for delegation if it can demonstrate, to ICANN's reasonable satisfaction, that Registry Operator is working diligently and in good faith toward successfully completing the steps necessary for delegation of the TLD. Any fees paid by Registry Operator to ICANN prior to such termination date shall be retained by ICANN in full.

(c) ICANN may, upon notice to Registry Operator, terminate this Agreement if (i) Registry Operator fails to cure a material breach of Registry Operator's obligations set forth in Section 2.12 of this Agreement within thirty (30) calendar days of delivery of notice of such breach by ICANN, or if the Continued Operations Instrument is not in effect for greater than sixty (60) consecutive calendar days at any time following the Effective Date, (ii) an arbitrator or court of competent jurisdiction has finally determined that Registry Operator is in material breach of such covenant, and (iii) Registry Operator fails to cure such breach within ten (10) calendar days or such other time period as may be determined by the arbitrator or court of competent jurisdiction.

(d) ICANN may, upon notice to Registry Operator, terminate this Agreement if (i) Registry Operator makes an assignment for the benefit of creditors or similar act, (ii) attachment, garnishment or similar proceedings are commenced against Registry Operator, which proceedings are a material threat to Registry Operator's ability to operate the registry for the TLD, and are not dismissed within sixty (60) calendar days of their commencement, (iii) a trustee, receiver, liquidator or equivalent is appointed in place of Registry Operator or maintains control over any of Registry Operator's property, (iv) execution is levied upon any material property of Registry Operator, (v) proceedings are instituted by or against Registry Operator under any bankruptcy, insolvency, reorganization or other laws relating to the relief of debtors and such proceedings are not dismissed within sixty (60) calendar days of their commencement, or (vi) Registry Operator files for protection under the United States Bankruptcy Code, 11 U.S.C. Section 101, et seq., or a foreign equivalent or liquidates, dissolves or otherwise discontinues its operations or the operation of the TLD.

(e) ICANN may, upon thirty (30) calendar days' notice to Registry Operator, terminate this Agreement pursuant to Section 2 of Specification 7 or Sections 2 and 3 of Specification 11, subject to Registry Operator's right to challenge such termination as set forth in the applicable procedure described therein.

(f) ICANN may, upon notice to Registry Operator, terminate this Agreement if (i) Registry Operator knowingly employs any officer who is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such officer is not terminated within thirty (30) calendar days of Registry Operator's knowledge of the foregoing, or (ii) any member of Registry Operator's board of directors or similar governing body is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of

competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such member is not removed from Registry Operator's board of directors or similar governing body within thirty (30) calendar days of Registry Operator's knowledge of the foregoing.

(g) ICANN may, upon thirty (30) calendar days' notice to Registry Operator, terminate this Agreement as specified in Section 7.5.

4.4 Termination by Registry Operator.

(a) Registry Operator may terminate this Agreement upon notice to ICANN if (i) ICANN fails to cure any fundamental and material breach of ICANN's covenants set forth in Article 3, within thirty (30) calendar days after Registry Operator gives ICANN notice of such breach, which notice will include with specificity the details of the alleged breach, (ii) an arbitrator or court of competent jurisdiction has finally determined that ICANN is in fundamental and material breach of such covenants, and (iii) ICANN fails to comply with such determination and cure such breach within ten (10) calendar days or such other time period as may be determined by the arbitrator or court of competent jurisdiction.

(b) Registry Operator may terminate this Agreement for any reason upon one hundred eighty (180) calendar day advance notice to ICANN.

4.5 Transition of Registry upon Termination of Agreement. Upon expiration of the Term pursuant to Section 4.1 or Section 4.2 or any termination of this Agreement pursuant to Section 4.3 or Section 4.4, Registry Operator shall provide ICANN or any successor registry operator that may be designated by ICANN for the TLD in accordance with this Section 4.5 with all data (including the data escrowed in accordance with Section 2.3) regarding operations of the registry for the TLD necessary to maintain operations and registry functions that may be reasonably requested by ICANN or such successor registry operator. After consultation with Registry Operator, ICANN shall determine whether or not to transition operation of the TLD to a successor registry operator in its sole discretion and in conformance with the Registry Transition Process; provided, however, that (i) ICANN will take into consideration any intellectual property rights of Registry Operator (as communicated to ICANN by Registry Operator) in determining whether to transition operation of the TLD to a successor registry operator and (ii) if Registry Operator demonstrates to ICANN's reasonable satisfaction that (A) all domain name registrations in the TLD are registered to, and maintained by, Registry Operator or its Affiliates for their exclusive use, (B) Registry Operator does not sell, distribute or transfer control or use of any registrations in the TLD to any third party that is not an Affiliate of Registry Operator, and (C) transitioning operation of the TLD is not necessary to protect the public interest, then ICANN may not transition operation of the TLD to a successor registry operator upon the expiration or termination of this Agreement without the consent of Registry Operator (which shall not be unreasonably withheld, conditioned or delayed). For the avoidance of doubt, the foregoing sentence shall not prohibit ICANN from delegating the TLD pursuant

to a future application process for the delegation of top-level domains, subject to any processes and objection procedures instituted by ICANN in connection with such application process intended to protect the rights of third parties. Registry Operator agrees that ICANN may make any changes it deems necessary to the IANA database for DNS and WHOIS records with respect to the TLD in the event of a transition of the TLD pursuant to this Section 4.5. In addition, ICANN or its designee shall retain and may enforce its rights under the Continued Operations Instrument for the maintenance and operation of the TLD, regardless of the reason for termination or expiration of this Agreement.

4.6 Effect of Termination. Upon any expiration of the Term or termination of this Agreement, the obligations and rights of the parties hereto shall cease, provided that such expiration or termination of this Agreement shall not relieve the parties of any obligation or breach of this Agreement accruing prior to such expiration or termination, including, without limitation, all accrued payment obligations arising under Article 6. In addition, Article 5, Article 7, Section 2.12, Section 4.5, and this Section 4.6 shall survive the expiration or termination of this Agreement. For the avoidance of doubt, the rights of Registry Operator to operate the registry for the TLD shall immediately cease upon any expiration of the Term or termination of this Agreement.

ARTICLE 5.

DISPUTE RESOLUTION

5.1 Mediation. In the event of any dispute arising under or in connection with this Agreement, before either party may initiate arbitration pursuant to Section 5.2 below, ICANN and Registry Operator must attempt to resolve the dispute through mediation in accordance with the following terms and conditions:

(a) A party shall submit a dispute to mediation by written notice to the other party. The mediation shall be conducted by a single mediator selected by the parties. If the parties cannot agree on a mediator within fifteen (15) calendar days of delivery of written notice pursuant to this Section 5.1, the parties will promptly select a mutually acceptable mediation provider entity, which entity shall, as soon as practicable following such entity's selection, designate a mediator, who is a licensed attorney with general knowledge of contract law, has no ongoing business relationship with either party and, to the extent necessary to mediate the particular dispute, general knowledge of the domain name system. Any mediator must confirm in writing that he or she is not, and will not become during the term of the mediation, an employee, partner, executive officer, director, or security holder of ICANN or Registry Operator. If such confirmation is not provided by the appointed mediator, then a replacement mediator shall be appointed pursuant to this Section 5.1(a).

(b) The mediator shall conduct the mediation in accordance with the rules and procedures that he or she determines following consultation with the parties. The parties shall discuss the dispute in good faith and attempt, with the mediator's assistance, to reach an amicable resolution of the dispute. The mediation shall be treated

as a settlement discussion and shall therefore be confidential and may not be used against either party in any later proceeding relating to the dispute, including any arbitration pursuant to Section 5.2. The mediator may not testify for either party in any later proceeding relating to the dispute.

(c) Each party shall bear its own costs in the mediation. The parties shall share equally the fees and expenses of the mediator. Each party shall treat information received from the other party pursuant to the mediation that is appropriately marked as confidential (as required by Section 7.15) as Confidential Information of such other party in accordance with Section 7.15.

(d) If the parties have engaged in good faith participation in the mediation but have not resolved the dispute for any reason, either party or the mediator may terminate the mediation at any time and the dispute can then proceed to arbitration pursuant to Section 5.2 below. If the parties have not resolved the dispute for any reason by the date that is ninety (90) calendar days following the date of the notice delivered pursuant to Section 5.1(a), the mediation shall automatically terminate (unless extended by agreement of the parties) and the dispute can then proceed to arbitration pursuant to Section 5.2 below.

5.2 Arbitration. Disputes arising under or in connection with this Agreement that are not resolved pursuant to Section 5.1, including requests for specific performance, will be resolved through binding arbitration conducted pursuant to the rules of the International Court of Arbitration of the International Chamber of Commerce. The arbitration will be conducted in the English language and will occur in Los Angeles County, California. Any arbitration will be in front of a single arbitrator, unless (i) ICANN is seeking punitive or exemplary damages, or operational sanctions, (ii) the parties agree in writing to a greater number of arbitrators, or (iii) the dispute arises under Section 7.6 or 7.7. In the case of clauses (i), (ii) or (iii) in the preceding sentence, the arbitration will be in front of three arbitrators with each party selecting one arbitrator and the two selected arbitrators selecting the third arbitrator. In order to expedite the arbitration and limit its cost, the arbitrator(s) shall establish page limits for the parties' filings in conjunction with the arbitration, and should the arbitrator(s) determine that a hearing is necessary, the hearing shall be limited to one (1) calendar day, provided that in any arbitration in which ICANN is seeking punitive or exemplary damages, or operational sanctions, the hearing may be extended for one (1) additional calendar day if agreed upon by the parties or ordered by the arbitrator(s) based on the arbitrator(s) independent determination or the reasonable request of one of the parties thereto. The prevailing party in the arbitration will have the right to recover its costs and reasonable attorneys' fees, which the arbitrator(s) shall include in the awards. In the event the arbitrators determine that Registry Operator has been repeatedly and willfully in fundamental and material breach of its obligations set forth in Article 2, Article 6 or Section 5.4 of this Agreement, ICANN may request the arbitrators award punitive or exemplary damages, or operational sanctions (including without limitation an order temporarily restricting Registry Operator's right to sell new registrations). Each party shall treat information received from the other party pursuant to the arbitration that is appropriately marked as confidential (as required by Section 7.15) as

Confidential Information of such other party in accordance with Section 7.15. In any litigation involving ICANN concerning this Agreement, jurisdiction and exclusive venue for such litigation will be in a court located in Los Angeles County, California; however, the parties will also have the right to enforce a judgment of such a court in any court of competent jurisdiction.

5.3 Limitation of Liability. ICANN's aggregate monetary liability for violations of this Agreement will not exceed an amount equal to the Registry-Level Fees paid by Registry Operator to ICANN within the preceding twelve-month period pursuant to this Agreement (excluding the Variable Registry-Level Fee set forth in Section 6.3, if any). Registry Operator's aggregate monetary liability to ICANN for breaches of this Agreement will be limited to an amount equal to the fees paid to ICANN during the preceding twelve-month period (excluding the Variable Registry-Level Fee set forth in Section 6.3, if any), and punitive and exemplary damages, if any, awarded in accordance with Section 5.2, except with respect to Registry Operator's indemnification obligations pursuant to Section 7.1 and Section 7.2. In no event shall either party be liable for special, punitive, exemplary or consequential damages arising out of or in connection with this Agreement or the performance or nonperformance of obligations undertaken in this Agreement, except as provided in Section 5.2. Except as otherwise provided in this Agreement, neither party makes any warranty, express or implied, with respect to the services rendered by itself, its servants or agents, or the results obtained from their work, including, without limitation, any implied warranty of merchantability, non-infringement or fitness for a particular purpose.

5.4 Specific Performance. Registry Operator and ICANN agree that irreparable damage could occur if any of the provisions of this Agreement was not performed in accordance with its specific terms. Accordingly, the parties agree that they each shall be entitled to seek from the arbitrator or court of competent jurisdiction specific performance of the terms of this Agreement (in addition to any other remedy to which each party is entitled).

ARTICLE 6.

FEES

6.1 Registry-Level Fees.

(a) Registry Operator shall pay ICANN a registry-level fee equal to (i) the registry fixed fee of US\$6,250 per calendar quarter and (ii) the registry-level transaction fee (collectively, the "Registry-Level Fees"). The registry-level transaction fee will be equal to the number of annual increments of an initial or renewal domain name registration (at one or more levels, and including renewals associated with transfers from one ICANN-accredited registrar to another, each a "Transaction"), during the applicable calendar quarter multiplied by US\$0.25; provided, however that the registry-level transaction fee shall not apply until and unless more than 50,000 Transactions have occurred in the TLD during any calendar quarter or any consecutive four calendar quarter period in the

aggregate (the “Transaction Threshold”) and shall apply to each Transaction that occurred during each quarter in which the Transaction Threshold has been met, but shall not apply to each quarter in which the Transaction Threshold has not been met. Registry Operator’s obligation to pay the quarterly registry-level fixed fee will begin on the date on which the TLD is delegated in the DNS to Registry Operator. The first quarterly payment of the registry-level fixed fee will be prorated based on the number of calendar days between the delegation date and the end of the calendar quarter in which the delegation date falls.

(b) Subject to Section 6.1(a), Registry Operator shall pay the Registry-Level Fees on a quarterly basis to an account designated by ICANN within thirty (30) calendar days following the date of the invoice provided by ICANN.

6.2 Cost Recovery for RSTEP. Requests by Registry Operator for the approval of Additional Services pursuant to Section 2.1 may be referred by ICANN to the Registry Services Technical Evaluation Panel (“RSTEP”) pursuant to that process at <http://www.icann.org/en/registries/rsep/>. In the event that such requests are referred to RSTEP, Registry Operator shall remit to ICANN the invoiced cost of the RSTEP review within fourteen (14) calendar days of receipt of a copy of the RSTEP invoice from ICANN, unless ICANN determines, in its sole and absolute discretion, to pay all or any portion of the invoiced cost of such RSTEP review.

6.3 Variable Registry-Level Fee.

(a) If the ICANN accredited registrars (accounting, in the aggregate, for payment of two-thirds of all registrar-level fees (or such portion of ICANN accredited registrars necessary to approve variable accreditation fees under the then-current registrar accreditation agreement), do not approve, pursuant to the terms of their registrar accreditation agreements with ICANN, the variable accreditation fees established by the ICANN Board of Directors for any ICANN fiscal year, upon delivery of notice from ICANN, Registry Operator shall pay to ICANN a variable registry-level fee, which shall be paid on a fiscal quarter basis, and shall accrue as of the beginning of the first fiscal quarter of such ICANN fiscal year (the “Variable Registry-Level Fee”). The fee will be calculated and invoiced by ICANN on a quarterly basis, and shall be paid by Registry Operator within sixty (60) calendar days with respect to the first quarter of such ICANN fiscal year and within twenty (20) calendar days with respect to each remaining quarter of such ICANN fiscal year, of receipt of the invoiced amount by ICANN. The Registry Operator may invoice and collect the Variable Registry-Level Fees from the registrars that are party to a registry-registrar agreement with Registry Operator (which agreement may specifically provide for the reimbursement of Variable Registry-Level Fees paid by Registry Operator pursuant to this Section 6.3); provided, that the fees shall be invoiced to all ICANN accredited registrars if invoiced to any. The Variable Registry-Level Fee, if collectible by ICANN, shall be an obligation of Registry Operator and shall be due and payable as provided in this Section 6.3 irrespective of Registry Operator’s ability to seek and obtain reimbursement of such fee from registrars. In the event ICANN later collects variable accreditation fees for which Registry Operator has paid ICANN a Variable Registry-Level Fee, ICANN shall reimburse the Registry Operator an appropriate amount of the Variable Registry-Level Fee, as reasonably

determined by ICANN. If the ICANN accredited registrars (as a group) do approve, pursuant to the terms of their registrar accreditation agreements with ICANN, the variable accreditation fees established by the ICANN Board of Directors for a fiscal year, ICANN shall not be entitled to a Variable-Level Fee hereunder for such fiscal year, irrespective of whether the ICANN accredited registrars comply with their payment obligations to ICANN during such fiscal year.

(b) The amount of the Variable Registry-Level Fee will be specified for each registrar, and may include both a per-registrar component and a transactional component. The per-registrar component of the Variable Registry-Level Fee shall be specified by ICANN in accordance with the budget adopted by the ICANN Board of Directors for each ICANN fiscal year. The transactional component of the Variable Registry-Level Fee shall be specified by ICANN in accordance with the budget adopted by the ICANN Board of Directors for each ICANN fiscal year but shall not exceed US\$0.25 per domain name registration (including renewals associated with transfers from one ICANN accredited registrar to another) per year.

6.4 Pass Through Fees. Registry Operator shall pay to ICANN (i) a one-time fee equal to US\$5,000 for access to and use of the Trademark Clearinghouse as described in Specification 7 (the “RPM Access Fee”) and (ii) an amount specified by ICANN not to exceed US\$0.25 per Sunrise Registration and Claims Registration (as such terms are used in Trademark Clearinghouse RPMs incorporated herein pursuant to Specification 7) (the “RPM Registration Fee”). The RPM Access Fee will be invoiced as of the Effective Date of this Agreement, and Registry Operator shall pay such fee to an account specified by ICANN within thirty (30) calendar days following the date of the invoice. ICANN will invoice Registry Operator quarterly for the RPM Registration Fee, which shall be due in accordance with the invoicing and payment procedure specified in Section 6.1.

6.5 Adjustments to Fees. Notwithstanding any of the fee limitations set forth in this Article 6, commencing upon the expiration of the first year of this Agreement, and upon the expiration of each year thereafter during the Term, the then-current fees set forth in Section 6.1 and Section 6.3 may be adjusted, at ICANN’s discretion, by a percentage equal to the percentage change, if any, in (i) the Consumer Price Index for All Urban Consumers, U.S. City Average (1982-1984 = 100) published by the United States Department of Labor, Bureau of Labor Statistics, or any successor index (the “CPI”) for the month which is one (1) month prior to the commencement of the applicable year, over (ii) the CPI published for the month which is one (1) month prior to the commencement of the immediately prior year. In the event of any such increase, ICANN shall provide notice to Registry Operator specifying the amount of such adjustment. Any fee adjustment under this Section 6.5 shall be effective as of the first day of the first calendar quarter following at least thirty (30) days after ICANN’s delivery to Registry Operator of such fee adjustment notice.

6.6 Additional Fee on Late Payments. For any payments thirty (30) calendar days or more overdue under this Agreement, Registry Operator shall pay an additional fee on late payments at the rate of 1.5% per month or, if less, the maximum rate permitted by applicable law.

ARTICLE 7.

MISCELLANEOUS

7.1 Indemnification of ICANN.

(a) Registry Operator shall indemnify and defend ICANN and its directors, officers, employees, and agents (collectively, "Indemnitees") from and against any and all third-party claims, damages, liabilities, costs, and expenses, including reasonable legal fees and expenses, arising out of or relating to intellectual property ownership rights with respect to the TLD, the delegation of the TLD to Registry Operator, Registry Operator's operation of the registry for the TLD or Registry Operator's provision of Registry Services, provided that Registry Operator shall not be obligated to indemnify or defend any Indemnitee to the extent the claim, damage, liability, cost or expense arose: (i) due to the actions or omissions of ICANN, its subcontractors, panelists or evaluators specifically related to and occurring during the registry TLD application process (other than actions or omissions requested by or for the benefit of Registry Operator), or (ii) due to a breach by ICANN of any obligation contained in this Agreement or any willful misconduct by ICANN. This Section shall not be deemed to require Registry Operator to reimburse or otherwise indemnify ICANN for costs associated with the negotiation or execution of this Agreement, or with monitoring or management of the parties' respective obligations hereunder. Further, this Section shall not apply to any request for attorney's fees in connection with any litigation or arbitration between or among the parties, which shall be governed by Article 5 or otherwise awarded by a court of competent jurisdiction or arbitrator.

(b) For any claims by ICANN for indemnification whereby multiple registry operators (including Registry Operator) have engaged in the same actions or omissions that gave rise to the claim, Registry Operator's aggregate liability to indemnify ICANN with respect to such claim shall be limited to a percentage of ICANN's total claim, calculated by dividing the number of total domain names under registration with Registry Operator within the TLD (which names under registration shall be calculated consistently with Article 6 hereof for any applicable quarter) by the total number of domain names under registration within all top level domains for which the registry operators thereof are engaging in the same acts or omissions giving rise to such claim. For the purposes of reducing Registry Operator's liability under Section 7.1(a) pursuant to this Section 7.1(b), Registry Operator shall have the burden of identifying the other registry operators that are engaged in the same actions or omissions that gave rise to the claim, and demonstrating, to ICANN's reasonable satisfaction, such other registry operators' culpability for such actions or omissions. For the avoidance of doubt, in the event that a registry operator is engaged in the same acts or omissions giving rise to the claims, but such registry operator(s) do not have the same or similar indemnification obligations to ICANN as set forth in Section 7.1(a) above, the number of domains under management by such registry operator(s) shall nonetheless be included in the calculation in the preceding sentence.

7.2 Indemnification Procedures. If any third-party claim is commenced that is indemnified under Section 7.1 above, ICANN shall provide notice thereof to Registry

Operator as promptly as practicable. Registry Operator shall be entitled, if it so elects, in a notice promptly delivered to ICANN, to immediately take control of the defense and investigation of such claim and to employ and engage attorneys reasonably acceptable to ICANN to handle and defend the same, at Registry Operator's sole cost and expense, provided that in all events ICANN will be entitled to control at its sole cost and expense the litigation of issues concerning the validity or interpretation of ICANN's policies, Bylaws or conduct. ICANN shall cooperate, at Registry Operator's cost and expense, in all reasonable respects with Registry Operator and its attorneys in the investigation, trial, and defense of such claim and any appeal arising therefrom, and may, at its own cost and expense, participate, through its attorneys or otherwise, in such investigation, trial and defense of such claim and any appeal arising therefrom. No settlement of a claim that involves a remedy affecting ICANN other than the payment of money in an amount that is fully indemnified by Registry Operator will be entered into without the consent of ICANN. If Registry Operator does not assume full control over the defense of a claim subject to such defense in accordance with this Section 7.2, ICANN will have the right to defend the claim in such manner as it may deem appropriate, at the cost and expense of Registry Operator and Registry Operator shall cooperate in such defense.

7.3 Defined Terms. For purposes of this Agreement, unless such definitions are amended pursuant to a Consensus Policy at a future date, in which case the following definitions shall be deemed amended and restated in their entirety as set forth in such Consensus Policy, Security and Stability shall be defined as follows:

(a) For the purposes of this Agreement, an effect on "Security" shall mean (1) the unauthorized disclosure, alteration, insertion or destruction of registry data, or (2) the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards.

(b) For purposes of this Agreement, an effect on "Stability" shall refer to (1) lack of compliance with applicable relevant standards that are authoritative and published by a well-established and recognized Internet standards body, such as the relevant Standards-Track or Best Current Practice Requests for Comments ("RFCs") sponsored by the Internet Engineering Task Force; or (2) the creation of a condition that adversely affects the throughput, response time, consistency or coherence of responses to Internet servers or end systems operating in accordance with applicable relevant standards that are authoritative and published by a well-established and recognized Internet standards body, such as the relevant Standards-Track or Best Current Practice RFCs, and relying on Registry Operator's delegated information or provisioning of services.

7.4 No Offset. All payments due under this Agreement will be made in a timely manner throughout the Term and notwithstanding the pendency of any dispute (monetary or otherwise) between Registry Operator and ICANN.

7.5 Change of Control; Assignment and Subcontracting. Except as set forth in this Section 7.5, neither party may assign any of its rights and obligations under this Agreement without the prior written approval of the other party, which approval will not

be unreasonably withheld. For purposes of this Section 7.5, a direct or indirect change of control of Registry Operator or any subcontracting arrangement that relates to any Critical Function (as identified in Section 6 of Specification 10) for the TLD (a “Material Subcontracting Arrangement”) shall be deemed an assignment.

(a) Registry Operator must provide no less than thirty (30) calendar days advance notice to ICANN of any assignment or Material Subcontracting Arrangement, and any agreement to assign or subcontract any portion of the operations of the TLD (whether or not a Material Subcontracting Arrangement) must mandate compliance with all covenants, obligations and agreements by Registry Operator hereunder, and Registry Operator shall continue to be bound by such covenants, obligations and agreements. Registry Operator must also provide no less than thirty (30) calendar days advance notice to ICANN prior to the consummation of any transaction anticipated to result in a direct or indirect change of control of Registry Operator.

(b) Within thirty (30) calendar days of either such notification pursuant to Section 7.5(a), ICANN may request additional information from Registry Operator establishing (i) compliance with this Agreement and (ii) that the party acquiring such control or entering into such assignment or Material Subcontracting Arrangement (in any case, the “Contracting Party”) and the ultimate parent entity of the Contracting Party meets the ICANN-adopted specification or policy on registry operator criteria then in effect (including with respect to financial resources and operational and technical capabilities), in which case Registry Operator must supply the requested information within fifteen (15) calendar days.

(c) Registry Operator agrees that ICANN’s consent to any assignment, change of control or Material Subcontracting Arrangement will also be subject to background checks on any proposed Contracting Party (and such Contracting Party’s Affiliates).

(d) If ICANN fails to expressly provide or withhold its consent to any assignment, direct or indirect change of control of Registry Operator or any Material Subcontracting Arrangement within thirty (30) calendar days of ICANN’s receipt of notice of such transaction (or, if ICANN has requested additional information from Registry Operator as set forth above, thirty (30) calendar days of the receipt of all requested written information regarding such transaction) from Registry Operator, ICANN shall be deemed to have consented to such transaction.

(e) In connection with any such assignment, change of control or Material Subcontracting Arrangement, Registry Operator shall comply with the Registry Transition Process.

(f) Notwithstanding the foregoing, (i) any consummated change of control shall not be voidable by ICANN; provided, however, that, if ICANN reasonably determines to withhold its consent to such transaction, ICANN may terminate this Agreement pursuant to Section 4.3(g), (ii) ICANN may assign this Agreement without the

consent of Registry Operator upon approval of the ICANN Board of Directors in conjunction with a reorganization, reconstitution or re-incorporation of ICANN upon such assignee's express assumption of the terms and conditions of this Agreement, (iii) Registry Operator may assign this Agreement without the consent of ICANN directly to a wholly-owned subsidiary of Registry Operator, or, if Registry Operator is a wholly-owned subsidiary, to its direct parent or to another wholly-owned subsidiary of its direct parent, upon such subsidiary's or parent's, as applicable, express assumption of the terms and conditions of this Agreement, and (iv) ICANN shall be deemed to have consented to any assignment, Material Subcontracting Arrangement or change of control transaction in which the Contracting Party is an existing operator of a generic top-level domain pursuant to a registry agreement between such Contracting Party and ICANN (provided that such Contracting Party is then in compliance with the terms and conditions of such registry agreement in all material respects), unless ICANN provides to Registry Operator a written objection to such transaction within ten (10) calendar days of ICANN's receipt of notice of such transaction pursuant to this Section 7.5. Notwithstanding Section 7.5(a), in the event an assignment is made pursuant to clauses (ii) or (iii) of this Section 7.5(f), the assigning party will provide the other party with prompt notice following any such assignment.

7.6 Amendments and Waivers.

(a) If the ICANN Board of Directors determines that an amendment to this Agreement (including to the Specifications referred to herein) and all other registry agreements between ICANN and the Applicable Registry Operators (the "Applicable Registry Agreements") is desirable (each, a "Special Amendment"), ICANN may adopt a Special Amendment pursuant to the requirements of and process set forth in this Section 7.6; provided that a Special Amendment may not be a Restricted Amendment.

(b) Prior to submitting a Special Amendment for Registry Operator Approval, ICANN shall first consult in good faith with the Working Group regarding the form and substance of such Special Amendment. The duration of such consultation shall be reasonably determined by ICANN based on the substance of the Special Amendment. Following such consultation, ICANN may propose the adoption of a Special Amendment by publicly posting such amendment on its website for no less than thirty (30) calendar days (the "Posting Period") and providing notice of such proposed amendment to the Applicable Registry Operators in accordance with Section 7.9. ICANN will consider the public comments submitted on a Special Amendment during the Posting Period (including comments submitted by the Applicable Registry Operators).

(c) If, within one hundred eighty (180) calendar days following the expiration of the Posting Period (the "Approval Period"), the ICANN Board of Directors approves a Special Amendment (which may be in a form different than submitted for public comment, but must address the subject matter of the Special Amendment posted for public comment, as modified to reflect and/or address input from the Working Group and public comments), ICANN shall provide notice of, and submit, such Special Amendment for approval or disapproval by the Applicable Registry Operators. If, during the sixty (60) calendar day period following the date ICANN provides such notice to the Applicable

Registry Operators, such Special Amendment receives Registry Operator Approval, such Special Amendment shall be deemed approved (an "Approved Amendment") by the Applicable Registry Operators, and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Approved Amendment to Registry Operator (the "Amendment Effective Date"). In the event that a Special Amendment does not receive Registry Operator Approval, the Special Amendment shall be deemed not approved by the Applicable Registry Operators (a "Rejected Amendment"). A Rejected Amendment will have no effect on the terms and conditions of this Agreement, except as set forth below.

(d) If the ICANN Board of Directors reasonably determines that a Rejected Amendment falls within the subject matter categories set forth in Section 1.2 of Specification 1, the ICANN Board of Directors may adopt a resolution (the date such resolution is adopted is referred to herein as the "Resolution Adoption Date") requesting an Issue Report (as such term is defined in ICANN's Bylaws) by the Generic Names Supporting Organization (the "GNSO") regarding the substance of such Rejected Amendment. The policy development process undertaken by the GNSO pursuant to such requested Issue Report is referred to herein as a "PDP." If such PDP results in a Final Report supported by a GNSO Supermajority (as defined in ICANN's Bylaws) that either (i) recommends adoption of the Rejected Amendment as Consensus Policy or (ii) recommends against adoption of the Rejected Amendment as Consensus Policy, and, in the case of (i) above, the Board adopts such Consensus Policy, Registry Operator shall comply with its obligations pursuant to Section 2.2 of this Agreement. In either case, ICANN will abandon the Rejected Amendment and it will have no effect on the terms and conditions of this Agreement. Notwithstanding the foregoing provisions of this Section 7.6(d), the ICANN Board of Directors shall not be required to initiate a PDP with respect to a Rejected Amendment if, at any time in the twelve (12) month period preceding the submission of such Rejected Amendment for Registry Operator Approval pursuant to Section 7.6(c), the subject matter of such Rejected Amendment was the subject of a concluded or otherwise abandoned or terminated PDP that did not result in a GNSO Supermajority recommendation.

(e) If (a) a Rejected Amendment does not fall within the subject matter categories set forth in Section 1.2 of Specification 1, (b) the subject matter of a Rejected Amendment was, at any time in the twelve (12) month period preceding the submission of such Rejected Amendment for Registry Operator Approval pursuant to Section 7.6(c), the subject of a concluded or otherwise abandoned or terminated PDP that did not result in a GNSO Supermajority recommendation, or (c) a PDP does not result in a Final Report supported by a GNSO Supermajority that either (A) recommends adoption of the Rejected Amendment as Consensus Policy or (B) recommends against adoption of the Rejected Amendment as Consensus Policy (or such PDP has otherwise been abandoned or terminated for any reason), then, in any such case, such Rejected Amendment may still be adopted and become effective in the manner described below. In order for the Rejected Amendment to be adopted, the following requirements must be satisfied:

(i) the subject matter of the Rejected Amendment must be within the scope of ICANN's mission and consistent with a balanced application of its core values (as described in ICANN's Bylaws);

(ii) the Rejected Amendment must be justified by a Substantial and Compelling Reason in the Public Interest, must be likely to promote such interest, taking into account competing public and private interests that are likely to be affected by the Rejected Amendment, and must be narrowly tailored and no broader than reasonably necessary to address such Substantial and Compelling Reason in the Public Interest;

(iii) to the extent the Rejected Amendment prohibits or requires conduct or activities, imposes material costs on the Applicable Registry Operators, and/or materially reduces public access to domain name services, the Rejected Amendment must be the least restrictive means reasonably available to address the Substantial and Compelling Reason in the Public Interest;

(iv) the ICANN Board of Directors must submit the Rejected Amendment, along with a written explanation of the reasoning related to its determination that the Rejected Amendment meets the requirements set out in subclauses (i) through (iii) above, for public comment for a period of no less than thirty (30) calendar days; and

(v) following such public comment period, the ICANN Board of Directors must (a) engage in consultation (or direct ICANN management to engage in consultation) with the Working Group, subject matter experts, members of the GNSO, relevant advisory committees and other interested stakeholders with respect to such Rejected Amendment for a period of no less than sixty (60) calendar days; and (b) following such consultation, reapprove the Rejected Amendment (which may be in a form different than submitted for Registry Operator Approval, but must address the subject matter of the Rejected Amendment, as modified to reflect and/or address input from the Working Group and public comments) by the affirmative vote of at least two-thirds of the members of the ICANN Board of Directors eligible to vote on such matter, taking into account any ICANN policy affecting such eligibility, including ICANN's Conflict of Interest Policy (a "Board Amendment").

Such Board Amendment shall, subject to Section 7.6(f), be deemed an Approved Amendment, and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Board Amendment to Registry Operator (which effective date shall be deemed the Amendment Effective Date hereunder). Notwithstanding the foregoing, a Board Amendment may not amend the registry fees charged by ICANN hereunder, or amend this Section 7.6.

(f) Notwithstanding the provisions of Section 7.6(e), a Board Amendment shall not be deemed an Approved Amendment if, during the thirty (30) calendar day period following the approval by the ICANN Board of Directors of the Board Amendment, the Working Group, on the behalf of the Applicable Registry Operators, submits to the ICANN Board of Directors an alternative to the Board Amendment (an “Alternative Amendment”) that meets the following requirements:

(i) sets forth the precise text proposed by the Working Group to amend this Agreement in lieu of the Board Amendment;

(ii) addresses the Substantial and Compelling Reason in the Public Interest identified by the ICANN Board of Directors as the justification for the Board Amendment; and

(iii) compared to the Board Amendment is: (a) more narrowly tailored to address such Substantial and Compelling Reason in the Public Interest, and (b) to the extent the Alternative Amendment prohibits or requires conduct or activities, imposes material costs on Affected Registry Operators, or materially reduces access to domain name services, is a less restrictive means to address the Substantial and Compelling Reason in the Public Interest.

Any proposed amendment that does not meet the requirements of subclauses (i) through (iii) in the immediately preceding sentence shall not be considered an Alternative Amendment hereunder and therefore shall not supersede or delay the effectiveness of the Board Amendment. If, following the submission of the Alternative Amendment to the ICANN Board of Directors, the Alternative Amendment receives Registry Operator Approval, the Alternative Amendment shall supersede the Board Amendment and shall be deemed an Approved Amendment hereunder (and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Alternative Amendment to Registry Operator, which effective date shall be deemed the Amendment Effective Date hereunder), unless, within a period of sixty (60) calendar days following the date that the Working Group notifies the ICANN Board of Directors of Registry Operator Approval of such Alternative Amendment (during which time ICANN shall engage with the Working Group with respect to the Alternative Amendment), the ICANN Board of Directors by the affirmative vote of at least two-thirds of the members of the ICANN Board of Directors eligible to vote on such matter, taking into account any ICANN policy affecting such eligibility, including ICANN’s Conflict of Interest Policy, rejects the Alternative Amendment. If (A) the Alternative Amendment does not receive Registry Operator Approval within thirty (30) calendar days of submission of such Alternative Amendment to the Applicable Registry Operators (and the Working Group shall notify ICANN of the date of such submission), or (B) the ICANN Board of Directors rejects the Alternative Amendment by such two-thirds vote, the Board Amendment (and not the Alternative Amendment) shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice to Registry Operator (which

effective date shall be deemed the Amendment Effective Date hereunder). If the ICANN Board of Directors rejects an Alternative Amendment, the board shall publish a written rationale setting forth its analysis of the criteria set forth in Sections 7.6(f)(i) through 7.6(f)(iii). The ability of the ICANN Board of Directors to reject an Alternative Amendment hereunder does not relieve the Board of the obligation to ensure that any Board Amendment meets the criteria set forth in Section 7.6(e)(i) through 7.6(e)(v).

(g) In the event that Registry Operator believes an Approved Amendment does not meet the substantive requirements set out in this Section 7.6 or has been adopted in contravention of any of the procedural provisions of this Section 7.6, Registry Operator may challenge the adoption of such Special Amendment pursuant to the dispute resolution provisions set forth in Article 5, except that such arbitration shall be conducted by a three-person arbitration panel. Any such challenge must be brought within sixty (60) calendar days following the date ICANN provided notice to Registry Operator of the Approved Amendment, and ICANN may consolidate all challenges brought by registry operators (including Registry Operator) into a single proceeding. The Approved Amendment will be deemed not to have amended this Agreement during the pendency of the dispute resolution process.

(h) Registry Operator may apply in writing to ICANN for an exemption from the Approved Amendment (each such request submitted by Registry Operator hereunder, an "Exemption Request") during the thirty (30) calendar day period following the date ICANN provided notice to Registry Operator of such Approved Amendment. Each Exemption Request will set forth the basis for such request and provide detailed support for an exemption from the Approved Amendment. An Exemption Request may also include a detailed description and support for any alternatives to, or a variation of, the Approved Amendment proposed by such Registry Operator. An Exemption Request may only be granted upon a clear and convincing showing by Registry Operator that compliance with the Approved Amendment conflicts with applicable laws or would have a material adverse effect on the long-term financial condition or results of operations of Registry Operator. No Exemption Request will be granted if ICANN determines, in its reasonable discretion, that granting such Exemption Request would be materially harmful to registrants or result in the denial of a direct benefit to registrants. Within ninety (90) calendar days of ICANN's receipt of an Exemption Request, ICANN shall either approve (which approval may be conditioned or consist of alternatives to or a variation of the Approved Amendment) or deny the Exemption Request in writing, during which time the Approved Amendment will not amend this Agreement. If the Exemption Request is approved by ICANN, the Approved Amendment will not amend this Agreement; provided, that any conditions, alternatives or variations of the Approved Amendment required by ICANN shall be effective and, to the extent applicable, will amend this Agreement as of the Amendment Effective Date. If such Exemption Request is denied by ICANN, the Approved Amendment will amend this Agreement as of the Amendment Effective Date (or, if such date has passed, such Approved Amendment shall be deemed effective immediately on the date of such denial), provided that Registry Operator may, within thirty (30) calendar days following receipt of ICANN's determination, appeal ICANN's decision to deny the Exemption Request pursuant to the dispute resolution procedures set forth in Article 5. The Approved Amendment will be

deemed not to have amended this Agreement during the pendency of the dispute resolution process. For avoidance of doubt, only Exemption Requests submitted by Registry Operator that are approved by ICANN pursuant to this Section 7.6(j), agreed to by ICANN following mediation pursuant to Section 5.1 or through an arbitration decision pursuant to Section 5.2 shall exempt Registry Operator from any Approved Amendment, and no Exemption Request granted to any other Applicable Registry Operator (whether by ICANN or through arbitration) shall have any effect under this Agreement or exempt Registry Operator from any Approved Amendment.

(i) Except as set forth in this Section 7.6, Section 7.7 and as otherwise set forth in this Agreement and the Specifications hereto, no amendment, supplement or modification of this Agreement or any provision hereof shall be binding unless executed in writing by both parties, and nothing in this Section 7.6 or Section 7.7 shall restrict ICANN and Registry Operator from entering into bilateral amendments and modifications to this Agreement negotiated solely between the two parties. No waiver of any provision of this Agreement shall be binding unless evidenced by a writing signed by the party waiving compliance with such provision. No waiver of any of the provisions of this Agreement or failure to enforce any of the provisions hereof shall be deemed or shall constitute a waiver of any other provision hereof, nor shall any such waiver constitute a continuing waiver unless otherwise expressly provided. For the avoidance of doubt, nothing in this Sections 7.6 or 7.7 shall be deemed to limit Registry Operator's obligation to comply with Section 2.2.

(j) For purposes of this Section 7.6, the following terms shall have the following meanings:

(i) "Applicable Registry Operators" means, collectively, the registry operators of top-level domains party to a registry agreement that contains a provision similar to this Section 7.6, including Registry Operator.

(ii) "Registry Operator Approval" means the receipt of each of the following: (A) the affirmative approval of the Applicable Registry Operators whose payments to ICANN accounted for two-thirds of the total amount of fees (converted to U.S. dollars, if applicable, at the prevailing exchange rate published the prior day in the U.S. Edition of the Wall Street Journal for the date such calculation is made by ICANN) paid to ICANN by all the Applicable Registry Operators during the immediately previous calendar year pursuant to the Applicable Registry Agreements, and (B) the affirmative approval of a majority of the Applicable Registry Operators at the time such approval is obtained. For the avoidance of doubt, with respect to clause (B), each Applicable Registry Operator shall have one vote for each top-level domain operated by such Registry Operator pursuant to an Applicable Registry Agreement.

(iii) "Restricted Amendment" means the following: (A) an amendment of Specification 1, (B) except to the extent addressed in Section

2.10 hereof, an amendment that specifies the price charged by Registry Operator to registrars for domain name registrations, (C) an amendment to the definition of Registry Services as set forth in the first paragraph of Section 2.1 of Specification 6, or (D) an amendment to the length of the Term.

(iv) “Substantial and Compelling Reason in the Public Interest” means a reason that is justified by an important, specific, and articulated public interest goal that is within ICANN's mission and consistent with a balanced application of ICANN's core values as defined in ICANN's Bylaws.

(v) “Working Group” means representatives of the Applicable Registry Operators and other members of the community that the Registry Stakeholders Group appoints, from time to time, to serve as a working group to consult on amendments to the Applicable Registry Agreements (excluding bilateral amendments pursuant to Section 7.6(i)).

(k) Notwithstanding anything in this Section 7.6 to the contrary, (i) if Registry Operator provides evidence to ICANN's reasonable satisfaction that the Approved Amendment would materially increase the cost of providing Registry Services, then ICANN will allow up to one-hundred eighty (180) calendar days for Approved Amendment to become effective with respect to Registry Operator, and (ii) no Approved Amendment adopted pursuant to Section 7.6 shall become effective with respect to Registry Operator if Registry Operator provides ICANN with an irrevocable notice of termination pursuant to Section 4.4(b).

7.7 Negotiation Process.

(a) If either the Chief Executive Officer of ICANN (“CEO”) or the Chairperson of the Registry Stakeholder Group (“Chair”) desires to discuss any revision(s) to this Agreement, the CEO or Chair, as applicable, shall provide written notice to the other person, which shall set forth in reasonable detail the proposed revisions to this Agreement (a “Negotiation Notice”). Notwithstanding the foregoing, neither the CEO nor the Chair may (i) propose revisions to this Agreement that modify any Consensus Policy then existing, (ii) propose revisions to this Agreement pursuant to this Section 7.7 on or before June 30, 2014, or (iii) propose revisions or submit a Negotiation Notice more than once during any twelve (12) month period beginning on July 1, 2014.

(b) Following receipt of the Negotiation Notice by either the CEO or the Chair, ICANN and the Working Group (as defined in Section 7.6) shall consult in good faith negotiations regarding the form and substance of the proposed revisions to this Agreement, which shall be in the form of a proposed amendment to this Agreement (the “Proposed Revisions”), for a period of at least ninety (90) calendar days (unless a resolution is earlier reached) and attempt to reach a mutually acceptable agreement relating to the Proposed Revisions (the “Discussion Period”).

(c) If, following the conclusion of the Discussion Period, an agreement is reached on the Proposed Revisions, ICANN shall post the mutually agreed Proposed

Revisions on its website for public comment for no less than thirty (30) calendar days (the "Posting Period") and provide notice of such revisions to all Applicable Registry Operators in accordance with Section 7.9. ICANN and the Working Group will consider the public comments submitted on the Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registry Operators). Following the conclusion of the Posting Period, the Proposed Revisions shall be submitted for Registry Operator Approval (as defined in Section 7.6) and approval by the ICANN Board of Directors. If such approvals are obtained, the Proposed Revisions shall be deemed an Approved Amendment (as defined in Section 7.6) by the Applicable Registry Operators and ICANN, and shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days notice from ICANN to Registry Operator.

(d) If, following the conclusion of the Discussion Period, an agreement is not reached between ICANN and the Working Group on the Proposed Revisions, either the CEO or the Chair may provide the other person written notice (the "Mediation Notice") requiring each party to attempt to resolve the disagreements related to the Proposed Revisions through impartial, facilitative (non-evaluative) mediation in accordance with the terms and conditions set forth below. In the event that a Mediation Notice is provided, ICANN and the Working Group shall, within fifteen (15) calendar days thereof, simultaneously post the text of their desired version of the Proposed Revisions and a position paper with respect thereto on ICANN's website.

(i) The mediation shall be conducted by a single mediator selected by the parties. If the parties cannot agree on a mediator within fifteen (15) calendar days following receipt by the CEO or Chair, as applicable, of the Mediation Notice, the parties will promptly select a mutually acceptable mediation provider entity, which entity shall, as soon as practicable following such entity's selection, designate a mediator, who is a licensed attorney with general knowledge of contract law, who has no ongoing business relationship with either party and, to the extent necessary to mediate the particular dispute, general knowledge of the domain name system. Any mediator must confirm in writing that he or she is not, and will not become during the term of the mediation, an employee, partner, executive officer, director, or security holder of ICANN or an Applicable Registry Operator. If such confirmation is not provided by the appointed mediator, then a replacement mediator shall be appointed pursuant to this Section 7.7(d)(i).

(ii) The mediator shall conduct the mediation in accordance with the rules and procedures for facilitative mediation that he or she determines following consultation with the parties. The parties shall discuss the dispute in good faith and attempt, with the mediator's assistance, to reach an amicable resolution of the dispute.

(iii) Each party shall bear its own costs in the mediation. The parties shall share equally the fees and expenses of the mediator.

(iv) If an agreement is reached during the mediation, ICANN shall post the mutually agreed Proposed Revisions on its website for the Posting Period and provide notice to all Applicable Registry Operators in accordance with Section 7.9. ICANN and the Working Group will consider the public comments submitted on the agreed Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registry Operators). Following the conclusion of the Posting Period, the Proposed Revisions shall be submitted for Registry Operator Approval and approval by the ICANN Board of Directors. If such approvals are obtained, the Proposed Revisions shall be deemed an Approved Amendment (as defined in Section 7.6) by the Applicable Registry Operators and ICANN, and shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days notice from ICANN to Registry Operator.

(v) If the parties have not resolved the dispute for any reason by the date that is ninety (90) calendar days following receipt by the CEO or Chair, as applicable, of the Mediation Notice, the mediation shall automatically terminate (unless extended by agreement of the parties). The mediator shall deliver to the parties a definition of the issues that could be considered in future arbitration, if invoked. Those issues are subject to the limitations set forth in Section 7.7(e)(ii) below.

(e) If, following mediation, ICANN and the Working Group have not reached an agreement on the Proposed Revisions, either the CEO or the Chair may provide the other person written notice (an "Arbitration Notice") requiring ICANN and the Applicable Registry Operators to resolve the dispute through binding arbitration in accordance with the arbitration provisions of Section 5.2, subject to the requirements and limitations of this Section 7.7(e).

(i) If an Arbitration Notice is sent, the mediator's definition of issues, along with the Proposed Revisions (be those from ICANN, the Working Group or both) shall be posted for public comment on ICANN's website for a period of no less than thirty (30) calendar days. ICANN and the Working Group will consider the public comments submitted on the Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registry Operators), and information regarding such comments and consideration shall be provided to a three (3) person arbitrator panel. Each party may modify its Proposed Revisions before and after the Posting Period. The arbitration proceeding may not commence prior to the closing of such public comment period, and ICANN may consolidate all challenges brought by registry operators (including Registry Operator) into a single proceeding. Except as set forth in this Section 7.7, the arbitration shall be conducted pursuant to Section 5.2.

(ii) No dispute regarding the Proposed Revisions may be submitted for arbitration to the extent the subject matter of the Proposed

Revisions (i) relates to Consensus Policy, (ii) falls within the subject matter categories set forth in Section 1.2 of Specification 1, or (iii) seeks to amend any of the following provisions or Specifications of this Agreement: Articles 1, 3 and 6; Sections 2.1, 2.2, 2.5, 2.7, 2.9, 2.10, 2.16, 2.17, 2.19, 4.1, 4.2, 7.3, 7.6, 7.7, 7.8, 7.10, 7.11, 7.12, 7.13, 7.14, 7.16; Section 2.8 and Specification 7 (but only to the extent such Proposed Revisions seek to implement an RPM not contemplated by Sections 2.8 and Specification 7); Exhibit A; and Specifications 1, 4, 6, 10 and 11.

(iii) The mediator will brief the arbitrator panel regarding ICANN and the Working Group's respective proposals relating to the Proposed Revisions.

(iv) No amendment to this Agreement relating to the Proposed Revisions may be submitted for arbitration by either the Working Group or ICANN, unless, in the case of the Working Group, the proposed amendment has received Registry Operator Approval and, in the case of ICANN, the proposed amendment has been approved by the ICANN Board of Directors.

(v) In order for the arbitrator panel to approve either ICANN or the Working Group's proposed amendment relating to the Proposed Revisions, the arbitrator panel must conclude that such proposed amendment is consistent with a balanced application of ICANN's core values (as described in ICANN's Bylaws) and reasonable in light of the balancing of the costs and benefits to the business interests of the Applicable Registry Operators and ICANN (as applicable), and the public benefit sought to be achieved by the Proposed Revisions as set forth in such amendment. If the arbitrator panel concludes that either ICANN or the Working Group's proposed amendment relating to the Proposed Revisions meets the foregoing standard, such amendment shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days notice from ICANN to Registry Operator and deemed an Approved Amendment hereunder.

(f) With respect to an Approved Amendment relating to an amendment proposed by ICANN, Registry may apply in writing to ICANN for an exemption from such amendment pursuant to the provisions of Section 7.6.

(g) Notwithstanding anything in this Section 7.7 to the contrary, (a) if Registry Operator provides evidence to ICANN's reasonable satisfaction that the Approved Amendment would materially increase the cost of providing Registry Services, then ICANN will allow up to one-hundred eighty (180) calendar days for the Approved Amendment to become effective with respect to Registry Operator, and (b) no Approved Amendment adopted pursuant to Section 7.7 shall become effective with respect to Registry Operator if Registry Operator provides ICANN with an irrevocable notice of termination pursuant to Section 4.4(b).

7.8 No Third-Party Beneficiaries. This Agreement will not be construed to create any obligation by either ICANN or Registry Operator to any non-party to this Agreement, including any registrar or registered name holder.

7.9 General Notices. Except for notices pursuant to Sections 7.6 and 7.7, all notices to be given under or in relation to this Agreement will be given either (i) in writing at the address of the appropriate party as set forth below or (ii) via facsimile or electronic mail as provided below, unless that party has given a notice of change of postal or email address, or facsimile number, as provided in this Agreement. All notices under Sections 7.6 and 7.7 shall be given by both posting of the applicable information on ICANN's web site and transmission of such information to Registry Operator by electronic mail. Any change in the contact information for notice below will be given by the party within thirty (30) calendar days of such change. Other than notices under Sections 7.6 or 7.7, any notice required by this Agreement will be deemed to have been properly given (i) if in paper form, when delivered in person or via courier service with confirmation of receipt or (ii) if via facsimile or by electronic mail, upon confirmation of receipt by the recipient's facsimile machine or email server, provided that such notice via facsimile or electronic mail shall be followed by a copy sent by regular postal mail service within three (3) calendar days. Any notice required by Sections 7.6 or 7.7 will be deemed to have been given when electronically posted on ICANN's website and upon confirmation of receipt by the email server. In the event other means of notice become practically achievable, such as notice via a secure website, the parties will work together to implement such notice means under this Agreement.

If to ICANN, addressed to:
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA
Telephone: +1-310-301-5800
Facsimile: +1-310-823-8649
Attention: President and CEO

With a Required Copy to: General Counsel
Email: (As specified from time to time.)

If to Registry Operator, addressed to:
Dot Tech LLC
F/19, BC1, Ras Al Khaimah FTZ P.O Box # 16113
Ras Al Khaimah 16113
AE
Telephone: + 14153580831
Facsimile: + 15126847732
Attention: Brijesh Joshi, Director & General Manager
Email: dottech@radixregistry.com

7.10 Entire Agreement. This Agreement (including those specifications and documents incorporated by reference to URL locations which form a part of it) constitutes the entire agreement of the parties hereto pertaining to the operation of the TLD and supersedes all prior agreements, understandings, negotiations and discussions, whether oral or written, between the parties on that subject.

7.11 English Language Controls. Notwithstanding any translated version of this Agreement and/or specifications that may be provided to Registry Operator, the English language version of this Agreement and all referenced specifications are the official versions that bind the parties hereto. In the event of any conflict or discrepancy between any translated version of this Agreement and the English language version, the English language version controls. Notices, designations, determinations, and specifications made under this Agreement shall be in the English language.

7.12 Ownership Rights. Nothing contained in this Agreement shall be construed as (a) establishing or granting to Registry Operator any property ownership rights or interests of Registry Operator in the TLD or the letters, words, symbols or other characters making up the TLD string, or (b) affecting any existing intellectual property or ownership rights of Registry Operator.

7.13 Severability; Conflicts with Laws. This Agreement shall be deemed severable; the invalidity or unenforceability of any term or provision of this Agreement shall not affect the validity or enforceability of the balance of this Agreement or of any other term hereof, which shall remain in full force and effect. If any of the provisions hereof are determined to be invalid or unenforceable, the parties shall negotiate in good faith to modify this Agreement so as to effect the original intent of the parties as closely as possible. ICANN and the Working Group will mutually cooperate to develop an ICANN procedure for ICANN's review and consideration of alleged conflicts between applicable laws and non-WHOIS related provisions of this Agreement. Until such procedure is developed and implemented by ICANN, ICANN will review and consider alleged conflicts between applicable laws and non-WHOIS related provisions of this Agreement in a manner similar to ICANN's Procedure For Handling WHOIS Conflicts with Privacy Law.

7.14 Court Orders. ICANN will respect any order from a court of competent jurisdiction, including any orders from any jurisdiction where the consent or non-objection of the government was a requirement for the delegation of the TLD. Notwithstanding any other provision of this Agreement, ICANN's implementation of any such order will not be a breach of this Agreement

7.15 Confidentiality

(a) Subject to Section 7.15(c), during the Term and for a period of three (3) years thereafter, each party shall, and shall cause its and its Affiliates' officers, directors, employees and agents to, keep confidential and not publish or otherwise disclose to any third party, directly or indirectly, any information that is, and the disclosing party has marked as, or has otherwise designated in writing to the receiving party as, "confidential

trade secret,” “confidential commercial information” or “confidential financial information” (collectively, “Confidential Information”), except to the extent such disclosure is permitted by the terms of this Agreement.

(b) The confidentiality obligations under Section 7.15(a) shall not apply to any Confidential Information that (i) is or hereafter becomes part of the public domain by public use, publication, general knowledge or the like through no fault of the receiving party in breach of this Agreement, (ii) can be demonstrated by documentation or other competent proof to have been in the receiving party’s possession prior to disclosure by the disclosing party without any obligation of confidentiality with respect to such information, (iii) is subsequently received by the receiving party from a third party who is not bound by any obligation of confidentiality with respect to such information, (iv) has been published by a third party or otherwise enters the public domain through no fault of the receiving party, or (v) can be demonstrated by documentation or other competent evidence to have been independently developed by or for the receiving party without reference to the disclosing party’s Confidential Information.

(c) Each party shall have the right to disclose Confidential Information to the extent that such disclosure is (i) made in response to a valid order of a court of competent jurisdiction or, if in the reasonable opinion of the receiving party’s legal counsel, such disclosure is otherwise required by applicable law; provided, however, that the receiving party shall first have given notice to the disclosing party and given the disclosing party a reasonable opportunity to quash such order or to obtain a protective order or confidential treatment order requiring that the Confidential Information that is the subject of such order or other applicable law be held in confidence by such court or other third party recipient, unless the receiving party is not permitted to provide such notice under such order or applicable law, or (ii) made by the receiving party or any of its Affiliates to its or their attorneys, auditors, advisors, consultants, contractors or other third parties for use by such person or entity as may be necessary or useful in connection with the performance of the activities under this Agreement, provided that such third party is bound by confidentiality obligations at least as stringent as those set forth herein, either by written agreement or through professional responsibility standards.

* * * * *

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

By: _____
Akram Atallah
President, Global Domains Division

DOT TECH LLC

By: _____
Brijesh Joshi
Director & General Manager

EXHIBIT A

Approved Services

The ICANN gTLD Applicant Guidebook (located at <http://newgtlds.icann.org/en/applicants/agb>) and the RSEP specify processes for consideration of proposed registry services. Registry Operator may provide any service that is required by the terms of this Agreement. In addition, the following services (if any) are specifically identified as having been approved by ICANN prior to the effective date of the Agreement, and Registry Operator may provide such services:

1. DNS Service – TLD Zone Contents

Notwithstanding anything else in this Agreement, as indicated in section 2.2.3.3 of the gTLD Applicant Guidebook, permissible contents for the TLD's zone are:

- 1.1.** Apex SOA record
- 1.2.** Apex NS records and in-bailiwick glue for the TLD's DNS servers
- 1.3.** NS records and in-bailiwick glue for DNS servers of registered names in the TLD
- 1.4.** DS records for registered names in the TLD
- 1.5.** Records associated with signing the TLD zone (i.e., RRSIG, DNSKEY, NSEC, and NSEC3)

(Note: The above language effectively does not allow, among other things, the inclusion of DNS resource records that would enable a dotless domain name (e.g., apex A, AAAA, MX records) in the TLD zone.)

If Registry Operator wishes to place any DNS resource record type into its TLD DNS zone (other than those listed in Sections 1.1 through 1.5 above), it must describe in detail its proposal and submit a Registry Services Evaluation Process (RSEP) request. This will be evaluated per RSEP to determine whether the service would create a risk of a meaningful adverse impact on security or stability of the DNS. Registry Operator recognizes and acknowledges that a service based on the use of less-common DNS resource records in the TLD zone, even if approved, might not work as intended for all users due to lack of software support.

2. Anti-Abuse

Registry Operator may suspend, delete or otherwise make changes to domain names in compliance with its anti-abuse policy.

3. Registry Lock

Registry Operator may offer the Registry Lock service, which is a registry service that allows an authorized representative from the sponsoring Registrar, request the activation or deactivation of any of the following EPP statuses: serverUpdateProhibited, serverDeleteProhibited and/or serverTransferProhibited.

SPECIFICATION 1

CONSENSUS POLICIES AND TEMPORARY POLICIES SPECIFICATION

1. Consensus Policies.

- 1.1. “*Consensus Policies*” are those policies established (1) pursuant to the procedure set forth in ICANN’s Bylaws and due process, and (2) covering those topics listed in Section 1.2 of this Specification. The Consensus Policy development process and procedure set forth in ICANN’s Bylaws may be revised from time to time in accordance with the process set forth therein.
- 1.2. Consensus Policies and the procedures by which they are developed shall be designed to produce, to the extent possible, a consensus of Internet stakeholders, including the operators of gTLDs. Consensus Policies shall relate to one or more of the following:
 - 1.2.1 issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet or Domain Name System (“DNS”);
 - 1.2.2 functional and performance specifications for the provision of Registry Services;
 - 1.2.3 Security and Stability of the registry database for the TLD;
 - 1.2.4 registry policies reasonably necessary to implement Consensus Policies relating to registry operations or registrars;
 - 1.2.5 resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names); or
 - 1.2.6 restrictions on cross-ownership of registry operators and registrars or registrar resellers and regulations and restrictions with respect to registry operations and the use of registry and registrar data in the event that a registry operator and a registrar or registrar reseller are affiliated.
- 1.3. Such categories of issues referred to in Section 1.2 of this Specification shall include, without limitation:
 - 1.3.1 principles for allocation of registered names in the TLD (e.g., first-come/first-served, timely renewal, holding period after expiration);
 - 1.3.2 prohibitions on warehousing of or speculation in domain names by registries or registrars;

- 1.3.3 reservation of registered names in the TLD that may not be registered initially or that may not be renewed due to reasons reasonably related to (i) avoidance of confusion among or misleading of users, (ii) intellectual property, or (iii) the technical management of the DNS or the Internet (e.g., establishment of reservations of names from registration); and
 - 1.3.4 maintenance of and access to accurate and up-to-date information concerning domain name registrations; and procedures to avoid disruptions of domain name registrations due to suspension or termination of operations by a registry operator or a registrar, including procedures for allocation of responsibility for serving registered domain names in a TLD affected by such a suspension or termination.
 - 1.4. In addition to the other limitations on Consensus Policies, they shall not:
 - 1.4.1 prescribe or limit the price of Registry Services;
 - 1.4.2 modify the terms or conditions for the renewal or termination of the Registry Agreement;
 - 1.4.3 modify the limitations on Temporary Policies (defined below) or Consensus Policies;
 - 1.4.4 modify the provisions in the registry agreement regarding fees paid by Registry Operator to ICANN; or
 - 1.4.5 modify ICANN's obligations to ensure equitable treatment of registry operators and act in an open and transparent manner.
2. **Temporary Policies.** Registry Operator shall comply with and implement all specifications or policies established by the Board on a temporary basis, if adopted by the Board by a vote of at least two-thirds of its members, so long as the Board reasonably determines that such modifications or amendments are justified and that immediate temporary establishment of a specification or policy on the subject is necessary to maintain the stability or security of Registry Services or the DNS ("**Temporary Policies**").
 - 2.1. Such proposed specification or policy shall be as narrowly tailored as feasible to achieve those objectives. In establishing any Temporary Policy, the Board shall state the period of time for which the Temporary Policy is adopted and shall immediately implement the Consensus Policy development process set forth in ICANN's Bylaws.
 - 2.1.1 ICANN shall also issue an advisory statement containing a detailed explanation of its reasons for adopting the Temporary Policy and why

the Board believes such Temporary Policy should receive the consensus support of Internet stakeholders.

2.1.2 If the period of time for which the Temporary Policy is adopted exceeds ninety (90) calendar days, the Board shall reaffirm its temporary adoption every ninety (90) calendar days for a total period not to exceed one (1) year, in order to maintain such Temporary Policy in effect until such time as it becomes a Consensus Policy. If the one (1) year period expires or, if during such one (1) year period, the Temporary Policy does not become a Consensus Policy and is not reaffirmed by the Board, Registry Operator shall no longer be required to comply with or implement such Temporary Policy.

3. **Notice and Conflicts.** Registry Operator shall be afforded a reasonable period of time following notice of the establishment of a Consensus Policy or Temporary Policy in which to comply with such policy or specification, taking into account any urgency involved. In the event of a conflict between Registry Services and Consensus Policies or any Temporary Policy, the Consensus Policies or Temporary Policy shall control, but only with respect to subject matter in conflict.

SPECIFICATION 2

DATA ESCROW REQUIREMENTS

Registry Operator will engage an independent entity to act as data escrow agent (“**Escrow Agent**”) for the provision of data escrow services related to the Registry Agreement. The following Technical Specifications set forth in Part A, and Legal Requirements set forth in Part B, will be included in any data escrow agreement between Registry Operator and the Escrow Agent, under which ICANN must be named a third-party beneficiary. In addition to the following requirements, the data escrow agreement may contain other provisions that are not contradictory or intended to subvert the required terms provided below.

PART A – TECHNICAL SPECIFICATIONS

1. **Deposits.** There will be two types of Deposits: Full and Differential. For both types, the universe of Registry objects to be considered for data escrow are those objects necessary in order to offer all of the approved Registry Services.
 - 1.1. “**Full Deposit**” will consist of data that reflects the state of the registry as of 00:00:00 UTC (Coordinated Universal Time) on the day that such Full Deposit is submitted to Escrow Agent.
 - 1.2. “**Differential Deposit**” means data that reflects all transactions that were not reflected in the last previous Full or Differential Deposit, as the case may be. Each Differential Deposit will contain all database transactions since the previous Deposit was completed as of 00:00:00 UTC of each day, but Sunday. Differential Deposits must include complete Escrow Records as specified below that were not included or changed since the most recent full or Differential Deposit (i.e., newly added or modified domain names).
2. **Schedule for Deposits.** Registry Operator will submit a set of escrow files on a daily basis as follows:
 - 2.1. Each Sunday, a Full Deposit must be submitted to the Escrow Agent by 23:59 UTC.
 - 2.2. The other six (6) days of the week, a Full Deposit or the corresponding Differential Deposit must be submitted to Escrow Agent by 23:59 UTC.
3. **Escrow Format Specification.**
 - 3.1. **Deposit’s Format.** Registry objects, such as domains, contacts, name servers, registrars, etc. will be compiled into a file constructed as described in draft-arias-noguchi-registry-data-escrow, see Part A, Section 9, reference 1 of this Specification and draft-arias-noguchi-dnrd-objects-mapping, see Part A, Section 9, reference 2 of this Specification (collectively, the “DNDE Specification”). The DNDE Specification describes some elements as

optional; Registry Operator will include those elements in the Deposits if they are available. If not already an RFC, Registry Operator will use the most recent draft version of the DNDE Specification available at the Effective Date. Registry Operator may at its election use newer versions of the DNDE Specification after the Effective Date. Once the DNDE Specification is published as an RFC, Registry Operator will implement that version of the DNDE Specification, no later than one hundred eighty (180) calendar days after. UTF-8 character encoding will be used.

- 3.2. **Extensions.** If a Registry Operator offers additional Registry Services that require submission of additional data, not included above, additional “extension schemas” shall be defined in a case by case basis to represent that data. These “extension schemas” will be specified as described in Part A, Section 9, reference 2 of this Specification. Data related to the “extensions schemas” will be included in the deposit file described in Part A, Section 3.1 of this Specification. ICANN and the respective Registry Operator shall work together to agree on such new objects’ data escrow specifications.
4. **Processing of Deposit files.** The use of compression is recommended in order to reduce electronic data transfer times, and storage capacity requirements. Data encryption will be used to ensure the privacy of registry escrow data. Files processed for compression and encryption will be in the binary OpenPGP format as per OpenPGP Message Format - RFC 4880, see Part A, Section 9, reference 3 of this Specification. Acceptable algorithms for Public-key cryptography, Symmetric-key cryptography, Hash and Compression are those enumerated in RFC 4880, not marked as deprecated in OpenPGP IANA Registry, see Part A, Section 9, reference 4 of this Specification, that are also royalty-free. The process to follow for the data file in original text format is:
 - (1) The XML file of the deposit as described in Part A, Section 9, reference 1 of this Specification must be named as the containing file as specified in Section 5 but with the extension xml.
 - (2) The data file(s) are aggregated in a tarball file named the same as (1) but with extension tar.
 - (3) A compressed and encrypted OpenPGP Message is created using the tarball file as sole input. The suggested algorithm for compression is ZIP as per RFC 4880. The compressed data will be encrypted using the escrow agent’s public key. The suggested algorithms for Public-key encryption are Elgamal and RSA as per RFC 4880. The suggested algorithms for Symmetric-key encryption are TripleDES, AES128 and CAST5 as per RFC 4880.
 - (4) The file may be split as necessary if, once compressed and encrypted, it is larger than the file size limit agreed with the escrow agent. Every part of a

split file, or the whole file if not split, will be called a processed file in this section.

- (5) A digital signature file will be generated for every processed file using the Registry Operator's private key. The digital signature file will be in binary OpenPGP format as per RFC 4880 Section 9, reference 3, and will not be compressed or encrypted. The suggested algorithms for Digital signatures are DSA and RSA as per RFC 4880. The suggested algorithm for Hashes in Digital signatures is SHA256.
- (6) The processed files and digital signature files will then be transferred to the Escrow Agent through secure electronic mechanisms, such as, SFTP, SCP, HTTPS file upload, etc. as agreed between the Escrow Agent and the Registry Operator. Non-electronic delivery through a physical medium such as CD-ROMs, DVD-ROMs, or USB storage devices may be used if authorized by ICANN.
- (7) The Escrow Agent will then validate every (processed) transferred data file using the procedure described in Part A, Section 8 of this Specification.

5. **File Naming Conventions.** Files will be named according to the following convention: {gTLD}_{YYYY-MM-DD}_{type}_S{#}_R{rev}.{ext} where:

- 5.1. {gTLD} is replaced with the gTLD name; in case of an IDN-TLD, the ASCII-compatible form (A-Label) must be used;
- 5.2. {YYYY-MM-DD} is replaced by the date corresponding to the time used as a timeline watermark for the transactions; i.e. for the Full Deposit corresponding to 2009-08-02T00:00Z, the string to be used would be "2009-08-02";
- 5.3. {type} is replaced by:
 - (1) "full", if the data represents a Full Deposit;
 - (2) "diff", if the data represents a Differential Deposit;
 - (3) "thin", if the data represents a Bulk Registration Data Access file, as specified in Section 3 of Specification 4;
- 5.4. {#} is replaced by the position of the file in a series of files, beginning with "1"; in case of a lone file, this must be replaced by "1".
- 5.5. {rev} is replaced by the number of revision (or resend) of the file beginning with "0":

5.6. {ext} is replaced by “sig” if it is a digital signature file of the quasi-homonymous file. Otherwise it is replaced by “ryde”.

6. **Distribution of Public Keys.** Each of Registry Operator and Escrow Agent will distribute its public key to the other party (Registry Operator or Escrow Agent, as the case may be) via email to an email address to be specified. Each party will confirm receipt of the other party’s public key with a reply email, and the distributing party will subsequently reconfirm the authenticity of the key transmitted via offline methods, like in person meeting, telephone, etc. In this way, public key transmission is authenticated to a user able to send and receive mail via a mail server operated by the distributing party. Escrow Agent, Registry Operator and ICANN will exchange public keys by the same procedure.
7. **Notification of Deposits.** Along with the delivery of each Deposit, Registry Operator will deliver to Escrow Agent and to ICANN (using the API described in draft-lozano-icann-registry-interfaces, see Part A, Section 9, reference 5 of this Specification (the “Interface Specification”)) a written statement (which may be by authenticated e-mail) that includes a copy of the report generated upon creation of the Deposit and states that the Deposit has been inspected by Registry Operator and is complete and accurate. Registry Operator will include the Deposit’s “id” and “resend” attributes in its statement. The attributes are explained in Part A, Section 9, reference 1 of this Specification.

If not already an RFC, Registry Operator will use the most recent draft version of the Interface Specification at the Effective Date. Registry Operator may at its election use newer versions of the Interface Specification after the Effective Date. Once the Interface Specification is published as an RFC, Registry Operator will implement that version of the Interface Specification, no later than one hundred eighty (180) calendar days after such publishing.

8. **Verification Procedure.**
 - (1) The signature file of each processed file is validated.
 - (2) If processed files are pieces of a bigger file, the latter is put together.
 - (3) Each file obtained in the previous step is then decrypted and uncompressed.
 - (4) Each data file contained in the previous step is then validated against the format defined in Part A, Section 9, reference 1 of this Specification.
 - (5) If Part A, Section 9, reference 1 of this Specification includes a verification process, that will be applied at this step.

If any discrepancy is found in any of the steps, the Deposit will be considered incomplete.

9. **References.**

- (1) Domain Name Data Escrow Specification (work in progress),
<http://tools.ietf.org/html/draft-arias-noguchi-registry-data-escrow>
- (2) Domain Name Registration Data (DNRD) Objects Mapping,
<http://tools.ietf.org/html/draft-arias-noguchi-dnrd-objects-mapping>
- (3) OpenPGP Message Format, <http://www.rfc-editor.org/rfc/rfc4880.txt>
- (4) OpenPGP parameters,
<http://www.iana.org/assignments/pgp-parameters/pgp-parameters.xhtml>
- (5) ICANN interfaces for registries and data escrow agents,
<http://tools.ietf.org/html/draft-lozano-icann-registry-interfaces>

PART B – LEGAL REQUIREMENTS

1. **Escrow Agent.** Prior to entering into an escrow agreement, the Registry Operator must provide notice to ICANN as to the identity of the Escrow Agent, and provide ICANN with contact information and a copy of the relevant escrow agreement, and all amendments thereto. In addition, prior to entering into an escrow agreement, Registry Operator must obtain the consent of ICANN to (a) use the specified Escrow Agent, and (b) enter into the form of escrow agreement provided. ICANN must be expressly designated as a third-party beneficiary of the escrow agreement. ICANN reserves the right to withhold its consent to any Escrow Agent, escrow agreement, or any amendment thereto, all in its sole discretion.
2. **Fees.** Registry Operator must pay, or have paid on its behalf, fees to the Escrow Agent directly. If Registry Operator fails to pay any fee by the due date(s), the Escrow Agent will give ICANN written notice of such non-payment and ICANN may pay the past-due fee(s) within fifteen (15) calendar days after receipt of the written notice from Escrow Agent. Upon payment of the past-due fees by ICANN, ICANN shall have a claim for such amount against Registry Operator, which Registry Operator shall be required to submit to ICANN together with the next fee payment due under the Registry Agreement.
3. **Ownership.** Ownership of the Deposits during the effective term of the Registry Agreement shall remain with Registry Operator at all times. Thereafter, Registry Operator shall assign any such ownership rights (including intellectual property rights, as the case may be) in such Deposits to ICANN. In the event that during the term of the Registry Agreement any Deposit is released from escrow to ICANN, any intellectual property rights held by Registry Operator in the Deposits will automatically be licensed to ICANN or to a party designated in writing by ICANN on a non-exclusive, perpetual, irrevocable, royalty-free, paid-up basis, for any use related to the operation, maintenance or transition of the TLD.
4. **Integrity and Confidentiality.** Escrow Agent will be required to (i) hold and maintain the Deposits in a secure, locked, and environmentally safe facility, which is accessible only to authorized representatives of Escrow Agent, (ii) protect the integrity and confidentiality of the Deposits using commercially reasonable measures and (iii) keep and safeguard each Deposit for one (1) year. ICANN and Registry Operator will be provided the right to inspect Escrow Agent’s applicable records upon reasonable prior notice and during normal business hours. Registry Operator and ICANN will be provided with the right to designate a third-party auditor to audit Escrow Agent’s compliance with the technical specifications and maintenance requirements of this Specification 2 from time to time.

If Escrow Agent receives a subpoena or any other order from a court or other judicial tribunal pertaining to the disclosure or release of the Deposits, Escrow Agent will promptly notify the Registry Operator and ICANN unless prohibited by law. After notifying the Registry Operator and ICANN, Escrow Agent shall allow

sufficient time for Registry Operator or ICANN to challenge any such order, which shall be the responsibility of Registry Operator or ICANN; provided, however, that Escrow Agent does not waive its rights to present its position with respect to any such order. Escrow Agent will cooperate with the Registry Operator or ICANN to support efforts to quash or limit any subpoena, at such party's expense. Any party requesting additional assistance shall pay Escrow Agent's standard charges or as quoted upon submission of a detailed request.

5. **Copies.** Escrow Agent may be permitted to duplicate any Deposit, in order to comply with the terms and provisions of the escrow agreement.
6. **Release of Deposits.** Escrow Agent will make available for electronic download (unless otherwise requested) to ICANN or its designee, within twenty-four (24) hours, at the Registry Operator's expense, all Deposits in Escrow Agent's possession in the event that the Escrow Agent receives a request from Registry Operator to effect such delivery to ICANN, or receives one of the following written notices by ICANN stating that:
 - 6.1. the Registry Agreement has expired without renewal, or been terminated; or
 - 6.2. ICANN has not received a notification as described in Part B, Sections 7.1 and 7.2 of this Specification from Escrow Agent within five (5) calendar days after the Deposit's scheduled delivery date; (a) ICANN gave notice to Escrow Agent and Registry Operator of that failure; and (b) ICANN has not, within seven (7) calendar days after such notice, received the notification from Escrow Agent; or
 - 6.3. ICANN has received notification as described in Part B, Sections 7.1 and 7.2 of this Specification from Escrow Agent of failed verification of the latest escrow deposit for a specific date or a notification of a missing deposit, and the notification is for a deposit that should have been made on Sunday (i.e., a Full Deposit); (a) ICANN gave notice to Registry Operator of that receipt; and (b) ICANN has not, within seven (7) calendar days after such notice, received notification as described in Part B, Sections 7.1 and 7.2 of this Specification from Escrow Agent of verification of a remediated version of such Full Deposit; or
 - 6.4. ICANN has received five notifications from Escrow Agent within the last thirty (30) calendar days notifying ICANN of either missing or failed escrow deposits that should have been made Monday through Saturday (i.e., a Differential Deposit), and (x) ICANN provided notice to Registry Operator of the receipt of such notifications; and (y) ICANN has not, within seven (7) calendar days after delivery of such notice to Registry Operator, received notification from Escrow Agent of verification of a remediated version of such Differential Deposit; or

- 6.5. Registry Operator has: (i) ceased to conduct its business in the ordinary course; or (ii) filed for bankruptcy, become insolvent or anything analogous to any of the foregoing under the laws of any jurisdiction anywhere in the world; or
- 6.6. Registry Operator has experienced a failure of critical registry functions and ICANN has asserted its rights pursuant to Section 2.13 of the Agreement; or
- 6.7. a competent court, arbitral, legislative, or government agency mandates the release of the Deposits to ICANN; or
- 6.8. pursuant to Contractual and Operational Compliance Audits as specified under Section 2.11 of the Agreement.

Unless Escrow Agent has previously released the Registry Operator's Deposits to ICANN or its designee, Escrow Agent will deliver all Deposits to ICANN upon expiration or termination of the Registry Agreement or the Escrow Agreement.

7. **Verification of Deposits.**

- 7.1. Within twenty-four (24) hours after receiving each Deposit or corrected Deposit, Escrow Agent must verify the format and completeness of each Deposit and deliver to ICANN a notification generated for each Deposit. Reports will be delivered electronically using the API described in draft-lozano-icann-registry-interfaces, see Part A, Section 9, reference 5 of this Specification.
- 7.2. If Escrow Agent discovers that any Deposit fails the verification procedures or if Escrow Agent does not receive any scheduled Deposit, Escrow Agent must notify Registry Operator either by email, fax or phone and ICANN (using the API described in draft-lozano-icann-registry-interfaces, see Part A, Section 9, reference 5 of this Specification) of such nonconformity or non-receipt within twenty-four (24) hours after receiving the non-conformant Deposit or the deadline for such Deposit, as applicable. Upon notification of such verification or delivery failure, Registry Operator must begin developing modifications, updates, corrections, and other fixes of the Deposit necessary for the Deposit to be delivered and pass the verification procedures and deliver such fixes to Escrow Agent as promptly as possible.

8. **Amendments.** Escrow Agent and Registry Operator shall amend the terms of the Escrow Agreement to conform to this Specification 2 within ten (10) calendar days of any amendment or modification to this Specification 2. In the event of a conflict between this Specification 2 and the Escrow Agreement, this Specification 2 shall control.

9. **Indemnity.** Escrow Agent shall indemnify and hold harmless Registry Operator and ICANN, and each of their respective directors, officers, agents, employees, members,

and stockholders (“Indemnitees”) absolutely and forever from and against any and all claims, actions, damages, suits, liabilities, obligations, costs, fees, charges, and any other expenses whatsoever, including reasonable attorneys’ fees and costs, that may be asserted by a third party against any Indemnitee in connection with the misrepresentation, negligence or misconduct of Escrow Agent, its directors, officers, agents, employees and contractors.

SPECIFICATION 3

FORMAT AND CONTENT FOR REGISTRY OPERATOR MONTHLY REPORTING

Registry Operator shall provide one set of monthly reports per gTLD, using the API described in draft-lozano-icann-registry-interfaces, see Specification 2, Part A, Section 9, reference 5, with the following content.

ICANN may request in the future that the reports be delivered by other means and using other formats. ICANN will use reasonable commercial efforts to preserve the confidentiality of the information reported until three (3) months after the end of the month to which the reports relate. Unless set forth in this Specification 3, any reference to a specific time refers to Coordinated Universal Time (UTC). Monthly reports shall consist of data that reflects the state of the registry at the end of the month (UTC).

- 1. Per-Registrar Transactions Report.** This report shall be compiled in a comma separated-value formatted file as specified in RFC 4180. The file shall be named “gTLD-transactions-yyyymm.csv”, where “gTLD” is the gTLD name; in case of an IDN-TLD, the A-label shall be used; “yyyymm” is the year and month being reported. The file shall contain the following fields per registrar:

Field #	Field name	Description
01	registrar-name	Registrar’s full corporate name as registered with IANA
02	iana-id	For cases where the registry operator acts as registrar (i.e., without the use of an ICANN accredited registrar) 9999 should be used, otherwise the sponsoring Registrar IANA id should be used as specified in http://www.iana.org/assignments/registrar-ids
03	total-domains	total domain names under sponsorship in any EPP status but pendingCreate that have not been purged
04	total-nameservers	total name servers (either host objects or name server hosts as domain name attributes) associated with domain names registered for the TLD in any EPP status but pendingCreate that have not been purged
05	net-adds-1-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of one (1) year (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
06	net-adds-2-yr	number of domains successfully registered (i.e., not

		in EPP pendingCreate status) with an initial term of two(2) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
07	net-adds-3-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of three (3) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
08	net-adds-4-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of four (4) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
09	net-adds-5-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of five (5) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
10	net-adds-6-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of six (6) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
11	net-adds-7-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of seven (7) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
12	net-adds-8-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of eight (8) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
13	net-adds-9-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of nine (9) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
14	net-adds-10-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of ten (10) years (and not deleted within the add grace period). A transaction must be reported in the month

		the add grace period ends.
15	net-renews-1-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of one (1) year (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
16	net-renews-2-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of two (2) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
17	net-renews-3-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of three (3) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
18	net-renews-4-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of four (4) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
19	net-renews-5-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of five (5) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
20	net-renews-6-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of six (6) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.

21	net-renews-7-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of seven (7) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
22	net-renews-8-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of eight (8) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
23	net-renews-9-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of nine (9) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
24	net-renews-10-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of ten (10) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
25	transfer-gaining-successful	number of domain transfers initiated by this registrar that were successfully completed (either explicitly or automatically approved) and not deleted within the transfer grace period. A transaction must be reported in the month the transfer grace period ends.
26	transfer-gaining-nacked	number of domain transfers initiated by this registrar that were rejected (e.g., EPP transfer op="reject") by the other registrar
27	transfer-losing-successfully	number of domain transfers initiated by another registrar that were successfully completed (either explicitly or automatically approved)
28	transfer-losing-nacked	number of domain transfers initiated by another registrar that this registrar rejected (e.g., EPP transfer op="reject")

29	transfer-disputed-won	number of transfer disputes in which this registrar prevailed (reported in the month where the determination happened)
30	transfer-disputed-lost	number of transfer disputes this registrar lost (reported in the month where the determination happened)
31	transfer-disputed-nodecision	number of transfer disputes involving this registrar with a split or no decision (reported in the month where the determination happened)
32	deleted-domains-grace	domains deleted within the add grace period (does not include names deleted while in EPP pendingCreate status). A deletion must be reported in the month the name is purged.
33	deleted-domains-nograce	domains deleted outside the add grace period (does not include names deleted while in EPP pendingCreate status). A deletion must be reported in the month the name is purged.
34	restored-domains	domain names restored from redemption period
35	restored-noreport	total number of restored names for which the registrar failed to submit a restore report
36	agp-exemption-requests	total number of AGP (add grace period) exemption requests
37	agp-exemptions-granted	total number of AGP (add grace period) exemption requests granted
38	agp-exempted-domains	total number of names affected by granted AGP (add grace period) exemption requests
39	attempted-adds	number of attempted (both successful and failed) domain name create commands

The first line shall include the field names exactly as described in the table above as a “header line” as described in section 2 of RFC 4180. The last line of each report shall include totals for each column across all registrars; the first field of this line shall read “Totals” while the second field shall be left empty in that line. No other lines besides the ones described above shall be included. Line breaks shall be <U+000D, U+000A> as described in RFC 4180.

2. **Registry Functions Activity Report.** This report shall be compiled in a comma separated-value formatted file as specified in RFC 4180. The file shall be named “gTLD-activity-yyyymm.csv”, where “gTLD” is the gTLD name; in case of an IDN-TLD, the A-label shall be used; “yyyymm” is the year and month being reported. The file shall contain the following fields:

Field #	Field Name	Description
01	operational-registrars	number of operational registrars at the end of the reporting period
02	ramp-up-registrars	number of registrars that have received a password for access to OT&E at the end of the reporting period
03	pre-ramp-up-registrars	number of registrars that have requested access, but have not yet entered the ramp-up period at the end of the reporting period
04	zfa-passwords	number of active zone file access passwords at the end of the reporting period
05	whois-43-queries	number of WHOIS (port-43) queries responded during the reporting period
06	web-whois-queries	number of Web-based Whois queries responded during the reporting period, not including searchable Whois
07	searchable-whois-queries	number of searchable Whois queries responded during the reporting period, if offered
08	dns-udp-queries-received	number of DNS queries received over UDP transport during the reporting period
09	dns-udp-queries-responded	number of DNS queries received over UDP transport that were responded during the reporting period
10	dns-tcp-queries-received	number of DNS queries received over TCP transport during the reporting period
11	dns-tcp-queries-responded	number of DNS queries received over TCP transport that were responded during the reporting period
12	srs-dom-check	number of SRS (EPP and any other interface) domain name "check" requests responded during the reporting period
13	srs-dom-create	number of SRS (EPP and any other interface) domain name "create" requests responded during the reporting period
14	srs-dom-delete	number of SRS (EPP and any other interface) domain name "delete" requests responded during the reporting period
15	srs-dom-info	number of SRS (EPP and any other interface) domain name "info" requests responded during the reporting period

Field #	Field Name	Description
16	srs-dom-renew	number of SRS (EPP and any other interface) domain name "renew" requests responded during the reporting period
17	srs-dom-rgp-restore-report	number of SRS (EPP and any other interface) domain name RGP "restore" requests delivering a restore report responded during the reporting period
18	srs-dom-rgp-restore-request	number of SRS (EPP and any other interface) domain name RGP "restore" requests responded during the reporting period
19	srs-dom-transfer-approve	number of SRS (EPP and any other interface) domain name "transfer" requests to approve transfers responded during the reporting period
20	srs-dom-transfer-cancel	number of SRS (EPP and any other interface) domain name "transfer" requests to cancel transfers responded during the reporting period
21	srs-dom-transfer-query	number of SRS (EPP and any other interface) domain name "transfer" requests to query about a transfer responded during the reporting period
22	srs-dom-transfer-reject	number of SRS (EPP and any other interface) domain name "transfer" requests to reject transfers responded during the reporting period
23	srs-dom-transfer-request	number of SRS (EPP and any other interface) domain name "transfer" requests to request transfers responded during the reporting period
24	srs-dom-update	number of SRS (EPP and any other interface) domain name "update" requests (not including RGP restore requests) responded during the reporting period
25	srs-host-check	number of SRS (EPP and any other interface) host "check" requests responded during the reporting period
26	srs-host-create	number of SRS (EPP and any other interface) host "create" requests responded during the reporting period
27	srs-host-delete	number of SRS (EPP and any other interface) host "delete" requests responded during the reporting period

Field #	Field Name	Description
28	srs-host-info	number of SRS (EPP and any other interface) host "info" requests responded during the reporting period
29	srs-host-update	number of SRS (EPP and any other interface) host "update" requests responded during the reporting period
30	srs-cont-check	number of SRS (EPP and any other interface) contact "check" requests responded during the reporting period
31	srs-cont-create	number of SRS (EPP and any other interface) contact "create" requests responded during the reporting period
32	srs-cont-delete	number of SRS (EPP and any other interface) contact "delete" requests responded during the reporting period
33	srs-cont-info	number of SRS (EPP and any other interface) contact "info" requests responded during the reporting period
34	srs-cont-transfer-approve	number of SRS (EPP and any other interface) contact "transfer" requests to approve transfers responded during the reporting period
35	srs-cont-transfer-cancel	number of SRS (EPP and any other interface) contact "transfer" requests to cancel transfers responded during the reporting period
36	srs-cont-transfer-query	number of SRS (EPP and any other interface) contact "transfer" requests to query about a transfer responded during the reporting period
37	srs-cont-transfer-reject	number of SRS (EPP and any other interface) contact "transfer" requests to reject transfers responded during the reporting period
38	srs-cont-transfer-request	number of SRS (EPP and any other interface) contact "transfer" requests to request transfers responded during the reporting period
39	srs-cont-update	number of SRS (EPP and any other interface) contact "update" requests responded during the reporting period

The first line shall include the field names exactly as described in the table above as a "header line" as described in section 2 of RFC 4180. No other lines besides the ones

described above shall be included. Line breaks shall be <U+000D, U+000A> as described in RFC 4180.

For gTLDs that are part of a single-instance Shared Registry System, the Registry Functions Activity Report may include the total contact or host transactions for all the gTLDs in the system.

SPECIFICATION 4

REGISTRATION DATA PUBLICATION SERVICES

1. **Registration Data Directory Services.** Until ICANN requires a different protocol, Registry Operator will operate a WHOIS service available via port 43 in accordance with RFC 3912, and a web-based Directory Service at <whois.nic.TLD> providing free public query-based access to at least the following elements in the following format. ICANN reserves the right to specify alternative formats and protocols, and upon such specification, the Registry Operator will implement such alternative specification as soon as reasonably practicable.

Registry Operator shall implement a new standard supporting access to domain name registration data (SAC 051) no later than one hundred thirty-five (135) days after it is requested by ICANN if: 1) the IETF produces a standard (i.e., it is published, at least, as a Proposed Standard RFC as specified in RFC 2026); and 2) its implementation is commercially reasonable in the context of the overall operation of the registry.

- 1.1. The format of responses shall follow a semi-free text format outline below, followed by a blank line and a legal disclaimer specifying the rights of Registry Operator, and of the user querying the database.
- 1.2. Each data object shall be represented as a set of key/value pairs, with lines beginning with keys, followed by a colon and a space as delimiters, followed by the value.
- 1.3. For fields where more than one value exists, multiple key/value pairs with the same key shall be allowed (for example to list multiple name servers). The first key/value pair after a blank line should be considered the start of a new record, and should be considered as identifying that record, and is used to group data, such as hostnames and IP addresses, or a domain name and registrant information, together.
- 1.4. The fields specified below set forth the minimum output requirements. Registry Operator may output data fields in addition to those specified below, subject to approval by ICANN, which approval shall not be unreasonably withheld.
- 1.5. **Domain Name Data:**
 - 1.5.1 **Query format:** whois EXAMPLE.TLD
 - 1.5.2 **Response format:**

Domain Name: EXAMPLE.TLD
Domain ID: D1234567-TLD

WHOIS Server: whois.example.tld
Referral URL: http://www.example.tld
Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z
Registry Expiry Date: 2010-10-08T00:44:59Z
Sponsoring Registrar: EXAMPLE REGISTRAR LLC
Sponsoring Registrar IANA ID: 5555555
Domain Status: clientDeleteProhibited
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Domain Status: serverUpdateProhibited
Registrant ID: 5372808-ERL
Registrant Name: EXAMPLE REGISTRANT
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP
Registrant Postal Code: A1A1A1
Registrant Country: EX
Registrant Phone: +1.5555551212
Registrant Phone Ext: 1234
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE.TLD
Admin ID: 5372809-ERL
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: EX
Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213
Admin Fax Ext:
Admin Email: EMAIL@EXAMPLE.TLD
Tech ID: 5372811-ERL
Tech Name: EXAMPLE REGISTRAR TECHNICAL
Tech Organization: EXAMPLE REGISTRAR LLC
Tech Street: 123 EXAMPLE STREET
Tech City: ANYTOWN
Tech State/Province: AP
Tech Postal Code: A1A1A1
Tech Country: EX
Tech Phone: +1.1235551234

Tech Phone Ext: 1234
Tech Fax: +1.5555551213
Tech Fax Ext: 93
Tech Email: EMAIL@EXAMPLE.TLD
Name Server: NS01.EXAMPLEREGISTRAR.TLD
Name Server: NS02.EXAMPLEREGISTRAR.TLD
DNSSEC: signedDelegation
DNSSEC: unsigned
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<

1.6. Registrar Data:

1.6.1 **Query format:** whois "registrar Example Registrar, Inc."

1.6.2 **Response format:**

Registrar Name: Example Registrar, Inc.
Street: 1234 Admiralty Way
City: Marina del Rey
State/Province: CA
Postal Code: 90292
Country: US
Phone Number: +1.3105551212
Fax Number: +1.3105551213
Email: registrar@example.tld
WHOIS Server: whois.example-registrar.tld
Referral URL: http://www.example-registrar.tld
Admin Contact: Joe Registrar
Phone Number: +1.3105551213
Fax Number: +1.3105551213
Email: joeregistrar@example-registrar.tld
Admin Contact: Jane Registrar
Phone Number: +1.3105551214
Fax Number: +1.3105551213
Email: janeregistrar@example-registrar.tld
Technical Contact: John Geek
Phone Number: +1.3105551215
Fax Number: +1.3105551216
Email: johngeek@example-registrar.tld
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<

1.7. Nameserver Data:

1.7.1 **Query format:** whois "NS1.EXAMPLE.TLD", whois "nameserver (nameserver name)", or whois "nameserver (IP Address)"

1.7.2 Response format:

Server Name: NS1.EXAMPLE.TLD
IP Address: 192.0.2.123
IP Address: 2001:0DB8::1
Registrar: Example Registrar, Inc.
WHOIS Server: whois.example-registrar.tld
Referral URL: http://www.example-registrar.tld
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<

- 1.8. The format of the following data fields: domain status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers (the extension will be provided as a separate field as shown above), email addresses, date and times should conform to the mappings specified in EPP RFCs 5730-5734 so that the display of this information (or values return in WHOIS responses) can be uniformly processed and understood.
- 1.9. In order to be compatible with ICANN's common interface for WHOIS (InterNIC), WHOIS output shall be in the format outline above.
- 1.10. **Searchability.** Offering searchability capabilities on the Directory Services is optional but if offered by the Registry Operator it shall comply with the specification described in this section.
 - 1.10.1 Registry Operator will offer searchability on the web-based Directory Service.
 - 1.10.2 Registry Operator will offer partial match capabilities, at least, on the following fields: domain name, contacts and registrant's name, and contact and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state or province, etc.).
 - 1.10.3 Registry Operator will offer exact-match capabilities, at least, on the following fields: registrar id, name server name, and name server's IP address (only applies to IP addresses stored by the registry, i.e., glue records).
 - 1.10.4 Registry Operator will offer Boolean search capabilities supporting, at least, the following logical operators to join a set of search criteria: AND, OR, NOT.
 - 1.10.5 Search results will include domain names matching the search criteria.
 - 1.10.6 Registry Operator will: 1) implement appropriate measures to avoid abuse of this feature (e.g., permitting access only to legitimate

authorized users); and 2) ensure the feature is in compliance with any applicable privacy laws or policies.

- 1.11. Registry Operator shall provide a link on the primary website for the TLD (i.e., the website provided to ICANN for publishing on the ICANN website) to a web page designated by ICANN containing WHOIS policy and educational materials.

2. Zone File Access

2.1. Third-Party Access

- 2.1.1 **Zone File Access Agreement.** Registry Operator will enter into an agreement with any Internet user, which will allow such user to access an Internet host server or servers designated by Registry Operator and download zone file data. The agreement will be standardized, facilitated and administered by a Centralized Zone Data Access Provider, which may be ICANN or an ICANN designee (the "CZDA Provider"). Registry Operator (optionally through the CZDA Provider) will provide access to zone file data per Section 2.1.3 of this Specification and do so using the file format described in Section 2.1.4 of this Specification. Notwithstanding the foregoing, (a) the CZDA Provider may reject the request for access of any user that does not satisfy the credentialing requirements in Section 2.1.2 below; (b) Registry Operator may reject the request for access of any user that does not provide correct or legitimate credentials under Section 2.1.2 below or where Registry Operator reasonably believes will violate the terms of Section 2.1.5. below; and, (c) Registry Operator may revoke access of any user if Registry Operator has evidence to support that the user has violated the terms of Section 2.1.5 below.
- 2.1.2 **Credentialing Requirements.** Registry Operator, through the facilitation of the CZDA Provider, will request each user to provide it with information sufficient to correctly identify and locate the user. Such user information will include, without limitation, company name, contact name, address, telephone number, facsimile number, email address and IP address.
- 2.1.3 **Grant of Access.** Each Registry Operator (optionally through the CZDA Provider) will provide the Zone File FTP (or other Registry supported) service for an ICANN-specified and managed URL (specifically, <TLD>.zda.icann.org where <TLD> is the TLD for which the registry is responsible) for the user to access the Registry's zone data archives. Registry Operator will grant the user a non-exclusive, nontransferable, limited right to access Registry Operator's (optionally CZDA Provider's) Zone File hosting server, and to transfer

a copy of the top-level domain zone files, and any associated cryptographic checksum files no more than once per 24 hour period using FTP, or other data transport and access protocols that may be prescribed by ICANN. For every zone file access server, the zone files are in the top-level directory called <zone>.zone.gz, with <zone>.zone.gz.md5 and <zone>.zone.gz.sig to verify downloads. If the Registry Operator (or the CZDA Provider) also provides historical data, it will use the naming pattern <zone>-yyyymmdd.zone.gz, etc.

2.1.4 **File Format Standard.** Registry Operator (optionally through the CZDA Provider) will provide zone files using a subformat of the standard Master File format as originally defined in RFC 1035, Section 5, including all the records present in the actual zone used in the public DNS. Sub-format is as follows:

1. Each record must include all fields in one line as: <domain-name> <TTL> <class> <type> <RDATA>.
2. Class and Type must use the standard mnemonics and must be in lower case.
3. TTL must be present as a decimal integer.
4. Use of /X and /DDD inside domain names is allowed.
5. All domain names must be in lower case.
6. Must use exactly one tab as separator of fields inside a record.
7. All domain names must be fully qualified.
8. No \$ORIGIN directives.
9. No use of "@" to denote current origin.
10. No use of "blank domain names" at the beginning of a record to continue the use of the domain name in the previous record.
11. No \$INCLUDE directives.
12. No \$TTL directives.
13. No use of parentheses, e.g., to continue the list of fields in a record across a line boundary.
14. No use of comments.
15. No blank lines.

16. The SOA record should be present at the top and (duplicated at) the end of the zone file.
17. With the exception of the SOA record, all the records in a file must be in alphabetical order.
18. One zone per file. If a TLD divides its DNS data into multiple zones, each goes into a separate file named as above, with all the files combined using tar into a file called <tld>.zone.tar.

2.1.5 **Use of Data by User.** Registry Operator will permit user to use the zone file for lawful purposes; provided that (a) user takes all reasonable steps to protect against unauthorized access to and use and disclosure of the data and (b) under no circumstances will Registry Operator be required or permitted to allow user to use the data to, (i) allow, enable, or otherwise support the transmission by email, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than user's own existing customers, or (ii) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator or any ICANN-accredited registrar.

2.1.6 **Term of Use.** Registry Operator, through CZDA Provider, will provide each user with access to the zone file for a period of not less than three (3) months. Registry Operator will allow users to renew their Grant of Access.

2.1.7 **No Fee for Access.** Registry Operator will provide, and CZDA Provider will facilitate, access to the zone file to user at no cost.

2.2. **Co-operation**

2.2.1 **Assistance.** Registry Operator will co-operate and provide reasonable assistance to ICANN and the CZDA Provider to facilitate and maintain the efficient access of zone file data by permitted users as contemplated under this Schedule.

2.3. **ICANN Access.** Registry Operator shall provide bulk access to the zone files for the TLD to ICANN or its designee on a continuous basis in the manner ICANN may reasonably specify from time to time. Access will be provided at least daily. Zone files will include SRS data committed as close as possible to 00:00:00 UTC.

2.4. **Emergency Operator Access.** Registry Operator shall provide bulk access to the zone files for the TLD to the Emergency Operators designated by ICANN on a continuous basis in the manner ICANN may reasonably specify from time to time.

3. Bulk Registration Data Access to ICANN

- 3.1. **Periodic Access to Thin Registration Data.** In order to verify and ensure the operational stability of Registry Services as well as to facilitate compliance checks on accredited registrars, Registry Operator will provide ICANN on a weekly basis (the day to be designated by ICANN) with up-to-date Registration Data as specified below. Data will include data committed as of 00:00:00 UTC on the day previous to the one designated for retrieval by ICANN.
- 3.1.1 **Contents.** Registry Operator will provide, at least, the following data for all registered domain names: domain name, domain name repository object id (roid), registrar id (IANA ID), statuses, last updated date, creation date, expiration date, and name server names. For sponsoring registrars, at least, it will provide: registrar name, registrar repository object id (roid), hostname of registrar Whois server, and URL of registrar.
- 3.1.2 **Format.** The data will be provided in the format specified in Specification 2 for Data Escrow (including encryption, signing, etc.) but including only the fields mentioned in the previous section, i.e., the file will only contain Domain and Registrar objects with the fields mentioned above. Registry Operator has the option to provide a full deposit file instead as specified in Specification 2.
- 3.1.3 **Access.** Registry Operator will have the file(s) ready for download as of 00:00:00 UTC on the day designated for retrieval by ICANN. The file(s) will be made available for download by SFTP, though ICANN may request other means in the future.
- 3.2. **Exceptional Access to Thick Registration Data.** In case of a registrar failure, deaccreditation, court order, etc. that prompts the temporary or definitive transfer of its domain names to another registrar, at the request of ICANN, Registry Operator will provide ICANN with up-to-date data for the domain names of the losing registrar. The data will be provided in the format specified in Specification 2 for Data Escrow. The file will only contain data related to the domain names of the losing registrar. Registry Operator will provide the data as soon as commercially practicable, but in no event later than five (5) calendar days following ICANN's request. Unless otherwise agreed by Registry Operator and ICANN, the file will be made available for download by ICANN in the same manner as the data specified in Section 3.1 of this Specification.

SPECIFICATION 5

SCHEDULE OF RESERVED NAMES

Except to the extent that ICANN otherwise expressly authorizes in writing, and subject to the terms and conditions of this Specification, Registry Operator shall reserve the following labels from initial (i.e., other than renewal) registration within the TLD. If using self-allocation, the Registry Operator must show the registration in the RDDS. In the case of IDN names (as indicated below), IDN variants will be identified according to the registry operator IDN registration policy, where applicable.

1. **Example.** The ASCII label “EXAMPLE” shall be withheld from registration or allocated to Registry Operator at the second level and at all other levels within the TLD at which Registry Operator offers registrations (such second level and all other levels are collectively referred to herein as, “All Levels”). Such label may not be activated in the DNS, and may not be released for registration to any person or entity other than Registry Operator. Upon conclusion of Registry Operator’s designation as operator of the registry for the TLD, such withheld or allocated label shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such name without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.
2. **Two-character labels.** All two-character ASCII labels shall be withheld from registration or allocated to Registry Operator at the second level within the TLD. Such labels may not be activated in the DNS, and may not be released for registration to any person or entity other than Registry Operator, provided that such two-character label strings may be released to the extent that Registry Operator reaches agreement with the related government and country-code manager of the string as specified in the ISO 3166-1 alpha-2 standard. The Registry Operator may also propose the release of these reservations based on its implementation of measures to avoid confusion with the corresponding country codes, subject to approval by ICANN. Upon conclusion of Registry Operator’s designation as operator of the registry for the TLD, all such labels that remain withheld from registration or allocated to Registry Operator shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.
3. **Reservations for Registry Operations.**
 - 3.1. The following ASCII labels must be withheld from registration or allocated to Registry Operator at All Levels for use in connection with the operation of the registry for the TLD: WWW, RDDS and WHOIS. The following ASCII label must be allocated to Registry Operator at All Levels for use in connection with the operation of the registry for the TLD: NIC. Registry Operator may activate WWW, RDDS and WHOIS in the DNS, but must activate NIC in the

DNS, as necessary for the operation of the TLD. None of WWW, RDDS, WHOIS or NIC may be released or registered to any person (other than Registry Operator) or third party. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD all such withheld or allocated names shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

- 3.2. Registry Operator may activate in the DNS at All Levels up to one hundred (100) names (plus their IDN variants, where applicable) necessary for the operation or the promotion of the TLD. Registry Operator must act as the Registered Name Holder of such names as that term is defined in the then-current ICANN Registrar Accreditation Agreement (RAA). These activations will be considered Transactions for purposes of Section 6.1 of the Agreement. Registry Operator must either (i) register such names through an ICANN-accredited registrar; or (ii) self-allocate such names and with respect to those names submit to and be responsible to ICANN for compliance with ICANN Consensus Policies and the obligations set forth in Subsections 3.7.7.1 through 3.7.7.12 of the then-current RAA (or any other replacement clause setting out the terms of the registration agreement between a registrar and a registered name holder). At Registry Operator's discretion and in compliance with all other terms of this Agreement, such names may be released for registration to another person or entity.
- 3.3. Registry Operator may withhold from registration or allocate to Registry Operator names (including their IDN variants, where applicable) at All Levels in accordance with Section 2.6 of the Agreement. Such names may not be activated in the DNS, but may be released for registration to another person or entity at Registry Operator's discretion. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, all such names that remain withheld from registration or allocated to Registry Operator shall be transferred as specified by ICANN. Upon ICANN's request, Registry Operator shall provide a listing of all names withheld or allocated to Registry Operator pursuant to Section 2.6 of the Agreement. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.
4. **Country and Territory Names.** The country and territory names (including their IDN variants, where applicable) contained in the following internationally recognized lists shall be withheld from registration or allocated to Registry Operator at All Levels:
 - 4.1. the short form (in English) of all country and territory names contained on the ISO 3166-1 list, as updated from time to time, including the European

Union, which is exceptionally reserved on the ISO 3166-1 list, and its scope extended in August 1999 to any application needing to represent the name European Union

<http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166-1_decoding_table.htm>;

- 4.2. the United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World; and
- 4.3. the list of United Nations member states in 6 official United Nations languages prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names;

provided, that the reservation of specific country and territory names (including their IDN variants according to the registry operator IDN registration policy, where applicable) may be released to the extent that Registry Operator reaches agreement with the applicable government(s). Registry Operator must not activate such names in the DNS; provided, that Registry Operator may propose the release of these reservations, subject to review by ICANN's Governmental Advisory Committee and approval by ICANN. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, all such names that remain withheld from registration or allocated to Registry Operator shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

5. **International Olympic Committee; International Red Cross and Red Crescent Movement.** As instructed from time to time by ICANN, the names (including their IDN variants, where applicable) relating to the International Olympic Committee, International Red Cross and Red Crescent Movement listed at <http://www.icann.org/en/resources/registries/reserved> shall be withheld from registration or allocated to Registry Operator at the second level within the TLD. Additional International Olympic Committee, International Red Cross and Red Crescent Movement names (including their IDN variants) may be added to the list upon ten (10) calendar days notice from ICANN to Registry Operator. Such names may not be activated in the DNS, and may not be released for registration to any person or entity other than Registry Operator. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, all such names withheld from registration or allocated to Registry Operator shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.
6. **Intergovernmental Organizations.** As instructed from time to time by ICANN, Registry Operator will implement the protections mechanism determined by the

ICANN Board of Directors relating to the protection of identifiers for Intergovernmental Organizations. A list of reserved names for this Section 6 is available at <http://www.icann.org/en/resources/registries/reserved>. Additional names (including their IDN variants) may be added to the list upon ten (10) calendar days notice from ICANN to Registry Operator. Any such protected identifiers for Intergovernmental Organizations may not be activated in the DNS, and may not be released for registration to any person or entity other than Registry Operator. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, all such protected identifiers shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

SPECIFICATION 6

REGISTRY INTEROPERABILITY AND CONTINUITY SPECIFICATIONS

1. Standards Compliance

- 1.1. **DNS.** Registry Operator shall comply with relevant existing RFCs and those published in the future by the Internet Engineering Task Force (IETF), including all successor standards, modifications or additions thereto relating to the DNS and name server operations including without limitation RFCs 1034, 1035, 1123, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 4343, and 5966. DNS labels may only include hyphens in the third and fourth position if they represent valid IDNs (as specified above) in their ASCII encoding (e.g., “xn--ndk061n”).
- 1.2. **EPP.** Registry Operator shall comply with relevant existing RFCs and those published in the future by the Internet Engineering Task Force (IETF) including all successor standards, modifications or additions thereto relating to the provisioning and management of domain names using the Extensible Provisioning Protocol (EPP) in conformance with RFCs 5910, 5730, 5731, 5732 (if using host objects), 5733 and 5734. If Registry Operator implements Registry Grace Period (RGP), it will comply with RFC 3915 and its successors. If Registry Operator requires the use of functionality outside the base EPP RFCs, Registry Operator must document EPP extensions in Internet-Draft format following the guidelines described in RFC 3735. Registry Operator will provide and update the relevant documentation of all the EPP Objects and Extensions supported to ICANN prior to deployment.
- 1.3. **DNSSEC.** Registry Operator shall sign its TLD zone files implementing Domain Name System Security Extensions (“DNSSEC”). During the Term, Registry Operator shall comply with RFCs 4033, 4034, 4035, 4509 and their successors, and follow the best practices described in RFC 4641 and its successors. If Registry Operator implements Hashed Authenticated Denial of Existence for DNS Security Extensions, it shall comply with RFC 5155 and its successors. Registry Operator shall accept public-key material from child domain names in a secure manner according to industry best practices. Registry shall also publish in its website the DNSSEC Practice Statements (DPS) describing critical security controls and procedures for key material storage, access and usage for its own keys and secure acceptance of registrants’ public-key material. Registry Operator shall publish its DPS following the format described in RFC 6841.
- 1.4. **IDN.** If the Registry Operator offers Internationalized Domain Names (“IDNs”), it shall comply with RFCs 5890, 5891, 5892, 5893 and their successors. Registry Operator shall comply with the ICANN IDN Guidelines at <<http://www.icann.org/en/topics/idn/implementation-guidelines.htm>>,

as they may be amended, modified, or superseded from time to time. Registry Operator shall publish and keep updated its IDN Tables and IDN Registration Rules in the IANA Repository of IDN Practices as specified in the ICANN IDN Guidelines.

- 1.5. **IPv6.** Registry Operator shall be able to accept IPv6 addresses as glue records in its Registry System and publish them in the DNS. Registry Operator shall offer public IPv6 transport for, at least, two of the Registry's name servers listed in the root zone with the corresponding IPv6 addresses registered with IANA. Registry Operator should follow "DNS IPv6 Transport Operational Guidelines" as described in BCP 91 and the recommendations and considerations described in RFC 4472. Registry Operator shall offer public IPv6 transport for its Registration Data Publication Services as defined in Specification 4 of this Agreement; e.g., Whois (RFC 3912), Web based Whois. Registry Operator shall offer public IPv6 transport for its Shared Registration System (SRS) to any Registrar, no later than six (6) months after receiving the first request in writing from a gTLD accredited Registrar willing to operate with the SRS over IPv6.

2. **Registry Services**

- 2.1. **Registry Services.** "Registry Services" are, for purposes of the Agreement, defined as the following: (a) those services that are operations of the registry critical to the following tasks: the receipt of data from registrars concerning registrations of domain names and name servers; provision to registrars of status information relating to the zone servers for the TLD; dissemination of TLD zone files; operation of the registry DNS servers; and dissemination of contact and other information concerning domain name server registrations in the TLD as required by this Agreement; (b) other products or services that the Registry Operator is required to provide because of the establishment of a Consensus Policy as defined in Specification 1; (c) any other products or services that only a registry operator is capable of providing, by reason of its designation as the registry operator; and (d) material changes to any Registry Service within the scope of (a), (b) or (c) above.
- 2.2. **Wildcard Prohibition.** For domain names which are either not registered, or the registrant has not supplied valid records such as NS records for listing in the DNS zone file, or their status does not allow them to be published in the DNS, the use of DNS wildcard Resource Records as described in RFCs 1034 and 4592 or any other method or technology for synthesizing DNS Resources Records or using redirection within the DNS by the Registry is prohibited. When queried for such domain names the authoritative name servers must return a "Name Error" response (also known as NXDOMAIN), RCODE 3 as described in RFC 1035 and related RFCs. This provision applies for all DNS zone files at all levels in the DNS tree for which the Registry

Operator (or an affiliate engaged in providing Registration Services) maintains data, arranges for such maintenance, or derives revenue from such maintenance.

3. **Registry Continuity**

- 3.1. **High Availability.** Registry Operator will conduct its operations using network and geographically diverse, redundant servers (including network-level redundancy, end-node level redundancy and the implementation of a load balancing scheme where applicable) to ensure continued operation in the case of technical failure (widespread or local), or an extraordinary occurrence or circumstance beyond the control of the Registry Operator. Registry Operator's emergency operations department shall be available at all times to respond to extraordinary occurrences.
- 3.2. **Extraordinary Event.** Registry Operator will use commercially reasonable efforts to restore the critical functions of the registry within twenty-four (24) hours after the termination of an extraordinary event beyond the control of the Registry Operator and restore full system functionality within a maximum of forty-eight (48) hours following such event, depending on the type of critical function involved. Outages due to such an event will not be considered a lack of service availability.
- 3.3. **Business Continuity.** Registry Operator shall maintain a business continuity plan, which will provide for the maintenance of Registry Services in the event of an extraordinary event beyond the control of the Registry Operator or business failure of Registry Operator, and may include the designation of a Registry Services continuity provider. If such plan includes the designation of a Registry Services continuity provider, Registry Operator shall provide the name and contact information for such Registry Services continuity provider to ICANN. In the case of an extraordinary event beyond the control of the Registry Operator where the Registry Operator cannot be contacted, Registry Operator consents that ICANN may contact the designated Registry Services continuity provider, if one exists. Registry Operator shall conduct Registry Services Continuity testing at least once per year.

4. **Abuse Mitigation**

- 4.1. **Abuse Contact.** Registry Operator shall provide to ICANN and publish on its website its accurate contact details including a valid email and mailing address as well as a primary contact for handling inquiries related to malicious conduct in the TLD, and will provide ICANN with prompt notice of any changes to such contact details.
- 4.2. **Malicious Use of Orphan Glue Records.** Registry Operator shall take action to remove orphan glue records (as defined at <http://www.icann.org/en/committees/security/sac048.pdf>) when provided

with evidence in written form that such records are present in connection with malicious conduct.

5. **Supported Initial and Renewal Registration Periods**

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

6. **Name Collision Occurrence Management**

- 6.1. **No-Activation Period.** Registry Operator shall not activate any names in the DNS zone for the Registry TLD (except for "NIC") until at least 120 calendar days after the effective date of this agreement. Registry Operator may allocate names (subject to subsection 6.2 below) during this period only if Registry Operator causes registrants to be clearly informed of the inability to activate names until the No-Activation Period ends.

6.2. **Name Collision Occurrence Assessment**

- 6.2.1 Registry Operator shall not activate any names in the DNS zone for the Registry TLD except in compliance with a Name Collision Occurrence Assessment provided by ICANN regarding the Registry TLD. Registry Operator will either (A) implement the mitigation measures described in its Name Collision Occurrence Assessment before activating any second-level domain name, or (B) block those second-level domain names for which the mitigation measures as described in the Name Collision Occurrence Assessment have not been implemented and proceed with activating names that are not listed in the Assessment.
- 6.2.2 Notwithstanding subsection 6.2.1, Registry Operator may proceed with activation of names in the DNS zone without implementation of the measures set forth in Section 6.2.1 only if (A) ICANN determines that the Registry TLD is eligible for this alternative path to activation of names; and (B) Registry Operator blocks all second-level domain names identified by ICANN and set forth at <http://newgtlds.icann.org/en/announcements-and-media/announcement-2-17nov13-en> as such list may be modified by ICANN from time to time. Registry Operator may activate names pursuant to this subsection and later activate names pursuant to subsection 6.2.1.

- 6.2.3 The sets of names subject to mitigation or blocking pursuant to Sections 6.2.1 and 6.2.2 will be based on ICANN analysis of DNS information including "Day in the Life of the Internet" data maintained by the DNS Operations, Analysis, and Research Center (DNS-OARC) <<https://www.dns-oarc.net/oarc/data/ditl>>.
- 6.2.4 Registry Operator may participate in the development by the ICANN community of a process for determining whether and how these blocked names may be released.
- 6.2.5 If ICANN determines that the TLD is ineligible for the alternative path to activation of names, ICANN may elect not to delegate the TLD pending completion of the final Name Collision Occurrence Assessment for the TLD, and Registry Operator's completion of all required mitigation measures. Registry Operator understands that the mitigation measures required by ICANN as a condition to activation of names in the DNS zone for the TLD may include, without limitation, mitigation measures such as those described in Section 3.2 of the New gTLD Name Collision Occurrence Management Plan approved by the ICANN Board New gTLD Program Committee (NGPC) on 7 October 2013 as found at <<http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-annex-1-07oct13-en.pdf>>.

6.3. **Name Collision Report Handling**

- 6.3.1 During the first two years after delegation of the TLD, Registry Operator's emergency operations department shall be available to receive reports, relayed by ICANN, alleging demonstrably severe harm from collisions with overlapping use of the names outside of the authoritative DNS.
- 6.3.2 Registry Operator shall develop an internal process for handling in an expedited manner reports received pursuant to subsection 6.3.1 under which Registry Operator may, to the extent necessary and appropriate, remove a recently activated name from the TLD zone for a period of up to two years in order to allow the affected party to make changes to its systems.

SPECIFICATION 7

MINIMUM REQUIREMENTS FOR RIGHTS PROTECTION MECHANISMS

1. **Rights Protection Mechanisms.** Registry Operator shall implement and adhere to the rights protection mechanisms (“RPMs”) specified in this Specification. In addition to such RPMs, Registry Operator may develop and implement additional RPMs that discourage or prevent registration of domain names that violate or abuse another party’s legal rights. Registry Operator will include all RPMs required by this Specification 7 and any additional RPMs developed and implemented by Registry Operator in the registry-registrar agreement entered into by ICANN-accredited registrars authorized to register names in the TLD. Registry Operator shall implement in accordance with requirements set forth therein each of the mandatory RPMs set forth in the Trademark Clearinghouse as of the date hereof, as posted at <http://www.icann.org/en/resources/registries/tmch-requirements> (the “Trademark Clearinghouse Requirements”), which may be revised in immaterial respects by ICANN from time to time. Registry Operator shall not mandate that any owner of applicable intellectual property rights use any other trademark information aggregation, notification, or validation service in addition to or instead of the ICANN-designated Trademark Clearinghouse. If there is a conflict between the terms and conditions of this Agreement and the Trademark Clearinghouse Requirements, the terms and conditions of this Agreement shall control.
2. **Dispute Resolution Mechanisms.** Registry Operator will comply with the following dispute resolution mechanisms as they may be revised from time to time:
 - a. the Trademark Post-Delegation Dispute Resolution Procedure (PDDRP) and the Registration Restriction Dispute Resolution Procedure (RRDRP) adopted by ICANN (posted at <http://www.icann.org/en/resources/registries/pddrp> and <http://www.icann.org/en/resources/registries/rrdrp>, respectively). Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Agreement) following a determination by any PDDRP or RRDRP panel and to be bound by any such determination; and
 - b. the Uniform Rapid Suspension system (“URS”) adopted by ICANN (posted at <http://www.icann.org/en/resources/registries/urs>), including the implementation of determinations issued by URS examiners.

SPECIFICATION 8

CONTINUED OPERATIONS INSTRUMENT

1. The Continued Operations Instrument shall (a) provide for sufficient financial resources to ensure the continued operation of the critical registry functions related to the TLD set forth in Section 6 of Specification 10 to this Agreement for a period of three (3) years following any termination of this Agreement on or prior to the fifth anniversary of the Effective Date or for a period of one (1) year following any termination of this Agreement after the fifth anniversary of the Effective Date but prior to or on the sixth (6th) anniversary of the Effective Date, and (b) be in the form of either (i) an irrevocable standby letter of credit, or (ii) an irrevocable cash escrow deposit, each meeting the requirements set forth in item 50(b) of Attachment to Module 2 – Evaluation Questions and Criteria – of the gTLD Applicant Guidebook, as published and supplemented by ICANN prior to the date hereof (which is hereby incorporated by reference into this Specification 8). Registry Operator shall use its best efforts to take all actions necessary or advisable to maintain in effect the Continued Operations Instrument for a period of six (6) years from the Effective Date, and to maintain ICANN as a third party beneficiary thereof. If Registry Operator elects to obtain an irrevocable standby letter of credit but the term required above is unobtainable, Registry Operator may obtain a letter of credit with a one-year term and an “evergreen provision,” providing for annual extensions, without amendment, for an indefinite number of additional periods until the issuing bank informs ICANN of its final expiration or until ICANN releases the letter of credit as evidenced in writing, if the letter of credit otherwise meets the requirements set forth in item 50(b) of Attachment to Module 2 – Evaluation Questions and Criteria – of the gTLD Applicant Guidebook, as published and supplemented by ICANN prior to the date hereof; provided, however, that if the issuing bank informs ICANN of the expiration of such letter of credit prior to the sixth (6th) anniversary of the Effective Date, such letter of credit must provide that ICANN is entitled to draw the funds secured by the letter of credit prior to such expiration. The letter of credit must require the issuing bank to give ICANN at least thirty (30) calendar days’ notice of any such expiration or non-renewal. If the letter of credit expires or is terminated at any time prior to the sixth (6th) anniversary of the Effective Date, Registry Operator will be required to obtain a replacement Continued Operations Instrument. ICANN may draw the funds under the original letter of credit, if the replacement Continued Operations Instrument is not in place prior to the expiration of the original letter of credit. Registry Operator shall provide to ICANN copies of all final documents relating to the Continued Operations Instrument and shall keep ICANN reasonably informed of material developments relating to the Continued Operations Instrument. Registry Operator shall not agree to, or permit, any amendment of, or waiver under, the Continued Operations Instrument or other documentation relating thereto without the prior written consent of ICANN (such consent not to be unreasonably withheld).

2. If, notwithstanding the use of best efforts by Registry Operator to satisfy its obligations under the preceding paragraph, the Continued Operations Instrument expires or is terminated by another party thereto, in whole or in part, for any reason, prior to the sixth anniversary of the Effective Date, Registry Operator shall promptly (i) notify ICANN of such expiration or termination and the reasons therefor and (ii) arrange for an alternative instrument that provides for sufficient financial resources to ensure the continued operation of the critical registry functions related to the TLD set forth in Section 6 of Specification 10 to this Agreement for a period of three (3) years following any termination of this Agreement on or prior to the fifth anniversary of the Effective Date or for a period of one (1) year following any termination of this Agreement after the fifth anniversary of the Effective Date but prior to or on the sixth (6) anniversary of the Effective Date (an "Alternative Instrument"). Any such Alternative Instrument shall be on terms no less favorable to ICANN than the Continued Operations Instrument and shall otherwise be in form and substance reasonably acceptable to ICANN.
3. Notwithstanding anything to the contrary contained in this Specification 8, at any time, Registry Operator may replace the Continued Operations Instrument with an Alternative Instrument that (i) provides for sufficient financial resources to ensure the continued operation of the critical registry functions related to the TLD set forth in Section 6 of Specification 10 to this Agreement for a period of three (3) years following any termination of this Agreement on or prior to the fifth anniversary of the Effective Date or for a period one (1) year following any termination of this Agreement after the fifth anniversary of the Effective Date but prior to or on the sixth (6) anniversary of the Effective Date, and (ii) contains terms no less favorable to ICANN than the Continued Operations Instrument and is otherwise in form and substance reasonably acceptable to ICANN. In the event Registry Operator replaces the Continued Operations Instrument either pursuant to paragraph 2 or this paragraph 3, the terms of this Specification 8 shall no longer apply with respect to the original Continuing Operations Instrument, but shall thereafter apply with respect to such Alternative Instrument(s), and such instrument shall thereafter be considered the Continued Operations Instrument for purposes of this Agreement.

SPECIFICATION 9

REGISTRY OPERATOR CODE OF CONDUCT

1. In connection with the operation of the registry for the TLD, Registry Operator will not, and will not allow any parent, subsidiary, Affiliate, subcontractor or other related entity, to the extent such party is engaged in the provision of Registry Services with respect to the TLD (each, a “Registry Related Party”), to:
 - a. directly or indirectly show any preference or provide any special consideration to any registrar with respect to operational access to registry systems and related registry services, unless comparable opportunities to qualify for such preferences or considerations are made available to all registrars on substantially similar terms and subject to substantially similar conditions;
 - b. register domain names in its own right, except for names registered through an ICANN accredited registrar; provided, however, that Registry Operator may (a) reserve names from registration pursuant to Section 2.6 of the Agreement and (b) may withhold from registration or allocate to Registry Operator up to one hundred (100) names pursuant to Section 3.2 of Specification 5;
 - c. register names in the TLD or sub-domains of the TLD based upon proprietary access to information about searches or resolution requests by consumers for domain names not yet registered (commonly known as, “front-running”);
or
 - d. allow any Affiliated registrar to disclose Personal Data about registrants to Registry Operator or any Registry Related Party, except as reasonably necessary for the management and operations of the TLD, unless all unrelated third parties (including other registry operators) are given equivalent access to such user data on substantially similar terms and subject to substantially similar conditions.
2. If Registry Operator or a Registry Related Party also operates as a provider of registrar or registrar-reseller services, Registry Operator will, or will cause such Registry Related Party to, ensure that such services are offered through a legal entity separate from Registry Operator, and maintain separate books of accounts with respect to its registrar or registrar-reseller operations.
3. If Registry Operator or a Registry Related Party also operates as a provider of registrar or registrar-reseller services, Registry Operator will conduct internal reviews at least once per calendar year to ensure compliance with this Code of Conduct. Within twenty (20) calendar days following the end of each calendar year, Registry Operator will provide the results of the internal review, along with a certification executed by an executive officer of Registry Operator certifying as to

Registry Operator's compliance with this Code of Conduct, via email to an address to be provided by ICANN. (ICANN may specify in the future the form and contents of such reports or that the reports be delivered by other reasonable means.) Registry Operator agrees that ICANN may publicly post such results and certification; provided, however, ICANN shall not disclose Confidential Information contained in such results except in accordance with Section 7.15 of the Agreement.

4. Nothing set forth herein shall: (i) limit ICANN from conducting investigations of claims of Registry Operator's non-compliance with this Code of Conduct; or (ii) provide grounds for Registry Operator to refuse to cooperate with ICANN investigations of claims of Registry Operator's non-compliance with this Code of Conduct.
5. Nothing set forth herein shall limit the ability of Registry Operator or any Registry Related Party, to enter into arms-length transactions in the ordinary course of business with a registrar or reseller with respect to products and services unrelated in all respects to the TLD.
6. Registry Operator may request an exemption to this Code of Conduct, and such exemption may be granted by ICANN in ICANN's reasonable discretion, if Registry Operator demonstrates to ICANN's reasonable satisfaction that (i) all domain name registrations in the TLD are registered to, and maintained by, Registry Operator for the exclusive use of Registry Operator or its Affiliates, (ii) Registry Operator does not sell, distribute or transfer control or use of any registrations in the TLD to any third party that is not an Affiliate of Registry Operator, and (iii) application of this Code of Conduct to the TLD is not necessary to protect the public interest.

SPECIFICATION 10

REGISTRY PERFORMANCE SPECIFICATIONS

1. Definitions

- 1.1. **DNS.** Refers to the Domain Name System as specified in RFCs 1034, 1035, and related RFCs.
- 1.2. **DNSSEC proper resolution.** There is a valid DNSSEC chain of trust from the root trust anchor to a particular domain name, e.g., a TLD, a domain name registered under a TLD, etc.
- 1.3. **EPP.** Refers to the Extensible Provisioning Protocol as specified in RFC 5730 and related RFCs.
- 1.4. **IP address.** Refers to IPv4 or IPv6 addresses without making any distinction between the two. When there is need to make a distinction, IPv4 or IPv6 is used.
- 1.5. **Probes.** Network hosts used to perform (DNS, EPP, etc.) tests (see below) that are located at various global locations.
- 1.6. **RDDS.** Registration Data Directory Services refers to the collective of WHOIS and Web-based WHOIS services as defined in Specification 4 of this Agreement.
- 1.7. **RTT.** Round-Trip Time or RTT refers to the time measured from the sending of the first bit of the first packet of the sequence of packets needed to make a request until the reception of the last bit of the last packet of the sequence needed to receive the response. If the client does not receive the whole sequence of packets needed to consider the response as received, the request will be considered unanswered.
- 1.8. **SLR.** Service Level Requirement is the level of service expected for a certain parameter being measured in a Service Level Agreement (SLA).

2. Service Level Agreement Matrix

	Parameter	SLR (monthly basis)
DNS	DNS service availability	0 min downtime = 100% availability
	DNS name server availability	≤ 432 min of downtime (≈ 99%)
	TCP DNS resolution RTT	≤ 1500 ms, for at least 95% of the queries
	UDP DNS resolution RTT	≤ 500 ms, for at least 95% of the queries
	DNS update time	≤ 60 min, for at least 95% of the probes
RDDS	RDDS availability	≤ 864 min of downtime (≈ 98%)

	RDDS query RTT	≤ 2000 ms, for at least 95% of the queries
	RDDS update time	≤ 60 min, for at least 95% of the probes
EPP	EPP service availability	≤ 864 min of downtime (≈ 98%)
	EPP session-command RTT	≤ 4000 ms, for at least 90% of the commands
	EPP query-command RTT	≤ 2000 ms, for at least 90% of the commands
	EPP transform-command RTT	≤ 4000 ms, for at least 90% of the commands

Registry Operator is encouraged to do maintenance for the different services at the times and dates of statistically lower traffic for each service. However, note that there is no provision for planned outages or similar periods of unavailable or slow service; any downtime, be it for maintenance or due to system failures, will be noted simply as downtime and counted for SLA purposes.

3. DNS

- 3.1. **DNS service availability.** Refers to the ability of the group of listed-as-authoritative name servers of a particular domain name (e.g., a TLD), to answer DNS queries from DNS probes. For the service to be considered available at a particular moment, at least, two of the delegated name servers registered in the DNS must have successful results from “**DNS tests**” to each of their public-DNS registered “**IP addresses**” to which the name server resolves. If 51% or more of the DNS testing probes see the service as unavailable during a given time, the DNS service will be considered unavailable.
- 3.2. **DNS name server availability.** Refers to the ability of a public-DNS registered “**IP address**” of a particular name server listed as authoritative for a domain name, to answer DNS queries from an Internet user. All the public DNS-registered “**IP address**” of all name servers of the domain name being monitored shall be tested individually. If 51% or more of the DNS testing probes get undefined/unanswered results from “**DNS tests**” to a name server “**IP address**” during a given time, the name server “**IP address**” will be considered unavailable.
- 3.3. **UDP DNS resolution RTT.** Refers to the **RTT** of the sequence of two packets, the UDP DNS query and the corresponding UDP DNS response. If the **RTT** is 5 times greater than the time specified in the relevant **SLR**, the **RTT** will be considered undefined.
- 3.4. **TCP DNS resolution RTT.** Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the DNS response for only one DNS query. If the **RTT** is 5 times greater than the time specified in the relevant **SLR**, the **RTT** will be considered undefined.
- 3.5. **DNS resolution RTT.** Refers to either “**UDP DNS resolution RTT**” or “**TCP DNS resolution RTT**”.

- 3.6. **DNS update time.** Refers to the time measured from the reception of an EPP confirmation to a transform command on a domain name, until the name servers of the parent domain name answer “**DNS queries**” with data consistent with the change made. This only applies for changes to DNS information.
- 3.7. **DNS test.** Means one non-recursive DNS query sent to a particular “**IP address**” (via UDP or TCP). If DNSSEC is offered in the queried DNS zone, for a query to be considered answered, the signatures must be positively verified against a corresponding DS record published in the parent zone or, if the parent is not signed, against a statically configured Trust Anchor. The answer to the query must contain the corresponding information from the Registry System, otherwise the query will be considered unanswered. A query with a “**DNS resolution RTT**” 5 times higher than the corresponding SLR, will be considered unanswered. The possible results to a DNS test are: a number in milliseconds corresponding to the “**DNS resolution RTT**” or, undefined/unanswered.
- 3.8. **Measuring DNS parameters.** Every minute, every DNS probe will make an UDP or TCP “**DNS test**” to each of the public-DNS registered “**IP addresses**” of the name servers of the domain name being monitored. If a “**DNS test**” result is undefined/unanswered, the tested IP will be considered unavailable from that probe until it is time to make a new test.
- 3.9. **Collating the results from DNS probes.** The minimum number of active testing probes to consider a measurement valid is 20 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.
- 3.10. **Distribution of UDP and TCP queries.** DNS probes will send UDP or TCP “**DNS test**” approximating the distribution of these queries.
- 3.11. **Placement of DNS probes.** Probes for measuring DNS parameters shall be placed as near as possible to the DNS resolvers on the networks with the most users across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links.

4. **RDDS**

- 4.1. **RDDS availability.** Refers to the ability of all the RDDS services for the TLD, to respond to queries from an Internet user with appropriate data from the relevant Registry System. If 51% or more of the RDDS testing probes see any of the RDDS services as unavailable during a given time, the RDDS will be considered unavailable.

- 4.2. **WHOIS query RTT.** Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the WHOIS response. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.
- 4.3. **Web-based-WHOIS query RTT.** Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the HTTP response for only one HTTP request. If Registry Operator implements a multiple-step process to get to the information, only the last step shall be measured. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.
- 4.4. **RDDS query RTT.** Refers to the collective of “**WHOIS query RTT**” and “**Web-based- WHOIS query RTT**”.
- 4.5. **RDDS update time.** Refers to the time measured from the reception of an EPP confirmation to a transform command on a domain name, host or contact, up until the servers of the RDDS services reflect the changes made.
- 4.6. **RDDS test.** Means one query sent to a particular “**IP address**” of one of the servers of one of the RDDS services. Queries shall be about existing objects in the Registry System and the responses must contain the corresponding information otherwise the query will be considered unanswered. Queries with an **RTT** 5 times higher than the corresponding SLR will be considered as unanswered. The possible results to an RDDS test are: a number in milliseconds corresponding to the **RTT** or undefined/unanswered.
- 4.7. **Measuring RDDS parameters.** Every 5 minutes, RDDS probes will select one IP address from all the public-DNS registered “**IP addresses**” of the servers for each RDDS service of the TLD being monitored and make an “**RDDS test**” to each one. If an “**RDDS test**” result is undefined/unanswered, the corresponding RDDS service will be considered as unavailable from that probe until it is time to make a new test.
- 4.8. **Collating the results from RDDS probes.** The minimum number of active testing probes to consider a measurement valid is 10 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.
- 4.9. **Placement of RDDS probes.** Probes for measuring RDDS parameters shall be placed inside the networks with the most users across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links.

5. EPP

- 5.1. **EPP service availability.** Refers to the ability of the TLD EPP servers as a group, to respond to commands from the Registry accredited Registrars, who already have credentials to the servers. The response shall include appropriate data from the Registry System. An EPP command with “**EPP command RTT**” 5 times higher than the corresponding SLR will be considered as unanswered. If 51% or more of the EPP testing probes see the EPP service as unavailable during a given time, the EPP service will be considered unavailable.
- 5.2. **EPP session-command RTT.** Refers to the **RTT** of the sequence of packets that includes the sending of a session command plus the reception of the EPP response for only one EPP session command. For the login command it will include packets needed for starting the TCP session. For the logout command it will include packets needed for closing the TCP session. EPP session commands are those described in section 2.9.1 of EPP RFC 5730. If the **RTT** is 5 times or more the corresponding SLR, the **RTT** will be considered undefined.
- 5.3. **EPP query-command RTT.** Refers to the **RTT** of the sequence of packets that includes the sending of a query command plus the reception of the EPP response for only one EPP query command. It does not include packets needed for the start or close of either the EPP or the TCP session. EPP query commands are those described in section 2.9.2 of EPP RFC 5730. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.
- 5.4. **EPP transform-command RTT.** Refers to the **RTT** of the sequence of packets that includes the sending of a transform command plus the reception of the EPP response for only one EPP transform command. It does not include packets needed for the start or close of either the EPP or the TCP session. EPP transform commands are those described in section 2.9.3 of EPP RFC 5730. If the **RTT** is 5 times or more the corresponding SLR, the **RTT** will be considered undefined.
- 5.5. **EPP command RTT.** Refers to “**EPP session-command RTT**”, “**EPP query-command RTT**” or “**EPP transform-command RTT**”.
- 5.6. **EPP test.** Means one EPP command sent to a particular “**IP address**” for one of the EPP servers. Query and transform commands, with the exception of “create”, shall be about existing objects in the Registry System. The response shall include appropriate data from the Registry System. The possible results to an EPP test are: a number in milliseconds corresponding to the “**EPP command RTT**” or undefined/unanswered.

- 5.7. **Measuring EPP parameters.** Every 5 minutes, EPP probes will select one “IP address” of the EPP servers of the TLD being monitored and make an “EPP test”; every time they should alternate between the 3 different types of commands and between the commands inside each category. If an “EPP test” result is undefined/unanswered, the EPP service will be considered as unavailable from that probe until it is time to make a new test.
- 5.8. **Collating the results from EPP probes.** The minimum number of active testing probes to consider a measurement valid is 5 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.
- 5.9. **Placement of EPP probes.** Probes for measuring EPP parameters shall be placed inside or close to Registrars points of access to the Internet across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links.

6. Emergency Thresholds

The following matrix presents the emergency thresholds that, if reached by any of the services mentioned above for a TLD, would cause the emergency transition of the Registry for the TLD as specified in Section 2.13 of this Agreement.

Critical Function	Emergency Threshold
DNS Service (all servers)	4-hour total downtime / week
DNSSEC proper resolution	4-hour total downtime / week
EPP	24-hour total downtime / week
RDDS (WHOIS/Web-based WHOIS)	24-hour total downtime / week
Data Escrow	Breach of the Registry Agreement as described in Specification 2, Part B, Section 6.

7. Emergency Escalation

Escalation is strictly for purposes of notifying and investigating possible or potential issues in relation to monitored services. The initiation of any escalation and the subsequent cooperative investigations do not in themselves imply that a monitored service has failed its performance requirements.

Escalations shall be carried out between ICANN and Registry Operators, Registrars and Registry Operator, and Registrars and ICANN. Registry Operators and ICANN must provide said emergency operations departments. Current contacts must be maintained between

ICANN and Registry Operators and published to Registrars, where relevant to their role in escalations, prior to any processing of an Emergency Escalation by all related parties, and kept current at all times.

7.1. **Emergency Escalation initiated by ICANN**

Upon reaching 10% of the Emergency thresholds as described in Section 6 of this Specification, ICANN's emergency operations will initiate an Emergency Escalation with the relevant Registry Operator. An Emergency Escalation consists of the following minimum elements: electronic (i.e., email or SMS) and/or voice contact notification to the Registry Operator's emergency operations department with detailed information concerning the issue being escalated, including evidence of monitoring failures, cooperative troubleshooting of the monitoring failure between ICANN staff and the Registry Operator, and the commitment to begin the process of rectifying issues with either the monitoring service or the service being monitoring.

7.2. **Emergency Escalation initiated by Registrars**

Registry Operator will maintain an emergency operations department prepared to handle emergency requests from registrars. In the event that a registrar is unable to conduct EPP transactions with the registry for the TLD because of a fault with the Registry Service and is unable to either contact (through ICANN mandated methods of communication) the Registry Operator, or the Registry Operator is unable or unwilling to address the fault, the registrar may initiate an emergency escalation to the emergency operations department of ICANN. ICANN then may initiate an emergency escalation with the Registry Operator as explained above.

7.3. **Notifications of Outages and Maintenance**

In the event that a Registry Operator plans maintenance, it will provide notice to the ICANN emergency operations department, at least, twenty-four (24) hours ahead of that maintenance. ICANN's emergency operations department will note planned maintenance times, and suspend Emergency Escalation services for the monitored services during the expected maintenance outage period.

If Registry Operator declares an outage, as per its contractual obligations with ICANN, on services under a service level agreement and performance requirements, it will notify the ICANN emergency operations department. During that declared outage, ICANN's emergency operations department will note and suspend emergency escalation services for the monitored services involved.

8. **Covenants of Performance Measurement**

8.1. **No interference.** Registry Operator shall not interfere with measurement **Probes**, including any form of preferential treatment of the requests for the monitored services. Registry Operator shall respond to the measurement

tests described in this Specification as it would to any other request from an Internet user (for DNS and RDDS) or registrar (for EPP).

- 8.2. **ICANN testing registrar.** Registry Operator agrees that ICANN will have a testing registrar used for purposes of measuring the **SLRs** described above. Registry Operator agrees to not provide any differentiated treatment for the testing registrar other than no billing of the transactions. ICANN shall not use the registrar for registering domain names (or other registry objects) for itself or others, except for the purposes of verifying contractual compliance with the conditions described in this Agreement.

SPECIFICATION 11

PUBLIC INTEREST COMMITMENTS

1. Registry Operator will use only ICANN accredited registrars that are party to the Registrar Accreditation Agreement approved by the ICANN Board of Directors on 27 June 2013 in registering domain names. A list of such registrars shall be maintained by ICANN on ICANN's website.
2. (Intentionally omitted. Registry Operator has not included commitments, statements of intent or business plans provided for in its application to ICANN for the TLD.)
3. Registry Operator agrees to perform the following specific public interest commitments, which commitments shall be enforceable by ICANN and through the Public Interest Commitment Dispute Resolution Process established by ICANN (posted at <http://www.icann.org/en/resources/registries/picdrp>), which may be revised in immaterial respects by ICANN from time to time (the "PICDRP"). Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Agreement) following a determination by any PICDRP panel and to be bound by any such determination.
 - a. Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.
 - b. Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.
 - c. Registry Operator will operate the TLD in a transparent manner consistent with general principles of openness and non-discrimination by establishing, publishing and adhering to clear registration policies.

- d. Registry Operator of a “Generic String” TLD may not impose eligibility criteria for registering names in the TLD that limit registrations exclusively to a single person or entity and/or that person’s or entity’s “Affiliates” (as defined in Section 2.9(c) of the Registry Agreement). “Generic String” means a string consisting of a word or term that denominates or describes a general class of goods, services, groups, organizations or things, as opposed to distinguishing a specific brand of goods, services, groups, organizations or things from those of others.

EXHIBIT H

**HIGHLY CONFIDENTIAL –
ATTORNEYS' EYES ONLY**

Redacted – Third Party Designated Confidential Information

EXHIBIT I

CONFIDENTIAL

Redacted – Third Party Designated Confidential Information

EXHIBIT J

CONFIDENTIAL

Redacted – Third Party Designated Confidential Information

EXHIBIT K

CONFIDENTIAL

Redacted – Third Party Designated Confidential Information

EXHIBIT L

Case Detail

[Edit](#) [Clone](#) [SPAM](#)

▼ Case Information

Case Number	00225003 [View Hierarchy]	Internal Status	Closed
Account Name	Ruby Glen, LLC	Status	Closed
Contact Name	Daniel Schindler	Case Close Reason	Response Provided
Contact Type		Urgency	Moderate
Application ID	1-1527-54849	Severity	Sev 3
Registry		Case Record Type	General Case [Change]
Case Origin	Web	Category	Application Processing
Multiple Contacts Found	<input type="checkbox"/>	Sub Category	Initial Evaluation Process
Visible in Self-Service Portal	<input checked="" type="checkbox"/>	Case Owner	Jared Erwin [Change]
Suppress Notification	<input type="checkbox"/>	Assigned to	Jared Erwin
Updates On Case	<input type="checkbox"/>	Parent Case	
SLA Resolution status	SLA Exceeded		
Phone			

▼ Additional Information

Subject	.WEB Auction Postponement – Required Applicant Update
Description	<p>ICANN,</p> <p>It has come to our attention that one of the applicants for .WEB has failed to properly update its application. Upon information and belief, there have been changes to the Board of Directors and potential control of Nu Dot Co LLC ("NDC") that has materially changed its application. To our knowledge, however, NDC has not filed the required application change request.</p> <p>As you know, Section 1.2.7 of the Applicant Guidebook specifically states, "[i]f at any time during the evaluation process information previously submitted by an applicant becomes untrue or inaccurate, the applicant must promptly notify ICANN via submission of the appropriate forms. This includes applicant-specific information such as changes in the financial position and changes in ownership or control of the applicant... Failure to notify ICANN of any change in circumstances that would render any information provided in the application false or misleading may result in denial of the application." As you also know, ICANN has been clear that such requirements are in full force and effect until the registry agreement is executed with the successful applicant.</p> <p>Failure by No Dot Co LLC to maintain the accuracy of its application is detrimental to the other competing applicants, especially in light of the pending ICANN auction, creating an unfair competitive advantage for NDC.</p> <p>We request that ICANN investigate the change in NDC's Board and potential control and that the ICANN auction scheduled for July 27 be immediately postponed. The auction should be rescheduled after the final investigation is complete and NDC's requisite change request is resolved.</p> <p>We do not make this request lightly and haven't done so in well over 100 other scheduled ICANN auctions.</p> <p>Thank you and best regards, Jonathon Nevett</p>

Case Comments

[New](#)

[Case Comments Help](#)

Action	Public	Comment
		<p>Created By: Jared Erwin (6/27/2016 3:42 PM) Dear Daniel Schindler,</p> <p>Thank you for bringing this to our attention. We are reviewing the information provided, and we will work with the applicant directly should action be required. We note your request to postpone the auction for the .WEB/.WEBS contention set currently scheduled for 27 July 2016. Please continue to follow the standard auction process and monitor the Customer Portal for updates. If there are any changes to the auction date, we will notify you and all auction participants.</p>
Make Private	<input checked="" type="checkbox"/>	<p>Thank you for your attention. I will now resolve this case, but please do not hesitate to reopen it should you have any questions.</p> <p>Best regards, Jared Erwin New gTLD Operations</p>
		<p>Created By: Susan Yao (6/23/2016 10:17 AM) Dear Daniel Schindler,</p> <p>Thank you for your contacting ICANN Global Support on your request.</p>
Make Private	<input checked="" type="checkbox"/>	<p>Your request has been forwarded to our gTLD Team for processing. Someone from the team will be contacting you.</p> <p>Please do not hesitate to contact us if you have any other questions or concerns.</p> <p>Best regards, Susan Yao Global Support Analyst II ICANN Global Support</p>

EXHIBIT M

CONFIDENTIAL

Redacted – Third Party Designated Confidential Information

EXHIBIT N

CONFIDENTIAL

Redacted – Third Party Designated Confidential Information

EXHIBIT O

CONFIDENTIAL

Redacted – Third Party Designated Confidential Information

EXHIBIT P

CONFIDENTIAL

Redacted – Third Party Designated Confidential Information

EXHIBIT Q

From: Ausubel, Lawrence M. Contact Information Redacted
Sent: Wednesday, July 20, 2016 10:59 AM
Contact Information Redacted
To:
Cc: Contact Information Redacted
Subject: Reminders

Dear Jose Ignacio Rasco,

You are reminded that the Deposit Deadline for .WEB/.WEBS has passed and we are now in the Blackout Period. During the Blackout Period, all applicants for Contention Strings in the Auction are prohibited from cooperating or collaborating with respect to, discussing with each other, or disclosing to each other in any manner the substance of their own, or each other's, or any other competing applicants' bids or bidding strategies, or discussing or negotiating settlement agreements or post-Auction ownership transfer arrangements, with respect to any Contention Strings in the Auction.

You are also reminded of the following upcoming events in relation to the Auction:

- Connectivity Test: 21 July 2016 at 13:00 UTC (9:00 am New York time).
- Mock Auction: 26 July 2016 at 13:00 UTC (9:00 am New York time).
- Auction: 27 July 2016 at 13:00 UTC (9:00 am New York time).

Please feel free to contact us if you have any questions.

Kind regards,

Larry Ausubel
Power Auctions LLC

EXHIBIT R

CONFIDENTIAL

Redacted – Third Party Designated Confidential Information

EXHIBIT S

CONFIDENTIAL

Redacted – Third Party Designated Confidential Information

Redacted – Third Party Designated Confidential Information

EXHIBIT T

**HIGHLY CONFIDENTIAL –
ATTORNEYS' EYES ONLY**

Redacted – Third Party Designated Confidential Information