Internet Corporation for Assigned Names and Numbers

ARTICLES OF INCORPORATION OF INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

27

As Revised November 21, 1998

1. The name of this corporation is Internet Corporation for Assigned Names and Numbers (the "Corporation").

2. The name of the Corporation's initial agent for service of process in the State of California, United States of Ameri is C T Corporation System.

3. This Corporation is a nonprofit public benefit corporation and is not organized for the private gain of any person. It organized under the California Nonprofit Public Benefit Corporation Law for charitable and public purposes. The Corporation is organized, and will be operated, exclusively for charitable, educational, and scientific purposes within the meaning of § 501 (c)(3) of the Internal Revenue Code of 1986, as amended (the "Code"), or the corresponding provision of any future United States tax code. Any reference in these Articles to the Code shall include the corresponding provisions of any further United States tax code. In furtherance of the foregoing purposes, and in recognition of the fact that the Internet is an international network of networks, owned by no single nation, individual o organization, the Corporation shall, except as limited by Article 5 hereof, pursue the charitable and public purposes c lessening the burdens of government and promoting the global public interest in the operational stability of the Interne by (i) coordinating the assignment of Internet technical parameters as needed to maintain universal connectivity on t Internet; (ii) performing and overseeing functions related to the coordination of the Internet Protocol ("IP (Intellectual Property; or Internet Protocol)") address space; (iii) performing and overseeing functions related to the coordination c the Internet domain name system ("DNS (Domain Name System)"), including the development of policies for determining the circumstances under which new top-level domains are added to the DNS (Domain Name System) root system; (iv) overseeing operation of the authoritative Internet DNS (Domain Name System) root server system; and (v) engaging in any other related lawful activity in furtherance of items (i) through (iv).

4. The Corporation shall operate for the benefit of the Internet community as a whole, carrying out its activities in conformity with relevant principles of international law and applicable international conventions and local law and, to the extent appropriate and consistent with these Articles and its Bylaws, through open and transparent processes th enable competition and open entry in Internet-related markets. To this effect, the Corporation shall cooperate as appropriate with relevant international organizations.

5. Notwithstanding any other provision (other than Article 8) of these Articles:

a. The Corporation shall not carry on any other activities not permitted to be carried on (i) by a corporation exempt from United States income tax under § 501 (c)(3) of the Code or (ii) by a corporation, contributions to which are deductible under § 170 (c)(2) of the Code.

b. No substantial part of the activities of the Corporation shall be the carrying on of propaganda, or otherwise attempting to influence legislation, and the Corporation shall be empowered to make the election under § 501 (h) of the Code.

c. The Corporation shall not participate in, or intervene in (including the publishing or distribution of statements) any political campaign on behalf of or in opposition to any candidate for public office.

d. No part of the net earnings of the Corporation shall inure to the benefit of or be distributable to its members, directors, trustees, officers, or other private persons, except that the Corporation shall be authorized and empowered to pay reasonable compensation for services rendered and to make payments and distributions in furtherance of the purposes set forth in Article 3 hereof.

e. In no event shall the Corporation be controlled directly or indirectly by one or more "disqualified persons" (as defined in § 4946 of the Code) other than foundation managers and other than one or more organizations described in paragraph (1) or (2) of § 509 (a) of the Code.

6. To the full extent permitted by the California Nonprofit Public Benefit Corporation Law or any other applicable laws presently or hereafter in effect, no director of the Corporation shall be personally liable to the Corporation or its members, should the Corporation elect to have members in the future, for or with respect to any acts or omissions i the performance of his or her duties as a director of the Corporation. Any repeal or modification of this Article 6 shall not adversely affect any right or protection of a director of the Corporation existing immediately prior to such repeal o modification.

7. Upon the dissolution of the Corporation, the Corporation's assets shall be distributed for one or more of the exemp purposes set forth in Article 3 hereof and, if possible, to a § 501 (c)(3) organization organized and operated exclusive to lessen the burdens of government and promote the global public interest in the operational stability of the Internet, or shall be distributed to a governmental entity for such purposes, or for such other charitable and public purposes that lessen the burdens of government by providing for the operational stability of the Internet. Any assets not so disposed of shall be disposed of by a court of competent jurisdiction of the county in which the principal office of the Corporation is then located, exclusively for such purposes or to such organization or organizations, as such court shall determine, that are organized and operated exclusively for such purposes, unless no such corporation exists, and in such case any assets not disposed of shall be distributed to a § 501(c)(3) corporation chosen by such court.

8. Notwithstanding anything to the contrary in these Articles, if the Corporation determines that it will not be treated as a corporation exempt from federal income tax under § 501(c)(3) of the Code, all references herein to § 501(c)(3) of the Code shall be deemed to refer to § 501(c)(6) of the Code and Article 5(a)(ii), (b), (c) and (e) shall be deemed not to be a part of these Articles.

9. These Articles may be amended by the affirmative vote of at least two-thirds of the directors of the Corporation. When the Corporation has members, any such amendment must be ratified by a two-thirds (2/3) majority of the members voting on any proposed amendment.

Governance (/en/about/governance)

Guidelines (/en/about/governance/guidelines)

Articles of Incorporation (/en/about/governance/articles)

Bylaws (/en/about/governance/bylaws)

Board Documents (http://www.icann.org/en/groups/board/documents)

Board Code of Conduct (http://www.icann.org/en/groups/board/governance/code-of-conduct)

Board Conflicts of Interest Policy (http://www.icann.org/en/groups/board/governance/coi)

Board Statements of Interest (http://www.icann.org/en/groups/board/sois)

Summary of Conflicts of Interest and Ethics Practices Review (/en/about/governance/coi/summary-ethics-review-13may13-en)

Agreements (/en/about/agreements)

Accountability & Transparency (http://www.icann.org/en/news/in-focus/accountability)

AOC Review (/en/about/aoc-review)

Annual Report (/en/about/annual-report)

Financials (/en/about/financials)

Document Disclosure (/en/about/transparency)

Planning (/en/about/planning)

Stay Connected

Your email address please.

News Alerts: ☐ HTML ☐ Plain Text
Newsletter: ☐ HTML ☐ Plain Text
Compliance Newsletter: ☐ HTML ☐ Plain Text
Policy Update: ☐ HTML ☐ Plain Text

Subscribe

Follow us @icann (https://twitter.com/#!/icann/)
Videos (http://www.youtube.com/icannnews)
Photos on Flickr (http://www.flickr.com/photos/icann/)
Facebook (http://www.facebook.com/icannorg)

ICANN Blog (http://blog.icann.org/)
Community Wiki (https://community.icann.org/)
Planet ICANN (/en/groups/planet-icann)

RSS Feeds (/en/news/rss)

 Press (/news/press) | Site Map (/sitemap) | Privacy Policy (/help/privacy)

ICANN Network
myICANN (http://www.myicann.org/)
ASO (http://aso.icann.org)
ALAC (http://www.atlarge.icann.org)
ccNSO (http://ccnso.icann.org)
GAC (http://gac.icann.org)
GNSO (http://gnso.icann.org)
RSSAC (/en/groups/rssac)
SSAC (/en/groups/ssac)
Community Wiki (http://community.icann.org)
Meetings (http://meetings.icann.org)
New gTLDs (http://newgtlds.icann.org)
Help

(/en/help)
Acronym Helper

Example: ccTLD

New gTLD Application Submitted to ICANN by: Dot Registry LLC

String: INC

Originally Posted: 13 June 2012

Application ID: 1-880-35979

Applicant Information

1. Full legal name

Dot Registry LLC

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact n ormation Redacted

4. Fax number

Contact nformation Redacted

5. If applicable, website or URL

Primary Contact

6(a). Name

Ms. Tess Pattison-Wade

6(b). Title

Executive Director

6(c). Address

6(d). Phone Number

Contact n ormation 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 nformation Redacted

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Limited Liability Company

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

Kansas

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

Christopher Michael Parrott	Director of Finance
Paul Eugene Spurgeon	COO
Scott Adam Schactman	Director Law & 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

Ecyber Solutions Group Inc	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.

INC

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.

To build confidence, trust, reliance, and loyalty for consumers and business owners alike by creating a dedicated gTLD to specifically serve the Community of Registered Corporations. Through our registry service, we will foster consumer peace of mind with confidence by ensuring that all domains bearing our gTLD string are members of the Registered Community of Corporations. Our verification process will create an unprecedented level of security for online consumers by authenticating each of our registrant's right to conduct business in the United States. The ".INC" gTLD will fill a unique void in the current DNS and assist in decreasing the burden on existing domain names by identifying members of the Registered Community of Corporations.

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

With the increased popularity of the Internet as a consumer marketplace and the ease with which individuals are able to access information online, it is essential that safeguards be put in place to validate and identify legitimate businesses.
Businesses representing themselves as corporations by including Inc., Incorporated or Corporation in their business names create an expectation amongst consumers that they have the legal right to conduct business as a corporation. Unfortunately, consumers are currently unable to quickly verify the accuracy of this representation. Fraudulent business entities rely on this consumer assumption and the lack of available verification resources to prey on both businesses and consumers. As online commerce replaces brick-and-mortar businesses, there has been a corresponding rise in business identity theft online, which in turn creates a lack of consumer confidence.
In the vast majority of states, the Secretary of State is responsible for overseeing the business entities in the state – from the registration of corporations or verification of business filings, to the administration of the Uniform Commercial Code, an act, which provides for the uniform application of business contracts and practices across the United States. The Secretaries' role is critical to the chartering of businesses (including, but not limited to the formation of corporations) that wish to operate in their state. In this regard, the Secretaries of State maintain all records of business activities within the state, and in some states, the Secretary of State has wide-ranging regulatory authority over businesses as well.
The ".INC" gTLD will be exclusively available to members of the Community of Registered Corporations, as verified through the records of each registrant's Secretary of State's Office (or other state official where applicable). By verifying that a registrant is a registered U.S. corporation, DOT Registry will be able to bring unprecedented clarity and security to consumers and business owners, assuring Internet users, registry applicants, and others that web addresses ending in ".INC" are a hallmark of a valid corporation recognized by a governmental authority of the United States. This process will decrease the possibility of identity misrepresentation in a cyber setting and assist lesser-known businesses in legitimizing their services to consumers.
In January 2012, after many public forums and contributions from consumer advocates, the Business Services Committee of the National Association of Secretaries of State (NASS) released the NASS White Paper on Business Identity Theft, indicating that at least 26 states have reported business identity theft cases resulting from fraudulent business representations online. North Carolina Secretary of State Elaine Marshall, who serves as Co-Chair of the NASS Business Services Committee, indicates that the primary function of the White Paper is to "Harness new technology to develop cost-effective solutions, and ultimately make it harder for identity thieves to prey upon state-based businesses."
With the implementation of the ".INC" gTLD, consumers would have the ability to quickly

identify the presented business as a valid U.S. corporation. As ".INC" registrations grow, we will see a reduction in the ease with which criminals are able to hide behind fictitious entities because consumers will be conditioned to look for the appropriate gTLD ending before conducting business online. This simple gTLD extension would provide an efficient and cost-effective solution to a growing economic concern in the United States by creating a verifiable online business community network. Through this innovative concept, the DNS system will help to build a stronger more resilient business platform for members of the Registered Community of Corporations, while fostering increased user confidence, by ensuring accurate business representation.

It is our goal to provide an efficient and secure application process by minimizing the input required by the registrant and creating a streamlined, efficient evaluation process. We will accomplish this by reviewing the applicant's proof of business registration with their State. Registry Applicants will only be awarded a domain through DOT Registry if the Registrant is an active member of the Community of Registered Corporations. "Active" in this context can be defined as any corporation registered with a Secretary of State in the United States and its territories, that is determined to be authorized to conduct business within that State at the time of their registration. Registrant's "Active" status will be verified on an annual basis to ensure the reputation and validity of the ".INC" gTLD.

DOT Registry will also ensure that registrants are represented by a web address that is both simple and intuitive allowing for easy recognition by search engines and internet users. Awarded addresses will identify the registrant's company and may be presented in the shortest, most memorable way.

At DOT Registry, we believe in complete transparency, consistent with the Secretaries of State Policy with regard to "Active" members of the Community of Registered Corporations becoming publicly recorded upon completion of their entity registration process. Further, DOT Registry is informed by the position of the United States Senate Task Force for Financial Integrity and Economic Development, which was created to advocate for improved levels of transparency and accountability with regard to beneficial ownership, control, and accounts of companies. Over the last decade the Task Force has focused specifically on combatting fraudulent business registrations which result in "fake" entities absorbing, hiding, and transferring wealth outside the reach of law enforcement agencies. Because of this DOT Registry will not allow private or proxy registrations.

All approved domain registrants will be made public and available, so as to further validate DOT Registry's mission of fostering consumer peace of mind by creating a gTLD string dedicated solely to valid members of the Community of Registered Corporations. These transparency mechanisms will also serve as a deterrent for fraudulent entities by creating an expectation among consumers as to who they are conducting business with.

The social implications of business identity theft and consumer confusion are a paramount concern to DOT Registry. In our currently unstable economy, stimulating economic growth is vital. One means to such growth is by defusing the rampant, legitimate fear caused by online crimes and abuse, which leads to curtailed consumer behavior. By introducing the ".INC" domain into the DNS, DOT Registry will attempt to reduce the social impact of identity theft on business owners which will in turn reduce consumer fears related to spending and ultimately boost economic growth in regards to consumption and purchase power. Further, the ".INC" gTLD will strive to foster competition by presenting members of the Community of Registered Corporations with a highly valued customized domain name that not only represents their business, but also their validity in the marketplace. Within the current existing top-level domains it is hard for businesses to find naming options that appropriately represent them. One advantage of the ".INC" gTLD is that it will drive the "right" kind of online registrations by offering a valued alternative to the currently overcrowded and often unrestricted name space. Registrants will be inspired to pursue ".INC" domains not only because they will be guaranteed a name representative to their business, but also because of the increased validity for their business operations brought about by the ".INC" verification process. DOT Registry anticipates that the security offered through a ".INC" extension will increase consumer traffic to websites which in turn will boost advertising revenue online and consumer purchasing.

Successful implementation of the ".INC" domain will require two registration goals: (1)

capture newly formed corporations and assist them in securing a ".INC" domain relative to their legal business name, and (2) converting existing online members of our community to a ".INC" domain relative to their legal business name. These goals will be accomplished by the following practices:

1) Through our Founder's Program, DOT Registry will secure key community tenants in the name space who will act as innovative leaders to assist us in changing the online culture of business representation by promoting the benefits of the ".INC" gTLD and shaping economic growth through increased consumer confidence.

2) DOT Registry will work closely with companies such as Legalzoom and CSC (both companies assist in the formation of entities and their registration processes), as well as individual Secretary of State's offices, to capture newly admitted members of the community.

3) DOT Registry will educate members of the Community of Registered Corporations on the benefits and importance of using a ".INC" gTLD by building a strong relationship with organizations like the Small Business Administration and the Better Business Bureau, which promote business validation and consumer insight. By working closely with these well-known and highly regarded entities, DOT Registry will be able to reach a larger majority of community members and enhance our message's validity.

4) DOT Registry will strive to create consumer and Internet user awareness through a strong Internet marketing presence and by developing a relationship with the National Association of Consumer Advocates, which was formed with the intention of curbing consumer abuse through predatory business practices.

At DOT Registry, we strive to meet the exact needs of our registrants and the Internet users who patronize them. This will be accomplished by the creation of a seamless connection and strong communication channel between our organization and the governmental authority charged with monitoring the creation and good standing of corporations. DOT Registry will work closely with each Secretary of State's office to tailor our validation process to complement each office's current information systems and to maximize the benefits of accurate information reporting. These processes are essential in fully assisting consumers in making educated decisions in regards to what businesses to patronize. The reach of the ".INC" gTLD will not only impact online consumerism, but also offer an additional validation process for consumers to research contractors, businesses, and solicitors before choosing to do business with them in person.

The guidelines listed below were developed through collaborations with both NASS and individual Secretary of State's offices in order to ensure the integrity of the ".INC" domain. All policies comply with ICANN-developed consensus policies.

To maintain the integrity of our mission statement and our relationship with each Secretary of State's office we will implement Registration Guidelines. In order to apply for a domain name ending in ".INC", a Registrant must be registered with one of the Secretary of State's offices in the United States, the District of Columbia, or any of the U.S. possessions or territories as a corporation pursuant to that jurisdiction's laws on valid corporate registration. In addition, Applicant will implement the following Registration Guidelines and naming conventions:

1) A Registrant will only be awarded the ".INC" domain that matches or includes a substantial part of the Registrant's legal name. For example, Blue Star Partners, Inc. would be able to purchase either BlueStarPartners.INC or BlueStar.INC.

2) Registrants will not be allowed to register product line registrations, regardless of the products affiliation to the corporation. All awarded domains must match or include a substantial part of the Registrant's legal name.

3) If there are registrants applying for the same domain names, which correspond to their legal business names as registered in different states, then the ".INC" domain will be awarded on a first-come, first-served basis to the first registrant.

4) However, if a registrant has a trademark registered with the United States Patent and Trademark Office (USPTO), then such registrant will have priority over any other registrant to be awarded the applied for ".INC" domain.

5) If a registrant's ".INC" domain has already been awarded to another registrant with the same or similar legal name, then DOT Registry will offer to award such registrant a

".INC" domain with a distinctive denominator including but not limited to a tag, company describer, or name abbreviation. For example, if BlueStar.INC was awarded to Blue Star Partners, Inc. of California, then Blue Star Partners, Inc. of Kansas would be offered the opportunity to use BlueStarPartners.INC.

6) DOT Registry will work closely with the Secretary of State's Offices throughout the United States, with NASS and with a number of other agencies and organizations in maintaining the integrity and security of its domain names. DOT Registry will utilize the Secretary of States' online resources to confirm that companies applying for their ".INC" domain are in fact registered businesses.

7) All registrants that are awarded the ".INC" domain will agree to a one-year minimum contract for their domain names that will automatically renew for an additional year on an annual basis if such contract is not terminated prior to the expiration of the renewal date.

8) DOT Registry or it's designated agent will annually verify each registrants community status. Verification will occur in a process similar to the original registration process for each registrant, in which the registrars will verify each registrant's "Active" Status with the applicable state authority. Each registrar will evaluate whether its registrants can still be considered "Active" members of the Community of Registered Corporations. In this regard, the following items would be considered violations of DOT Registry's Registration Guidelines, and may result in dissolution of a registrant's awarded ".INC" domain:

(a) If a registrant previously awarded the ".INC" domain ceases to be registered with the State.

(b) If a registrant previously awarded a ".INC" domain is dissolved and⁄or forfeits the domain for any reason.

(c) If a registrant previously awarded the ".INC" domain is administratively dissolved by the State.

Any registrant is found to be "Inactive," or which falls into scenarios (a) through (c) above, they will be issued a probationary warning by their registrar, allowing for the registrant to restore its active status or resolve its dissolution with its applicable Secretary of State's office. If the registrant is unable to restore itself to "Active" status within the defined 30 day probationary period, their previously assigned ".INC" will be forfeited. DOT Registry reserves the right to change the definition of "Active" in accordance with the policies of the Secretaries of State. Domains will be temporarily suspended during the review process.

9) If DOT Registry discovers that a registrant wrongfully applied for and was awarded a ".INC" domain, then such ".INC" will be immediately forfeited to DOT Registry. Wrongful application includes but is not limited to: a registrant misrepresenting itself as a member of the Community of Registered Corporations, a registrant participating in illegal or fraudulent actions, or where a registrant would be in violation of our abuse policies described in Question 28 (including promoting or facilitating spam, trademark or copyright infringement, phishing, pharming, willful distribution of malware, fast flux hosting, botnet command and control, distribution of pornography, illegal access to other computers or networks, and domain kiting⁄tasting).

10) In the case of domain forfeiture due to any of the above described options, all payments received by the Registrant for registration services to date or in advance payment will be non-refundable.

11) All registration information will be made publicly available. DOT Registry will not accept blind registration or registration by proxy. DOT Registry'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 Registry will provide a Web-based WHOIS application, which will be located at www.whois.inc. 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.

12) Awarded names are non-transferrable to entities outside of the designated community, regardless of affiliation to any member of the community. In the event that a registrant's business entity merges, is acquired, or sold, the new entity will be allowed

to maintain the previously awarded ".INC" domain until the domain renewal date, at which point they will be evaluated as described in number seven (7) above. Further, any entity acquiring a ".INC" domain through the processes described in this guideline that does not meet the registration criteria and wishes to maintain the awarded domain will be allowed a grace period after the renewal verification process to correct any non-compliance issues in order to continue operating their acquired domain. If the said entity is unable to comply with DOT Registry's guidelines, the awarded domain will be revoked.
13) If an application is unable to be verified or does not meet the requirements of the sponsored community, the application will be considered invalid.
14) DOT Registry will implement a reserved names policy consisting of both names DOT Registry wishes to reserve for our own purposes as the registry operator and names protected by ICANN. DOT Regisgtry will respect all ICANN reserved names including, but not limited to, two letter country codes and existing TLD's. Additionally, DOT Registry 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.

In addition to DOT Registry's comprehensive eligibility, verification, and policing mechanisms, DOT Registry will implement a series of Rights Protection Mechanisms (RPM), including 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; and stringent take down policies and all required dispute resolution policies.

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

".INC" was proposed for the sole purpose of eliminating business and consumer vulnerability in a cyber setting. In order to maintain the integrity of that mission and minimize the negative consequences to consumers and business owners, the following policies will be adhered to:
(a) No information collected from any registrant 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 correct data inaccuracies as needed.
(e) All data will be kept secure.
DOT Registry will strictly uphold the rules set forth in their registration guidelines in order to accurately service the Community of Registered Corporations and mitigate any negative consequences to consumers or Internet users.
Price structures for the ".INC" gTLD are designed to reflect the cost of verification within our community requirements and the ongoing cost of operations. Price escalation will only occur to accommodate rising business costs or fees implemented by the Secretaries of State with regard to verifying the "Active" status of a Registrant. Any price increases would be submitted to ICANN as required in our Registry Agreement and will be compiled in a thoughtful and responsible manner, in order to best reduce the affects on both the registrants and the overall retail market.
DOT Registry 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 Registry 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. DOT Registry shall provide additional financial incentives to it's Registrars for pre-authentication of Registrant data prior to such data being passed to the registry. DOT Registry will provide for lower renewal and bulk registration fees in its RRAs for registrations which have been pre-authenticated and which DOT Registry can rely on as accurate data to be entered into its WhoIs database.

Additionally, DOT Registry , through our founders program will provide a 25% discount to founders participants as a participation incentive. It is possible that DOT Registry 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?

Yes

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

DOT Registry plans to serve the Community of Registered Corporations. Members of the community are defined as businesses registered as corporations within the United States or its territories. This would include Corporations, Incorporated Businesses, Benefit Corporations, Mutual Benefit Corporations and Non-Profit Corporations. Corporations or "INC's" as they are commonly abbreviated, represent one of the most complex business entity structures in the U.S. Corporations commonly participate in acts of commerce, public services, and product creation.
Corporations are the oldest form of organized business in the United States, with the first organized corporation dating back to the 18th century. In 1819 The US Supreme Court formalized their policy on corporation formation by enhancing the rights granted to US Corporations. This policy change for the United States spurred increased corporate registrations and acted as an early economic boom for the states. Well known early corporations included the British East India Company, Carnegie Steel Company, and Standard Oil. The creation of corporations is synonymous with the development of free enterprise in the United States and much of our countries infrastructure and services were created by early and innovative corporations.
Corporation creation has been viewed as especially unique throughout US history because corporations are considered the only business model that are recognized by law to have the rights and responsibilities similar to natural persons. Corporations can exercise human rights against real individuals and the state. Additionally, they themselves can be responsible for human rights violations. This unique human element makes corporations

acutely responsible for their actions as an entity. This feature becomes especially applicable when we begin to view corporations as a community. “Community” is defined by Merriam Webster’s dictionary as a group sharing common characteristics or interests and perceived or perceiving itself as distinct in some respect from the larger society within which it exists. DOT Registry believes that corporations fall well within this definition due to their specific registration requirements, which set them apart from individuals and other business entities, while granting them operating privileges and distinct rights and responsibilities.

A corporation is defined as a business created under the laws of a State as a separate legal entity, that has privileges and liabilities that are distinct from those of its members. While corporate law varies in different jurisdictions, there are four characteristics of the business corporation that remain consistent: legal personality, limited liability, transferable shares, and centralized management under a board structure. Corporate statutes typically empower corporations to own property, sign binding contracts, and pay taxes in a capacity separate from that of its shareholders.

Business formation favors the corporate entity structure because it provides its shareholders with limited personal liability and a unique taxing structure.

Corporations provide the backbone of the American business culture. Fortune 500’s top ten US corporations for 2011 include: Wal-Mart Stores, Exxon Mobil, Chevron, ConocoPhillips, Fannie Mae, General Electric, Berkshire Hathaway, General Motors, Bank of America and Ford Motors. From this listing one can ascertain that corporations span every genre of business and play an intricate role in the daily lives of consumers. From gas stations to hospitals, grocery stores to financial lending institutions corporations drive the stock market, industry production, and consumer spending.

With almost 470,000 new corporations registered in the United States in 2010 (as reported by the International Association of Commercial Administrators) resulting in over 8,000,000 total corporations in the US, it is hard for the average consumer to not conduct business with a corporation.

Corporations can be formed through any jurisdiction of the United States. Therefore members of this community exist in all 50 US states and its territories. Corporation formation guidelines are dictated by state law and can vary based on each State’s regulations. Persons form a corporation by filing required documents with the appropriate state authority, usually the Secretary of State. Most states require the filing of Articles of Incorporation. These are considered public documents and are similar to articles of organization, which establish a limited liability company as a legal entity. At minimum, the Articles of Incorporation give a brief description of proposed business activities, shareholders, stock issued and the registered business address.

Corporations are expected to conduct business in conjunction with the policies of the State in which they are formed, and the Secretary of State periodically evaluates a corporation’s level of good standing based on their commercial interactions with both the state and consumers. DOT Registry or its designated agents would verify membership to the Community of Corporations by collecting data on each Registrant and cross-referencing the information with their applicable registration state. In order to maintain the reputation of the “.INC” string and accurately delineate the member to consumers, Registrants would only be awarded a domain that accurately represents their registered legal business name. Additionally, DOT Registry will not allow blind registrations or registration by proxy, therefore DOT Registry’s WHOIS service will tie directly back to each member’s state registration information and will be publicly available in order to provide complete transparency for consumers.

Over 64% of US public corporations are registered in the state of Delaware. Because of this preeminence, Dot Registry has drawn on Delaware Law as an example of formation requirements and operating privileges.

According to Delaware Law corporations may be formed by:

(a) Any person, partnership, association or corporation, singly or jointly with others, and without regard to such person’s or entity’s residence, domicile or state of incorporation, may incorporate or organize a corporation under this chapter by filing with the Division of Corporations in the Department of State a certificate of incorporation

which shall be executed, acknowledged and filed in accordance with this title.
(b) A corporation may be incorporated or organized under this chapter to conduct or promote any lawful business or purposes, except as may otherwise be provided by the Constitution or other law of this State.
Entities are required to comply with formation practices in order to receive the right to conduct business in the US. Once formed a corporation must be properly maintained. Corporations are expected to comply with state regulations, submit annual filings, and pay specific taxes and fees. Should a corporation fail to comply with state statutes it could result in involuntary dissolution by the state in addition to imposed penalties, taxes and fees.
All entities bearing the words Corporation or Incorporated in their business name create the assumption that they have been awarded the privileges associated to that title such as: the ability to conduct commerce transactions within US borders or territories, the ability to market products, solicit consumers and provide reputable services in exchange for monetary values, and finally to provide jobs or employment incentives to other citizens. Membership in the Community of Corporations is established through your business entity registration. In order to maintain your membership to this community you must remain an "Active" member of the community. Active" in this context can be defined as any corporation registered with a Secretary of State in the United States and its territories, that is determined to be authorized to conduct business within that State.

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

DOT Registry, LLC is owned solely by ECYBER Solutions Group, Inc., a registered Corporation in the State of Kansas. DOT Registry has a direct relationship to the proposed community because of our ownership makeup. In addition, DOT Registry is a corporate affiliate of the National Association of Secretaries of State (NASS), an organization which acts as a medium for the exchange of information between states and fosters cooperation in the development of public policy, and is working to develop individual relationships with each Secretary of State's office in order to ensure our continued commitment to honor and respect the authorities of each state.
DOT Registry is acutely aware of our responsibility to uphold our mission statement of: building confidence, trust, reliance, and loyalty for consumers and business owners alike by creating a dedicated gTLD to specifically serve the Community of Corporations.DOT Registry has also specifically pledged to various Secretaries of State to responsibly manage this gTLD in a manner that will both protect and promote business development in the US. Further our policies were developed through direct collaboration with the state offices so as to mitigate any possibility of misrepresenting their regulations.
In order to ensure that we accomplish this goal and preserve the credibility of our operations DOT Registry has taken the following advance actions to ensure compliance and community protection:
1) Developed registration policies that are currently reflective of common state law dictating the creation and retention of corporations in the United States.
2) Created a strong partnership with CSC (an ICANN approved registrar also specializing in corporate formation services). Through this partnership DOT Registry was able to develop a streamlined verification process to validate potential Registrants as members of the community and ensure that continued annual verifications are completed in a time sensitive and efficient manner. This process will ensure that consumers are not misled by domains registered with the ".INC" gTLD. Additionally, this process will create peace of mind amongst community members by ensuring that their integrity is not diminished by falsely identified corporations being represented by a ".INC" extension.
3) Built a strong relationship with several Secretaries of State in order to receive and give consistent input on policy implementation and state regulation updates. DOT Registry has also notified NASS that we have designed our registration policies and

procedures to address NASS' concerns about verification requirements in the TLD.
4) Established an in-house legal and policy director to review, enhance, and ensure compliance and consistency with all registration guidelines and community representations.
As indicated in many of the attached letters, DOT Registry will be held specifically accountable for protecting the integrity of its restrictions and of the members of this community. DOT Registry will consult directly with NASS and policy advisors in the state offices consistently in order to continue to accurately represent the Community of Corporations and live up to the vast standards associated to the ".INC" gTLD.
In furtherance of this goal, DOT Registry has attached letters from critical advocates for and representatives of the proposed community, including:
1) Various Secretary of States Offices: Specifically The Secretary of State of Delaware which represents over 55% of public corporations in the United States and a majority of members in this community and The Secretary of State of South Dakota, which is working towards combatting business identity theft and fictitious business registration.
2) Members of the community including but not limited to CSC our registrar partner and Legal Zoom, the nation's leading provider for online business registration.
DOT Registry can be viewed as an exemplary community representative not only through its pledged commitment to excellence, but also through its continued commitment to build relationships with the state offices charged with registering and overseeing members of this community. DOT Registry pledges through its registry policies to uphold a common standard of evaluation for all applicants and to add increased integrity to the Community of Registered Corporations. These pledges are further enforced by the endorsement letters from the above organizations, which call the authentication/verification measures proposed by DOT Registry critical to the success of the proposed community.
Similarly, DOT Registry will adhere to all standards of business operations as described in the Kansas state business statutes and will be equally accountable to consumers to deliver continuously accurate findings and valid registrations.

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

The goal of the ".INC" gTLD is to build confidence, trust, reliance, and loyalty for consumers and business owners alike by creating a dedicated gTLD to specifically serve the Community of Corporations. Through our registry service, we will foster consumer peace of mind with confidence by ensuring that all domains bearing our gTLD string are members of the Community of Corporations. Our verification process will create an unprecedented level of security for online consumers by authenticating each of our registrant's right to conduct business in the United States. The ".INC" gTLD will fill a unique void in the current DNS and assist in decreasing the burden on existing domain names by identifying members of the Registered Community of Corporations. The creation of the ".INC" gTLD will bring innovation and unprecedented coordination of this valuable service of verification, a purpose endorsed by many individual Secretary of States and NASS. Additionally, ".lNC" will further promote the importance of accurate business registrations in the US, while assisting in combatting business identity theft by increasing registration visibility through our WHOIS services and strict abuse policies.
The intended registrants of the ".INC" gTLD would consist of members of the Community of Corporations. This would be verified by collecting data on each Registrant and cross-referencing the information with their applicable registration state. In order to ensure that this process is accomplished in a secure and time effective manner DOT Registry will develop partnerships with each Secretary of State's office in order to create the applicable applications to securely verify registrant data.
End-users for this TLD would include everyday consumers, members of the community, businesses without the community, and consumers looking for more accurate information with

regards to those with whom they may conduct business. DOT Registry plans to initiate a robust marketing campaign geared towards the proposed end-users in order to ensure that consumers are aware of what ".INC" stands for and its significance throughout the Community of Corporations. In addition to the vast consumer benefits from the creation of the ".INC" gTLD, DOT Registry believes that ".INC" domains would be considerably beneficial to business end users. Since DOT Registry will not allow blind registration or registration by proxy businesses viewing ".INC" sites would be able to instantly ascertain what businesses operate under the blanket of parent companies, are subsidiaries of other businesses, and of course where a corporation is domiciled. This easily identifiable information not only assists businesses in accurately identifying who they are doing business with, it would also assist in locating sales and use tax information, identifying applicable state records, and tracking an entity's history. These factors could help to determine the outcome of sales, mergers, contract negotiations, and business relationships. Ensuring that this kind of transparency and accountability – qualitities previously not attainable in a TLD – shall be at the fingertips of potential business partners or investors.
Our registry policies will be adapted to match any changing state statutes in relation to the definition and creation of corporations in the U.S., ensuring the longevity and reputation of our registry services and our commitment to consumers to only represent valid U.S. corporations. Much like the perpetuity of the members of the Community of Corporations, the ".INC" gTLD will enjoy a similar immortality, for as long as incorporated entities continue to exist in the United States the ".INC" relevance will not diminish. As awareness of the gTLD's mission becomes more widely recognized by end-users expectations to understand who you choose to do business with will increase, making the need for the ".INC" gTLD more prominent.
In addition, it is our concern that the implementation of the gTLD string ".INC" as a generic string, without the restrictions and community delineations described in this application and endorsed by NASS and the various Secretaries of State, could promote confusion among consumers and provide clever criminal enthusiasts the tools necessary to misrepresent themselves as a U.S.-based corporation. There is an expectation amongst consumers that entities using the words corporation, incorporated, or INC in their business name have the legal right and ability to conduct business in the United States. This representation by non-members of the Community of Registered Corporations is not only fraudulent, but a great disservice to consumers

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

".INC" was chosen as our gTLD string because it is the commonly used abbreviation for the entity type that makes up the membership of our community. In the English language the word incorporation is primarily shortened to Inc. when used to delineate business entity types. For example, McMillion Incorporated would additionally be referred to as McMillion Inc. Since all of our community members are incorporated businesses we believed that ".INC" would be the simplest, most straightforward way to accurately represent our community. Inc. is a recognized abbreviation in all 50 states and US Territories denoting the corporate status of an entity. Our research indicates that Inc. as corporate identifier is used in three other jurisdictions (Canada, Australia, and the Philippines) though their formation regulations are different from the United States and their entity designations would not fall within the boundaries of our community definition.

20(e). Provide a description of the applicant's intended registration policies in

support of the community-based purpose of the applied-for gTLD.

In order to accurately protect the integrity of our domain name and serve the proposed community the following safeguards will be adapted:

1)All Registrants will be required to submit a minimum of: Their registered business address, State of Incorporation, name and contact information of responsible party, and legally registered business name. DOT Registry or its agents will use this information to cross-reference the applicable state's registration records in order to verify the accuracy of the Registrant's application. Should DOT Registry be unable to verify the legitimacy of the Registrants application additional information might be requested in order to award a domain name.
2)A Registrant will only be awarded the ".INC" domain that matches or includes a substantial part of the Registrant's legal name. For example, Blue Star Partners, Inc. would be able to purchase either BlueStarPartners.INC or BlueStar.INC.
3)Registrants will not be allowed to register product line registrations, regardless of the product's affiliation to the corporation. All awarded domains must match or include a substantial part of the Registrant's legal name.
4)If there are registrants applying for the same domain names, which correspond to their legal business names as registered in different states, then the ".INC" domain will be awarded on a first-come, first-served basis to the first registrant.
5)However, if a registrant has a trademark registered with the United States Patent and Trademark Office (USPTO), then such registrant will have priority over any other registrant to be awarded the applied for ".INC" domain.
6)If a registrant's ".INC" domain has already been awarded to another registrant with the same or similar legal name, then DOT Registry will offer to award such registrant a ".INC" domain with a distinctive denominator including but not limited to a geographic tag, company describer, or name abbreviation. For example, if BlueStar.INC was awarded to Blue Star, Inc. of California, then Blue Star, Inc. of Kansas would be offered the opportunity to use BlueStar-KS.INC. Companies will be able to choose a geographic tag that either matches their State of Incorporation or their principal place of business, which is listed with their applicable Secretary of State's office or legally reciprocal jurisdiction.
7)DOT Registry will work closely with the Secretary of State's Offices throughout the United States, with NASS and with a number of other agencies and organizations in maintaining the integrity and security of its domain names. DOT Registry will utilize the Secretary of States' online resources to confirm that companies applying for their ".INC" domain are in fact registered businesses.
8)DOT Registry or its designated agent will annually verify each registrants community status. Verification will occur in a process similar to the original registration process for each registrant, in which the registrars will verify each registrant's "Active" Status with the applicable state authority. Each registrar will evaluate whether its registrants can still be considered "Active" members of the Community of Registered Corporations. In this regard, the following items would be considered violations of DOT Registry's Registration Guidelines, and may result in dissolution of a registrant's awarded ".INC" domain:
(a)If a registrant previously awarded the ".INC" domain ceases to be registered with the State.
(b)If a registrant previously awarded a ".INC" domain is dissolved and⁄or forfeits the domain for any reason.
(c)If a registrant previously awarded the ".INC" domain is administratively dissolved by the State.
Any registrant found to be "Inactive," or which falls into scenarios (a) through (c) above, will be issued a probationary warning by their registrar, allowing for the registrant to restore its active status or resolve its dissolution with its applicable Secretary of State's office. If the registrant is unable to restore itself to "Active" status within the defined 30 day probationary period their previously assigned ".INC" will be forfeited.

DOT Registry reserves the right to change the definition of “Active” in accordance with the policies of the Secretaries of State.
9)If DOT Registry discovers that a registrant wrongfully applied for and was awarded a “.INC” domain, then such “.INC” will be immediately forfeited to DOT Registry. Wrongful application includes but is not limited to: a registrant misrepresenting itself as a member of the Community of Registered Corporations, a registrant participating in illegal or fraudulent actions, or where a registrant would be in violation of our abuse policies described in Question 28 (including promoting or facilitating spam, trademark or copyright infringement, phishing, pharming, willful distribution of malware, fast flux hosting, botnet command and control, distribution of pornography, illegal access to other computers or networks, and domain kiting⁄tasting).
10)All registration information will be made publicly available. DOT Registry will not accept blind registration or registration by proxy. DOT Registry’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 Registry will provide a Web-based WHOIS application, which will be located at www.whois.inc. The WHOIS Web application will be an intuitive and easy to use application which will allow the general public to easily access registration information for each “.INC” site. A complete description of these services can be found in Question 26 below.
11)Awarded names are non-transferrable to entities outside of the designated community, regardless of affiliation to any member of the community. In the event that a registrant’s business entity merges, is acquired, or sold, the new entity will be allowed to maintain the previously awarded “.INC” domain until the domain renewal date, at which point they will be evaluated as described in number seven (7) above. Further, any entity acquiring a “.INC” domain through the processes described in this guideline that does not meet the registration criteria and wishes to maintain the awarded domain will be allowed a 30 day grace period after the renewal verification process to correct any non-compliance issues in order to continue operating their acquired domain. If the said entity is unable to comply with DOT Registry’s guidelines, the awarded domain will be revoked.
12)If an application is unable to be verified or does not meet the requirements of the sponsored community, the application will be considered invalid.In addition to Applicant’s comprehensive eligibility, verification, and policing mechanisms, DOT Registry will implement a series of Rights Protection Mechanisms (RPM), including 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 policies in order to properly operate the registry; and Applicant shall comply with any RRDRP decision, further reinforcing the fact that Applicant is committed to acting in best interest of the community.DOT Registry will employ an in house Rights Protection Mechanism Team consisting of our Director of Legal and Policy and two additional support personnel. The RPM team will work to mitigate any RPM complaints, while protecting the general rights and integrity of the “,INC” gTLD. The RPM team will strictly enforce the rights protection mechanisms described in this application.
Membership verification will be performed via DOT Registry’s designated agents that which have software systems in place to efficiently interface with each state’s data records. By utilizing the resources of industry leaders in this field, DOT Registry will ensure accurate and timely verification in addition to our ability to meet the needs of such a vast community. “Active” status will be specifically verified by cross referencing an applicant’s registration data with state records. If this process is unable to be automated at any given time DOT Registry’s agents will manually verify the information by contacting the applicable state agencies. While manual verification will obviously employ a larger pool of resources, DOT Registry believes that its industry partners are sufficiently able to accomplish this task based on their employee pool and past business accomplishments. Registrants will be expected to provide a minimum of their legal registered name, state of incorporation, registered business address, and administrative contact. All additional

information required such as proof of incorporation or “active” status verification will be the sole responsibility of DOT Registry or its designated agents and will be acquired through the processes described herein.
DOT Registry will not restrict the content of “.INC” sites other then through the enforcement of our Abuse Mitigation practices or Rights Protection Mechanisms as described in question 28 and 29 of this application. All “.INC” sites will be expected to adhere to the content restrictions described in DOT Registry’s abuse policies. Any sites infringing on the legal rights of other individuals or companies, trademarks, or participating in the practice and promotion of illegal activities will be subject to Applicant’s take down procedures. “.INC” domains are designed for the sole use of community members with the intention of promoting their specific business activities.

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.

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

-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 ".INC" 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 Registry 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 ".INC". 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 Registry 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 ".INC" 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 Registry, 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 Registry will not be offering services that are unique to ".INC".

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 Registry has partnered with NeuStar, Inc ("Neustar"), an experienced TLD registry operator, for the operation of the ".INC" 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 ".INC" 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 Registry is mitigating the significant risks and costs associated with the development of a new system. Highlights of the SRS include:

-State-of-the-art, production proven multi-layer design

-Ability to rapidly and easily scale from low to high volume as a TLD grows

-Fully redundant architecture at two sites

-Support for IDN registrations in compliance with all standards

-Use by over 300 Registrars

-EPP connectivity over IPv6

-Performance being measured using 100% of all production transactions (not sampling).

24.2.2 SRS Systems, Software, Hardware, and Interoperability

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

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

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

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

-The IP address of the client

-Timestamp

-Transaction Details

-Processing Time.

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

24.2.3 SRS Design

The SRS incorporates a multi-layer architecture that is designed to mitigate risks and easily scale as volumes increase. The three layers of the SRS are:

-Protocol Layer

-Business Policy Layer

-Database.

Each of the layers is described below.

24.2.4 Protocol Layer

The first layer is the protocol layer, which includes the EPP interface to registrars. It consists of a high availability farm of load-balanced EPP servers. The servers are designed to be fast processors of transactions. The servers perform basic validations and then feed information to the business policy engines as described below. The protocol layer is horizontally scalable as dictated by volume.

The EPP servers authenticate against a series of security controls before granting service, as follows:

-The registrar’s host exchanges keys to initiates a TLS handshake session with the EPP server.

-The registrar’s host must provide credentials to determine proper access levels.

-The registrar’s IP address must be preregistered in the network firewalls and traffic-shapers.

24.2.5 Business Policy Layer

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

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

be scaled up or down as demand changes.

The SRS today processes over 30 million EPP transactions daily.

24.2.6 Database

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

Figure 24-1 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 ".INC" 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 ".INC".

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 ".INC" 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 ".INC" 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 ".INC" 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 ".INC" registry.

25. Extensible Provisioning Protocol (EPP)

25.1 Introduction

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

26. Whois

DOT Registry, 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 Registry, 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 Registry, 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 Registry, LLC's WHOIS services will include:

- Fully compliant with all relevant RFCs including 3912;
- Production proven, highly flexible, and scalable (DOT Registry, 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 Registry, 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 Registry, 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 Registry, LLC's registry services operator currently processes millions of WHOIS queries per day.

In addition to the WHOIS Service on port 43, DOT Registry, LLC will provide a Web-based WHOIS application, which will be located at www.whois.inc. 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 Registry, 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 Registry, 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 Registry, 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 Registry, 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 Registry, LLC's information, DOT Registry, 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

".INC" 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 ".INC".

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 ".INC" registry per the defined ".INC" 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 ".INC" 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 ".INC" 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 ".INC" registry.

-Hold Removes the domain from the DNS zone.

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

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

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

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

The lifecycle of a domain begins with the registration of the domain. All registrations must follow the EPP standard, as well as the specific business rules described in the response to Question 18 above. Upon registration a domain will either be in an active or inactive state. Domains in an active state are delegated and have their delegation information published to the zone. Inactive domains either have no delegation information or their delegation information in not published in the zone. Following the initial registration of a domain, one of five actions may occur during its lifecycle:

-Domain may be updated

-Domain may be deleted, either within or after the add-grace period

-Domain may be renewed at anytime during the term

-Domain may be auto-renewed by the Registry

-Domain may be transferred to another registrar.

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

27.2 Registration States

27.2.1 Domain Lifecycle Registration States

As described above the ".INC" 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 serverTranferProhibited status. This will cause the transfer request to fail.The domain goes back to its original state.

-DeleteProhibited: The domain is in clientDeleteProhibited and/or serverDeleteProhibited status.This will cause the delete command to fail.The domain goes back to its original state.

Note: the locked state is not represented as a distinct state on the diagram as a domain may be in a locked state in combination with any of the other states: inactive, active, pending transfer, or pending delete.

27.5.1 EPP RFC Consistency

As described above, the domain lifecycle is determined by ICANN policy and the EPP RFCs. Neustar has been operating ICANN TLDs for the past 10 years consistent and compliant with all the ICANN policies and related EPP RFCs.

27.6 Resources

The registration lifecycle and associated business rules are largely determined by policy and business requirements; as such the Product Management and Policy teams will play a critical role in working Applicant to determine the precise rules that meet the requirements of the TLD. Implementation of the lifecycle rules will be the responsibility of Development/Engineering team, with testing performed by the Quality Assurance team.Neustar's SRS implementation is very flexible and configurable, and in many case development is not required to support business rule changes.

The ".INC" 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 ".INC" registry.

28. Abuse Prevention and Mitigation

General Statement of Policy

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

Anti-Abuse Policy

DOT Registry 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 Registry with broad power to suspend, cancel, or transfer domain names that violate the Abuse Policy. DOT Registry will publish the Abuse Policy on its home website at NIC.INC and clearly provide DOT Registry'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 Registry 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 Registry'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 Registry will catalog all abuse communications in its CRM software using a ticketing system that maintains records of all abuse complaints indefinitely. Moreover, DOT Registry 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 Registry reserves the right to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary to ; (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 Registry, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) to correct mistakes made by the DOT Registry, 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 Registry'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 Registry will take great care to ensure that trademark and copyright infringement does not occur within the .INC TLD. DOT Registry 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 Registry;
- 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 Registry 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 Registry will provide a domain name anti-abuse procedure modeled after the DMCA's notice-and-takedown procedure.

At all times, DOT Registry will publish on its home website at NIC.INC 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 Registry's Legal Time who will review and if

applicable remedy any Complaint regarding an alleged violation of the Abuse Policy. DOT Registry 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 Registry's CRM software and relayed to DOT Registry's Abuse Team. A member of DOT Registry'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 Registry will notify the Complainant of the results of the Complaint within ten (10) days of receiving the Complaint.

DOT Registry'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 Registry considers the matter closed.

If the quick look does not resolve the matter, DOT Registry's Abuse Team will give the Complaint a full review. Any Registrant that has been determined to be in violation of DOT Registry 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 Registry's Abuse Team will alert it's Registry services team to immediately cancel the resolution of the domain name. DOT Registry'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 Registry's Abuse Team for further review. If DOT Registry's Abuse Team is satisfied by the Registrant's response that the use is not abusive, DOT Registry's Abuse Team will submit a request by the registry services provider to reactivate the domain name. DOT Registry'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 Registry 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 Registry's registry services personnel, DOT Registry 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 Registry 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 Registry will place the domain on “serverHold”.

Maintenance of Registration Criteria

If a Registrant previously awarded the “.INC” domain ceases to be registered with a Secretary of State or legally applicable jurisdiction, such Registrant will be required to forfeit the assigned “.INC” domain at their designated renewal date.
If DOT Registry discovers that a Registrant wrongfully applied for and was awarded a “.INC” domain, then such “.INC” will be immediately forfeited to DOT Registry.
If a Registrant previously awarded a “.INC” domain is dissolved and⁄or forfeited for any reason, then such “.INC” domain will be forfeited to DOT Registry at their designated renewal time; unless such Registrant takes all reasonable steps to become reinstated and such Registrant is reinstated within six months of being dissolved and⁄or forfeited.
If a Registrant previously awarded the “.INC” domain is administratively dissolved by the Secretary of State or legally applicable jurisdiction, then such “.INC” will be forfeited to DOT Registry at their designated renewal time, unless such Registrant is reinstated within six months of being administratively dissolved.
A Registrant’s “Active” Status will be verified annually. Any Registrant not considered “Active” by the definition listed above in question 18 will be given a probationary warning, allowing time for the Registrant to restore itself to “Active” Status. If the Registrant is unable to restore itself to “Active” status within the defined probationary period, their previously assigned “.INC” will be forfeited. In addition, DOT Registry’s definition of “Active” may change in accordance with the policies of the Secretaries of State.
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 Registry has written evidence of actual abuse of orphaned glue, DOT Registry will take action to remove those records from the zone to mitigate such malicious conduct.

DOT Registry’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 Registry 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 Registry 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 Registry will offer thick WhoIs services, in which all authoritative WhoIs data—including contact data—is maintained at the registry. DOT Registry 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 Registry's registrar will provide DOT Registry with an authorization code to verify eligible Registrants provide accurate Registrant contact information.

In order to further promote WhoIs accuracy, DOT Registry will offer a mechanism whereby third parties can submit complaints directly to the DOT Registry (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 Registry 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 Registry reserves the right to cancel or suspend the applicable domain name(s) should DOT Registry determine that the domains are being used in a manner contrary to DOT Registry's abuse policy.

DOT Registry shall also require authentication and verification of all Registrant data. DOT Registry 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.

With regard to registrars, DOT Registry shall provide financial incentives for pre-authentication of Registrant data prior to such data being passed to the registry. DOT Registry will provide for lower renewal and bulk registration fees in its RRAs for registrations which have been pre-authenticated and which DOT Registry can rely on as accurate data to be entered into its WhoIs database.

DOT Registry will also maintain historical databases of Registrants and associated information which have provided inaccurate WhoIs information. DOT Registry will endeavor to use this database to uncover patterns of suspicious registrations which DOT Registry 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 Registry's abuse policy.

In addition, DOT Registry'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 Registry 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 Registry 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 Registry reserves the right to suspend the applicable domain name(s) should DOT Registry determine that the Registrant is using the domain in question in a manner contrary to DOT Registry's abuse policy. DOT Registry 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 Registry's registrar. Authentication of modified Registrant information shall be accomplished 48 Hours.

29. Rights Protection Mechanisms

DOT Registry 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 Registry will protect the legal rights of others by implementing RPMs and anti-abuse policies backed by robust responsiveness to complaints and requirements of DOT Registry'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 Registry 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 Registry's domain name registration policy, namely, that all registrants be validly registered corporations and all applied-for domains will only be awarded the ".INC" domain that matches or includes a substantial part of the Registrant's legal name. DOT Registry will assign its Rights Protection Team; which is lead by our Director of Legal and Policy and further supported by two dedicated employees to receive and authenticate all Sunrise Registrations.

DOT Registry'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 Registry 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-served basis and must be active corporations in good standing before they may be awarded the requested domain, or able to proceed to auction. Upon submission of all of the required information and documentation, registrar will forward the information to DOT Registry's [RPM Team] for authentication. DOT Registry's [RPM Team] will review the information and documentation and 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 Registry will notify its registrar and the domain name will be released for registration.
DOT Registry will incorporate a Sunrise Dispute Resolution Policy (SDRP). The SRDP 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 Registry'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 Registry'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 Registry considers the matter closed.

If the domain name is not found to have adequately met the SERs, DOT Registry's [RPM Team] will alert the registrar and registry services provider to immediately suspend the resolution of the domain name. Thereafter, DOT Registry'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 Registry's [RPM Team] to determine if the SERs are met. If DOT Registry's [RPM Team] is satisfied by the registrant's response, DOT Registry's [RPM Team] will submit a request to the registrar and the registry services provider to unsuspend the domain name. DOT Registry'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 Registry. 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: Applicant 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.
Any entity, applying for blocks under Sunrise B as a non-member of the sponsored community cannot apply for names in the TLD.

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 ".INC" 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 ".INC" Founder Website, concurrent with the launch of their .INC Founder Website, said press release must be approved by DOT Registry;
c) Founder's websites should be kept good working order, with unique, meaningful content, user-friendly interfaces, and broad user appeal, for the duration of the License Term,
d) Founders are expected to proactively market and promote ".INC" gTLD in a manner that is likely to produce widespread awareness of the unique advantages gained through the ".INC" string.
e) Founders are expected to participate in reasonable joint marketing initiatives with DOT Registry or its Agents, these would be discussed and mutually agreed upon, given the unique circumstances of each marketing venture.
f) Founders will allow DOT Registry 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 Registry's marketing, promotional and communications materials.
DOT Registry 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 Regsitry 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 Registry's registration guidelines or policies.
Registrants participating in the Founders program will receive 25% off their initial registration fees, additional discounts may be offered to founders at the time of renewal, should DOT Registry choose to offer additional discounts to founders or term extensions (not to exceed 5 years) DOT Registry will seek advance approval from ICANN via the specified channels.

Landrush
Landrush is a limited time opportunity for companies that want to secure a high value ".INC" 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
Applicants must meet 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 Applicants will be given first right to either register their requested domain or withdraw their application. Since ".INC" is a sponsored community domain for registered Corporations, 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 A Applicant chooses to register their name regardless of the contention, then the Sunrise B Applicant may choose to pursue further action independently of DOT Registry to contest the name.
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.INC) then DOT Registry will notify both Applicantts of the contention and proceed to an auction process as described in Section 9.
d) If a Sunrise A Applicant and a Landrush Applicant apply for the same domain name, the Sunrise A Applicant , all else being equal will have priority over the Landrush Applicant .
e) 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. INC), then DOT Registry 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 Registry's rejection. Reconsideration can be requested by completing a reconsideration form and filing a reconsideration fee with DOT Registry. Forms, fee information, and process documentation will be available on the DOT Registry website. Upon receipt of the reconsideration form and the corresponding fee, DOT Registry 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 Registry.

Auctions
Sunrise A names found to be in contention as described above will result in Auction. DOT Registry 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) When your auction account is created, it will be assigned a unique bidder alias in order to ensure confidential bidding. The bidder alias will not reflect any information about your account. You may change your bidder alias to a name of your choosing but once set, it cannot be changed again.
b) All auction participants are expected to keep their account information current, throughout the auction process.
c) Auction participants will receive up to date communication from the auctioneer as the auction progresses, bidding status changes, or issues arise.
d) Bidding
i) Auctions will follow a standard process flow: scheduled (upcoming), open and closed.
ii) 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.
iii) 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.
iv) 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.
e) Extensions
i) 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.
ii) Auction extensions are meant to provide a mechanism that is fair for bidders in all time zones to respond to being outbid.
iii) 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.
iv) 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.
f) 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 Registry. Participants are encouraged therefore to consider carefully each bid submitted as any bid could be a winning bid.

Trademark Claims Service

DOT Registry will offer a Trademark Claims Service indefinitely to provide maximum protection and value to rights holders. The Trademark Claims Service will be monitored and operated by DOT Registry's RPM Team that will receive all communications regarding the Trademark Claims Service and catalog them. DOT Registry'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 Registry'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 Registry'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 Registry'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 Registry 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 Registry'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 Registry'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 Registry 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 Registry's RPM Team will receive all UDRP Complaints and decisions, and will notify its registrar to cancel or transfer all registrations determined to by a UDRP

panel to be infringing within ten (10) business days of receiving the decision. DOT Registry'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 Registry 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 .INC 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.

DOT Registry will not permit registrants to use proxy services.

Thick WhoIs

DOT 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.

Grace Period

If a Registrant previously awarded a ".INC" domain is dissolved and⁄or forfeited for any reason, then such ".INC" domain will be forfeited to DOT Registry at their designated renewal time; unless such Registrant takes all reasonable steps to become reinstated and such Registrant is reinstated within six months of being dissolved and⁄or forfeited.

If a Registrant previously awarded the ".INC" domain is administratively dissolved by the Secretary of State or legally applicable jurisdiction, then such ".INC" will be forfeited to DOT Registry at their designated renewal time, unless such Registrant is reinstated within six months of being administratively dissolved.

Takedown Procedure

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

At all times, DOT Registry will publish on its home website at NIC.INC 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 Registrys RPM Team who will catalogue and ticket in DOT Registry's CRM software and review as outlined herein. DOT Registry 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 Registry's RPM Team. A member of DOT Registry'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 Registry will notify the Complainant of the results of the Complaint within (10) days of receiving the Complaint.

After sending the confirmation email, DOT Registry's RPM Team will review the Complaint. If DOT Registry or its registrar determines that the registration was in bad faith, DOT Registry 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 Registry's RPM Team If DOT Registry's RPM Team is satisfied by the registrant's response that the content has been taken down or is not infringing, DOT Registry's RPM Team will unsuspend the domain name. DOT Registry'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 Registry 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 Registry's response to Question 28.

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

30.(a).1 Security Policies

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

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 ".INC" 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 ”.INC”. 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 ".INC" 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

New gTLD Application Submitted to ICANN by: Dot Registry LLC

String: LLC

Originally Posted: 13 June 2012

Application ID: 1-880-17627

Applicant Information

1. Full legal name

Dot Registry LLC

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact n ormation Redacted

4. Fax number

Contact nformation Redacted

5. If applicable, website or URL

Primary Contact

6(a). Name

Ms. Tess Pattison-Wade

6(b). Title

Executive Director

6(c). Address

6(d). Phone Number

Contact n ormation 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 n ormation Redacted

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Limited Liability Company

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

Kansas

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

Christopher Michael Parrott	Director of Finance
Paul Eugene Spurgeon	COO
Scott Adam Schactman	Director Law & 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

Ecyber Solutions Group Inc	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.

LLC

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.

To build confidence, trust, reliance and loyalty for consumers and business owners alike by creating a dedicated gTLD to specifically serve the Community of Registered Limited Liability Companies. Through our registry service, we will foster consumer peace of mind with confidence by ensuring that all domains bearing our gTLD string are members of the Community of Registered Limited Liability Companies. Our verification process will create an unprecedented level of security for online consumers by authenticating each of our registrant's right to conduct business in the United States. The ".LLC" gTLD will fill a unique void in the current DNS and assist in decreasing the burden on existing domain names by identifying members of the Community of Registered Limited Liability Companies.

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

With the increased popularity of the Internet as a consumer marketplace and the ease with which individuals are able to access information online, it is essential that safeguards be put in place to validate and identify legitimate businesses.

Businesses representing themselves as Limited Liability Companies by including LLC in their business names create an expectation amongst consumers that they have the legal right, to conduct business as a Limited Liability Company. Unfortunately, consumers are currently unable to quickly verify the accuracy of this representation. Fraudulent business entities rely on this consumer assumption and the lack of available verification resources to prey on both businesses and consumers. As online commerce replaces the brick-and-mortar business model there has been a corresponding rise in business identity theft online, which in turn creates a lack of consumer confidence.

In the vast majority of states, the Secretary of State is responsible for overseeing business entity registrations for their state — from basic funcions such as the registration of corporations or verification of business filings, to the administration of the Uniform Commercial Code, an act which provides for the uniform application of business contracts and practices across the United States. The Secretaries' role is critical to the chartering of businesses (including, but not limited to the formation of Limited Liability Companies) that wish to operate in their state. In this regard, the Secretaries of State maintain all records of business activities within the state, and in some states, the Secretary of State has wide-ranging regulatory authority over businesses as well.
The ".LLC" gTLD will be exclusively available to members of the Community of Registered Limited Liability Companies, as verified through each applicant's Secretary of States Office. By verifying that an applicant is a registered Limited Liability Company, DOT Registry will be able to bring unprecedented clarity and security to consumers and business owners, assuring internet users, registry applicants, and others that web addresses ending in ".LLC" are a hallmark of a valid Limited Liability Company recognized by a governmental authority of the United States. This process will decrease the possibility of identity misrepresentation in a cyber setting and assist lesser-known businesses in legitimizing their services to consumers.

In January 2012 after many public forums and contributions from consumer advocates, the Business Services Committee of the National Association of Secretary of States (NASS) released the NASS White Paper on Business Identity Theft, indicating that at least 26 states have reported business identity theft cases resulting from fraudulent business representations online. North Carolina Secretary of State Elaine Marshall, who serves as Co-Chair of the NASS Business Services Committee, indicates that the primary function of

the White Paper is to, “Harness new technology to develop cost-effective solutions, and ultimately make it harder for identity thieves to prey upon state-based businesses.”

With the implementation of the “.LLC” gTLD, consumers would have the ability to quickly identify the presented business as a valid US Limited Liability Company. As “.LLC” registrations grow, we will see a reduction in the ease with which criminals are able to hide behind fictitious entities because consumers will be conditioned to look for the appropriate gTLD ending before conducting business online. This simple gTLD extension would provide an efficient and cost effective solution to a growing economic concern in the United States by creating a verifiable online business community network. Through this innovative concept, the DNS system will help to build a stronger more resilient business platform for members of the Community of Registered Limited Liability Companies, while fostering user confidence, by ensuring accurate business representation.

It is our goal to provide an efficient and secure application process by minimizing the input required by the registrant and creating a streamlined, efficient evaluation process. We will accomplish this by reviewing the applicant’s proof of business registration with their state. Registry Applicants will only be awarded a domain through DOT Registry if the Registrant is an active member of the Community of Registered Limited Liability Companies. “Active” in this context can be defined as any Limited Liability Company registered with a Secretary of State in the United States and it’s territories, that is determined to be authorized to conduct business within the state at the time of registration. Registrants “Active” status will be verified on an annual basis to ensure the reputation and validity of the “.LLC” gTLD

DOT Registry will also ensure that registrants are represented by a web address that is both simple and intuitive allowing for easy recognition by search engines and Internet users. Awarded addresses will identify the registrants company and may be presented in the shortest most memorable way.

At DOT Registry, we believe in complete transparency, consistent with the Secretary of State’s Policy with regard to “Active” members of the Community of Registered Limited Liability Companies becoming publicly recorded upon completion of their entity registration process. Further, DOT Registry is informed by the position of the Task Force for Financial Integrity and Economic Development, which was created to advocate for improved levels of transparency and accountability in regards to beneficial ownership, control, and accounts of companies. Over the last decade the Task Force has focused specifically on combatting fraudulent business registrations which result in “fake” entities absorbing, hiding and transferring wealth outside the reach of law enforcement agencies. Because of this DOT Registry will not allow private or proxy registrations.

All approved domain registrants will be made public and available, so as to further validate DOT Registry’s mission of fostering consumer peace of mind by creating a gTLD string dedicated solely to valid members of the Community of Registered Limited Liabilty Companies. These transparency mechanisms will also serve as a deterrent for fraudulent entities by creating an expectation among consumers as to who they are conducting business with.

The social implications of business identity theft and consumer confusion are a paramount concern to DOT Registry. In our currently unstable economy, stimulating economic growth is vital. One means to such growth is by defusing the rampant, legitimate fear caused by online crimes and abuse, which leads to curtailed consumer behavior. By introducing the “.LLC” domain into the DNS, DOT Registry will attempt to reduce the social impact of identity theft on business owners which will in turn reduce consumer fears related to spending and ultimately boost economic growth in regards to consumption and purchase power.

Further, the “.LLC” gTLD will strive to foster competition by presenting members of the

Community of Registered Limited Liability Companies with a highly valued customized domain name that not only represents their business, but also their validity in the marketplace. Within the current existing top-level domains it is hard for businesses to find naming options that appropriately represent them. One advantage of the ".LLC" gTLD is that it will drive the "right" kind of online registrations by offering a valued alternative to the currently overcrowded and often unrestricted name space. Registrants will be inspired to pursue ".LLC" domains not only because they will be guaranteed a name representative to their business, but also because of the increased validity for their business operations brought about by the ".LLC" verification process. DOT Registry anticipates that the security offered through a ".LLC" extension will increase consumer traffic to websites which in turn will boost advertising revenue online and consumer purchasing.
Successful implementation of the ".LLC" domain will require two registration goals: 1) Capture newly formed corporations and assist them in securing a ".LLC" domain appropriate to their legal business name, and 2) converting existing online members of our community to a ".LLC" domain appropriate to their legal business name. These goals will be accomplished by the following practices:
1) Through our Founders Program, DOT Registry will secure key community tenants in the name space who will act as innovative leaders to assist us in changing the online culture of business representation, by promoting the benefits of the ".LLC" gTLD and shaping economic growth through increased consumer confidence.
2) DOT Registry will work closely with companies such as Legalzoom and CSC (both companies assist in the formation of entities and their registration processes), as well as individual Secretary of State's offices to capture newly admitted members of the community.
3) DOT Registry will educate members of the Community of Registered Limited Liability Companies on the benefits and importance of using a ".LLC" gTLD by building a strong relationship with organizations like the Small Business Administration and the Better Business Bureau, which promote business validation and consumer insight. By working closely with these well- known and highly regarded entities DOT Registry will be able to reach a larger majority of community members and enhance our message's validity.
4) DOT Registry will strive to create consumer and Internet user awareness through a strong Internet marketing presence and by developing a relationship with the National Association of Consumer Advocates, which was formed with the intention of curbing consumer abuse through predatory business practices.

At DOT Registry, we strive to meet the exact needs of our registrants and the internet users who patronize them. This will be accomplished by the creation of a seamless connection and strong communication channel between our organization and the governmental authority charged with monitoring the creation and good standing of Limited Liability Companies. DOT Registry will work closely with each Secretary of State's office to tailor our validation process to compliment each office's current information systems and to maximize the benefits of accurate information reporting. These processes are essential in fully assisting consumers in making educated decisions in regards to what businesses to patronize. The reach of the ".LLC" gTLD will not only impact online consumerism, but also offer an additional validation process for consumers to research contractors, businesses, and solicitors before choosing to do business with them in person.

The guidelines listed below were developed through collaborations with both NASS and individual Secretary of State's offices in order to ensure the integrity of the ".LLC" domain. All policies comply with ICANN-developed consensus policies.
In order to maintain the integrity of our mission statement and our relationship with each Secretary of State's office we will implement Registration Guidelines. In order to apply for a domain name ending in ".LLC", a Registrant must be registered with one of the Secretary of State's offices in the United States, the District of Columbia, or any of the U.S. possessions or territories as a limited liability company pursuant to that jurisdiction's laws on valid business registration. In addition, DOT Registry will implement the following Registration Guidelines and naming conventions:
1) A Registrant will only be awarded the ".LLC" domain that matches or includes a

substantial part of the Registrant's legal name. For example, Blue Star Partners, LLC. would be able to purchase either BlueStarPartners.LLC or BlueStar.LLC.
2) Registrants will not be allowed to register product line registrations, regardless of the products affiliation to the limited liability company. All awarded domains must match or include a substantial part of the Registrant's legal name.
3) If there are registrants applying for the same domain names, which correspond to their legal business names as registered in different states, then the ".LLC" domain will be awarded on a first-come, first-served basis to the first registrant.
4) However, if a registrant has a trademark registered with the United States Patent and Trademark Office (USPTO), then such registrant will have priority over any other registrant to be awarded the applied for ".LLC" domain.
5) If a registrant's requested ".LLC" domain has already been awarded to another registrant with the same or similar legal name, then DOT Registry will offer to award such registrant a ".LLC" domain with a distinctive denominator including but not limited to a tag, company describer, or name abbreviation. For example, if BlueStar.LLC was awarded to Blue Star Partners, LLC. of California, then Blue Star Partners, LLC. of Kansas would be offered the opportunity to use BlueStarPartners.LLC.
6) DOT Registry will work closely with the Secretary of State's Offices throughout the United States, with NASS and with a number of other agencies and organizations in maintaining the integrity and security of its' domain names. DOT Registry will utilize the Secretary of States' data resources to confirm that companies applying for their ".LLC" domain are in fact registered businesses.
7) All registrants that are awarded the ".LLC" domain will agree to a one-year minimum contract for their domain names that will automatically renew for an additional year on an annual basis if such contract is not terminated prior to the expiration of the renewal date.
8) DOT Registry or it's designated agent will annually verify each registrants community status in order to determine whether or not the entity is still an "Active" member of the community. Verification will occur in a process similar to the original registration process for each registrant, in which each registrant's "Active" Status and registration information will be validated through the proper state authority. In this regard, the following items would be considered violations of DOT Registry's Registration Guidelines, and may result in dissolution of a registrant's awarded ".LLC" domain:
(a) If a registrant previously awarded the ".LLC" domain ceases to be registered with the State.
(b) If a registrant previously awarded a ".LLC" domain is dissolved and⁄or forfeits the domain for any reason.
(c) If a registrant previously awarded the ".LLC" domain is administratively dissolved by the State.
Any registrant found to be "Inactive," or which falls into scenarios (a) through (c) above, will be issued a probationary warning by DOT Registry, allowing for the registrant to restore its active status or resolve its dissolution with its applicable Secretary of State's office. If the registrant is unable to restore itself to "Active" status within the defined probationary period, their previously assigned ".LLC" will be forfeited. DOT Registry reserves the right to change the definition of "Active" in accordance with the policies of the Secretaries of State.

9) If DOT Registry discovers that a registrant wrongfully applied for and was awarded a ".LLC" domain, then such ".LLC" will be immediately forfeited to DOT Registry. Wrongful application includes but is not limited to: a registrant misrepresenting itself as a member of the Community of Registered Limited Liability Companies, a registrant participating in illegal or fraudulent actions, or where a registrant would be in violation of our abuse policies described in Question 28 (including promoting or facilitating spam, trademark or copyright infringement, phishing, pharming, willful distribution of malware, fast flux hosting, botnet command and control, distribution of pornography, illegal access to other computers or networks, and domain kiting⁄tasting).
10) In the case of domain forfeiture due to any of the above described options, all

payments received by the Registrant for registration services to date or in advance payment will be non-refundable.
11) All registration information will be made publicly available. DOT Registry will not accept blind registration or registration by proxy. DOT Registry'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 Registry will provide a Web-based WHOIS application, which will be located at www.whois.llc. 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.
12) Awarded names are non-transferrable to entities outside of the designated community, regardless of affiliation to any member of the community. In the event that a registrant's business entity merges, is acquired, or sold, the new entity will be allowed to maintain the previously awarded ".LLC" domain until the domain renewal date, at which point they will be evaluated as described in number seven (7) above. Further, any entity acquiring a ".LLC" domain through the processes described in this guideline that does not meet the registration criteria and wishes to maintain the awarded domain will be allowed a grace period after the renewal verification process to correct any non-compliance issues in order to continue operating their acquired domain. If the said entity is unable to comply with DOT Registry's guidelines, the awarded domain will be revoked.
13) If an application is unable to be verified or does not meet the requirements of the sponsored community, the application will be considered invalid.

14) DOT Registry will implement a reserved names policy consisting of both names DOT Registry wishes to reserve for our own purposes as the registry operator and names protected by ICANN. DOT Registry will respect all ICANN reserved names including, but not limited to, two letter country codes and existing TLD's. Additionally, DOT Registry 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.

In addition to DOT Registry's comprehensive eligibility, verification, and policing mechanisms, DOT Registry will implement a series of Rights Protection Mechanisms (RPM), including 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; and stringent take down policies and all required dispute resolution policies.

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

.LLC was proposed for the sole purpose of eliminating business and consumer vulnerability in a cyber setting. In order to maintain the integrity of that mission and minimize the negative consequences to consumers and business owners the following policies will be adhered to:

a) No information collected from any registrant 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 correct data inaccuracies as needed.
e) All data will be kept secure.

DOT Registry will strictly uphold the rules set forth in their registration guidelines in order to accurately service the Community of Registered Limited Liability Companies and mitigate any negative consequences to consumers or Internet users.
Price structures for the ".LLC" gTLD are designed to reflect the cost of verification within our community requirements and the ongoing cost of operations. Price escalation will only occur to accommodate rising business costs or fees implemented by the Secretaries of State with regard to verifying the "Active" status of a Registrant. Any price increases would be submitted to ICANN as required in our Registry Agreement and will be compiled in a thoughtful and responsible manner, in order to best reduce the affects on both the registrants and the overall retail market.
DOT Registry 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 Registry 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.With regard to Registrars, DOT Registry shall provide financial incentives for pre-authentication of Registrant data prior to such data being passed to the registry. DOT Registry will provide for lower renewal and bulk registration fees in its RRAs for registrations which have been pre-authenticated and which DOT Registry can rely on as accurate data to be entered into its WhoIs database

Additionally, DOT Registry , through our founders program will provide a 25% discount to founders participants as a participation incentive. It is possible that DOT Registry 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?

Yes

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

DOT Registry plans to serve the Community of Registered Limited Liability Companies. Members of the community are defined as businesses registered as limited liability companies with the United States or its territories. Limited Liability Companies or (LLC's) as they are commonly abbreviated, represent one of the most popular business entity structures in the US. LLC's commonly participate in acts of commerce, public services, and product creation.

Limited Liability Companies (LLC) are a relatively new business structure for the United

States, the first LLC was validated in the state of Wyoming in 1977 and in 1996 the National Conference of Commissioners on Uniform State Laws adopted the Uniform Limited Liability Company Act; providing for both the definition of an LLC and the governmental standards under which an LLC may be formed. It was through the Uniform Limited Liability Company Act that a standard set of policies were created to define, validate, and monitor the operations of LLC's, thus creating a unique and accountable business community in the United States.

An LLC is defined as a flexible form of enterprise that blends elements of partnership and corporate structures. It is a legal form of company that provides limited liability to its owners in the vast majority of United States jurisdictions. LLC's are a unique entity type because they are considered a hybrid, having certain characteristics of both a corporation and a partnership or sole proprietorship. LLC's are closely related to corporations in the sense that they participate in similar activities and provide limited liability to their partners. Additionally, LLC's share a key characteristic with partnerships through the availability of pass-through income taxation. LLC's are a more flexibile entity type than a corporation and are often well suited for businesses owned by a single owner.

Common advantages to forming an LLC include:

1) Flexibility in tax reporting, LLC's may choose if they would like to be taxed as a sole proprietorship, partnership, S Corporation, or C Corporation. This is the only business entity form in the United States that allows for taxation flexibility.
2) LLC's have much less administrative paperwork and reporting requirements then corporations.
3) Unless the LLC elects to be taxed as a C Corp, LLC's enjoy pass through taxation.
4) Limited liability, meaning that owners of an LLC, called "members" are protected from some or all liability acts and debts of the LLC.

LLC's have become increasingly popular in the United States because their formation provides owners with the protection of a corporation and the flexibility of a partnership.

With the number of registered LLC's in the United States totaling over five million in 2010 (as reported by the International Association of Commercial Administrators) it is hard for the average consumer to not conduct business with an LLC (popular LLC's in the United States include: AOL and BMW). Through the creation of DOT Registry's .LLC string, consumers can quickly validate that they are working with a member of the Community of Registered Limited Liability Companies, providing consumers with brand reassurance and peace of mind. DOT Registry believes that it is essential to identify limited liability companies online in order to expand on their creditability and further highlight their privilege to conduct business in the US. Proper representation of this community would allow consumers to make educated choices in choosing businesses to patronize and support.
LLC's can be formed through any jurisdiction of the United States. Therefore members of this community exist in all 50 US states and its territories. LLC formation guidelines are dictated by state law and can vary based on each state's regulations. Persons form an LLC by filing required documents with the appropriate state authority, usually the Secretary of State. Most states require the filing of Articles of Organization. These are considered public documents and are similar to articles of incorporation, which establish a corporation as a legal entity. At minimum, the articles of organization give a brief description of the intended business purposes, the registered agent, and registered business address.
LLC's are expected to conduct business in conjunction with the policies of the state in which they are formed, and the Secretary of State periodically evaluates a LLC's level of good standing based on their commercial interactions with both the state and consumers. DOT Registry or its designated agents would verify membership to the Community of Registered Limited Liability Companies by collecting data on each Registrant and cross-referencing the information with their applicable registration state. In order to maintain the reputation

of the ".LLC" string and accurately delineate the member to consumers, Registrants would only be awarded a domain that accurately represents their registered legal business name. Additionally, DOT Registry will not allow blind registrations or registration by proxy, therefore DOT Registry's WHOIS service will tie directly back to each member's state registration information and will be publicly available in order to provide complete transparency for consumers.
Entities are required to comply with formation practices in order to receive the right to conduct business in the US. Once formed an LLC must be properly maintained. LLC's are expected to comply with state regulations, submit annual filings, and pay specific taxes and fees. Should an LLC fail to comply with state statutes it could result in involuntary dissolution by the state in addition to imposed penalties, taxes and fees.
While state statutes vary, the majority of states have adopted the following guidelines in regards to the formation of LLC's:

(1) The name of each limited liability company must contain the words "Limited Liability Company" or the abbreviation "L.L.C." or the designation "LLC".

(2) In order to form a limited liability company, one or more authorized persons must execute the Articles of Organization. Which shall contain: the name of the limited liability company; the address of the registered office and the name and address of the registered agent for service of process required to be maintained; and any other matters the members determine to include therein.
(3) A Limited Liability Company may be organized to conduct or promote any lawful business or purposes, except as may otherwise be provided by the Constitution or other law of this State.
All entities bearing the abbreviation LLC in their business name create the assumption that they have been awarded the privileges associated to that title such as: the ability to conduct commerce transactions within US borders or territories, the ability to market products, solicit consumers and provide reputable services in exchange for monetary values, and finally to provide jobs or employment incentives to other citizens.
Membership in the Community of Registered Limited Liability Companies is established through your business entity registration. In order to maintain your membership to this community you must remain an "Active" member of the community. Active" in this context can be defined as any LLC registered with a Secretary of State in the United States and its territories, that is determined to be authorized to conduct business within that State at the time of their registration. Registrant's "Active" status will be verified on an annual basis as described above in question 18 in order to ensure the reputation and validity of the ".LLC" gTLD.
Since LLC's are not currently delineated on the Internet, the creation of this string would mark a unique advancement in consumer security and confidence in the United States. Essentially, this will create the first ever, clear delineator for the Community of Registered Limited Liability Companies.

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

DOT Registry is a registered LLC in the State of Kansas as defined by the Kansas LLC Statute: Kan. Stat. Ann. §§ 17-7662 through 17-76,142. By becoming a verifiable US LLC, DOT Registry becomes a member of the community it serves. In addition, DOT Registry is a corporate affiliate of the National Association of Secretaries of State (NASS), an organization which acts as a medium for the exchange of information between states and fosters cooperation in the development of public policy, and is working to develop individual relationships with each Secretary of State's office in order to ensure our continued commitment to honor and respect the authorities of each state.
DOT Registry is acutely aware of our responsibility to uphold our mission statement of:

building confidence, trust, reliance, and loyalty for consumers and business owners alike by creating a dedicated gTLD to specifically serve the Community of Registered Limited Liability Companies .DOT Registry has also specifically pledged to various Secretaries of State to responsibly manage this gTLD in a manner that will both protect and promote business development in the US. Further our policies were developed through direct collaboration with the state offices so as to mitigate any possibility of misrepresenting their regulations. In order to ensure that we accomplish our goal and preserve the credibility of our operations DOT Registry has taken the following advance actions to ensure compliance and community protection:

1) Developed registration policies that are currently reflective of common state law dictating the creation and retention of LLC's in the United States.

2) Created a strong partnership with CSC (an ICANN approved registrar also specializing in corporate formation services). Through this partnership DOT Registry was able to develop a streamlined verification process to validate potential Registrants as members of the community and ensure that continued annual verifications are completed in a time sensitive and efficient manner. This process will ensure that consumers are not misled by domains registered with the ".LLC" gTLD. Additionally, this process will create peace of mind amongst community members by ensuring that their integrity is not diminished by falsely identified corporations being represented by a ".LLC" extension.

3) Built a strong relationship with several Secretaries of State in order to receive and give consistent input on policy implementation and state regulation updates. DOT Registry has also notified NASS that we have designed our registration policies and procedures to address NASS' concerns about verification requirements in the TLD.

4) Established an in-house legal and policy director to review, enhance, and ensure compliance and consistency with all registration guidelines and community representations. As indicated in many of the attached letters, DOT Registry will be held specifically accountable for protecting the integrity of its restrictions and of the members of this community. DOT Registry will consult directly with NASS and policy advisors in the state offices consistently in order to continue to accurately represent the Community of Registered Limited Liability Companies and live up to the vast standards associated to the ".LLC" gTLD.

In furtherance of this goal, DOT Registry has attached letters from critical advocates for and representatives of the proposed community, including:

1) Various Secretary of States Offices: Specifically The Secretary of State of Delaware which is widely regarded as a leader in entity formation and policy in the United States and The Secretary of State of South Dakota, which is working towards combatting business identity theft and fictitious business registration.

2) Various members of the community that are interested in utilizing the ".LLC" gTLD

DOT Registry can be viewed as an exemplary community representative not only through its pledged commitment to excellence, but also through its continued commitment to build relationships with the state offices charged with registering members of this community. DOT Registry pledges through its registry policies to uphold a common standard of evaluation for all applicants and to add increased integrity to the Community of Limited Liability Companies. These pledges are further enforced by the endorsement letters from the above organizations, which call the authentication/verification measures proposed by DOT Registry critical to the success of the proposed community.

Similarly, DOT Registry will adhere to all standards of business operations as described in the Kansas state business statutes and will be equally accountable to consumers to deliver continuously accurate findings and valid registrations.

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

.The goal of the ".LLC" gTLD is to build confidence, trust, reliance, and loyalty for consumers and business owners alike by creating a dedicated gTLD to specifically serve the Community of Registered Limited Liability Companies. Through our registry service, we will foster consumer peace of mind with confidence by ensuring that all domains bearing our gTLD string are members of the Community of Registered Limited Liability Companies. Our verification process will create an unprecedented level of security for online consumers by authenticating each of our registrant's right to conduct business in the United States. The ".LLC" gTLD will fill a unique void in the current DNS and assist in decreasing the burden on existing domain names by identifying members of the Registered Community of Limited Liability Companies. The creation of the "LLC" gTLD will bring innovation and unprecedented coordination of this valuable service of verification, a purpose endorsed by many individual Secretary of States and NASS. Additionally, ".LLC" will further promote the importance of accurate business registrations in the US, while assisting in combatting business identity theft by increasing registration visibility through our WHOIS services and strict abuse policies.

The intended registrants of the ".LLC" gTLD would consist of members of the Community of Registered Limited Liability Companies. This would be verified by collecting data on each Registrant and cross-referencing the information with their applicable registration state. In order to ensure that this process is accomplished in a secure and time effective manner DOT Registry will develop partnerships with each Secretary of State's office in order to create the applicable applications to securely verify registrant data.

End-users for this TLD would include everyday consumers, members of the community, businesses within the community, and consumers looking for more accurate information with regards to those with whom they may conduct business. DOT Registry plans to initiate a robust marketing campaign geared towards the proposed end-users in order to ensure that consumers are aware of what ".LLC" stands for and its significance throughout the Community of Registered Limited Liability Companies. In addition to the vast consumer benefits from the creation of the ".LLC" gTLD, DOT Registry believes that ".LLC" domains would be considerably beneficial to business end users. Since DOT Registry will not allow blind registration or registration by proxy businesses viewing ".LLC" sites would be able to instantly ascertain what businesses operate under the blanket of parent companies, are subsidiaries of other businesses, and of course where an LLC is domiciled. This easily identifiable information not only assists businesses in accurately identifying who they are doing business with, it would also assist in locating sales and use tax information, identifying applicable state records, and tracking an entity's history. These factors could help to determine the outcome of sales, mergers, contract negotiations, and business relationships. Ensuring that this kind of transparency and accountability — qualities previously not attainable in a TLD — shall be at the fingertips of potential business partners or investors.

Our registry policies will be adapted to match any changing state statutes in relation to the definition and creation of LLC's in the U.S., ensuring the longevity and reputation of our registry services and our commitment to consumers to only represent valid U.S. limited liability companies. Much like the perpetuity of the members of the Community of Registered Limited Liability Companies, the ".LLC" gTLD will enjoy a similar immortality, for as long as LLC entities continue to exist in the United States the ".LLC" relevance will not diminish. As awareness of the gTLD's mission becomes more widely recognized by end-users expectations to understand who you choose to do business with will increase, making the need for the ".LLC" gTLD more prominent.

In addition, it is our concern that the implementation of the gTLD string ".LLC" as a generic string, without the restrictions and community delineations described in this application and endorsed by NASS and the various Secretaries of State, could promote confusion among consumers and provide clever criminal enthusiasts the tools necessary to misrepresent themselves as a U.S.-based LLC. There is an expectation amongst consumers that entities using the words Limited Liability Company in their business name have the legal right and ability to conduct business in the United States. This representation by non-members of the Community of Registered Limited Liability Companies is not only fraudulent, but a great disservice to consumers.

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

“.LLC” was chosen as our gTLD string because it is the commonly used abbreviation for the entity type that makes up the membership of our community. In the English language Limited Liability Company is primarily shortened to LLC when used to delineate business entity types. For example Red Bridge, LLC. could additionally be referred to Red Bridge Limited Liability Company. Since all of our community members are limited liability companies we believed that “.LLC” would be the simplest, most straight forward way to accurately represent our community.

LLC is a recognized abbreviation in all 50 states and US territories denoting the registration type of a business entity. Our research indicates that while other jurisdictions use LLC as a corporate identifier, their definitions are quite different and there are no other known associations or definitions of LLC in the English language.

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

In order to accurately protect the integrity of our domain name and serve the proposed community the following safeguards will be adapted:

1)	All Registrants will be required to submit a minimum of: Their registered business address, State of formation, name and contact information of responsible party, and legally registered business name. DOT Registry or its agents will use this information to cross-reference the applicable state’s registration records in order to verify the accuracy of the Registrant’s application. Should DOT Registry be unable to verify the legitimacy of the Registrants application additional information might be requested in order to award a domain name.

2)	A Registrant will only be awarded the “.LLC” domain that matches or includes a substantial part of the Registrant’s legal name. For example, Blue Star Partners, LLC. would be able to purchase either BlueStarPartners.LLC or BlueStar.LLC.
3)	Registrants will not be allowed to register product line registrations, regardless of the products affiliation to the limited liability company. All awarded domains must match or include a substantial part of the Registrant’s legal name.
4)	If there are registrants applying for the same domain names, which correspond to their legal business names as registered in different states, then the “.LLC” domain will be awarded on a first-come, first-served basis to the first registrant.
5)	However, if a registrant has a trademark registered with the United States Patent and Trademark Office (USPTO), then such registrant will have priority over any other registrant to be awarded the applied for “.LLC” domain.
6)	If a registrant’s “.LLC” domain has already been awarded to another registrant with the same or similar legal name, then DOT Registry will offer to award such registrant a “.LLC” domain with a distinctive denominator including but not limited to a tag, company describer, or name abbreviation. For example, if BlueStar.LLC was awarded to Blue Star Partners, LLC. of California, then Blue Star Partners, LLC. of Kansas would be offered the

opportunity to use BlueStarPartners.LLC.
7) DOT Registry will work closely with the Secretary of State's Offices throughout the United States, with NASS and with a number of other agencies and organizations in maintaining the integrity and security of its domain names. DOT Registry will utilize the Secretary of States' data resources to confirm that companies applying for their ".LLC" domain are in fact registered businesses.
8) DOT Registry or it's designated agent will annually verify each registrants community status in order to determine whether or not the entity is still an "Active" member of the community. Verification will occur in a process similar to the original registration process for each registrant, in which each registrant's "Active" Status and registration information will be validated through the proper state authority. In this regard, the following items would be considered violations of DOT Registry's Registration Guidelines, and may result in dissolution of a registrant's awarded ".LLC" domain:
(a) If a registrant previously awarded the ".LLC" domain ceases to be registered with the State.
(b) If a registrant previously awarded a ".LLC" domain is dissolved and⁄or forfeits the domain for any reason.
(c) If a registrant previously awarded the ".LLC" domain is administratively dissolved by the State.
Any registrant found to be "Inactive," or which falls into scenarios (a) through (c) above, will be issued a probationary warning by DOT Registry, allowing for the registrant to restore its active status or resolve its dissolution with its applicable Secretary of State's office. If the registrant is unable to restore itself to "Active" status within the defined probationary period, their previously assigned ".LLC" will be forfeited. DOT Registry reserves the right to change the definition of "Active" in accordance with the policies of the Secretaries of State.
9) If DOT Registry discovers that a registrant wrongfully applied for and was awarded a ".LLC" domain, then such ".LLC" will be immediately forfeited to DOT Registry. Wrongful application includes but is not limited to: a registrant misrepresenting itself as a member of the Community of Registered Limited Liability Companies, a registrant participating in illegal or fraudulent actions, or where a registrant would be in violation of our abuse policies described in Question 28 (including promoting or facilitating spam, trademark or copyright infringement, phishing, pharming, willful distribution of malware, fast flux hosting, botnet command and control, distribution of pornography, illegal access to other computers or networks, and domain kiting⁄tasting).
10) All registration information will be made publicly available. DOT Registry will not accept blind registration or registration by proxy. DOT Registry'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 Registry will provide a Web-based WHOIS application, which will be located at www.whois.llc. 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.
11) Awarded names are non-transferrable to entities outside of the designated community, regardless of affiliation to any member of the community. In the event that a registrant's business entity merges, is acquired, or sold, the new entity will be allowed to maintain the previously awarded ".LLC" domain until the domain renewal date, at which point they will be evaluated as described in number seven (7) above. Further, any entity acquiring a ".LLC" domain through the processes described in this guideline that does not meet the registration criteria and wishes to maintain the awarded domain will be allowed a grace period after the renewal verification process to correct any non-compliance issues in order to continue operating their acquired domain. If the said entity is unable to comply with DOT Registry's guidelines, the awarded domain will be revoked.
12) If an application is unable to be verified or does not meet the requirements of the sponsored community, the application will be considered invalid.
In addition to Applicant's comprehensive eligibility, verification, and policing mechanisms, DOT Registry will implement a series of Rights Protection Mechanisms (RPM), including 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 policies in order to properly operate the registry; and Applicant shall comply with any RRDRP decision, further reinforcing the fact that Applicant is committed to acting in best interest of the community.
DOT Registry will employ an in house Rights Protection Mechanism Team consisting of our Director of Legal and Policy and two additional support personnel. The RPM team will work to mitigate any RPM complaints, while protecting the general rights and integrity of the ",LLC" gTLD. The RPM team will strictly enforce the rights protection mechanisms described in this application.
Membership verification will be performed via DOT Registry's designated agents that which have software systems in place to efficiently interface with each state's data records. By utilizing the resources of industry leaders in this field, DOT Registry will ensure accurate and timely verification in addition to our ability to meet the needs of such a vast community. "Active" status will be specifically verified by cross referencing an applicant's registration data with state records. If this process is unable to be automated at any given time DOT Registry's agents will manually verify the information by contacting the applicable state agencies. While manual verification will obviously employ a larger pool of resources, DOT Registry believes that its industry partners are sufficiently able to accomplish this task based on their employee pool and past business accomplishments. Registrants will be expected to provide a minimum of their legal registered name, state of organization, registered business address, and administrative contact. All additional information required such as proof of incorporation or "active" status verification will be the sole responsibility of DOT Registry or its designated agents and will be acquired through the processes described herein.
DOT Registry will not restrict the content of ".LLC" sites other then through the enforcement of our Abuse Mitigation practices or Rights Protection Mechanisms as described in question 28 and 29 of this application. All ".LLC" sites will be expected to adhere to the content restrictions described in DOT Registry's abuse policies. Any sites infringing on the legal rights of other individuals or companies, trademarks, or participating in the practice and promotion of illegal activities will be subject to Applicant's take down procedures.
".LLC" domains are designed for the sole use of community members with the intention of promoting their specific business activities. Any Registrants falsely identifying themselves as a community members or inaccurately representing their intentions could be deemed in non-compliance with our registry policies resulting in the revocation of their awarded domain.

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

-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 ".LLC" 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 Registry 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 ".LLC". 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 Registry 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 ".LLC" 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 Registry, 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 Registry will not be offering services that are unique to ".LLC".

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 Registry has partnered with NeuStar, Inc (”Neustar”), an experienced TLD registry operator, for the operation of the ”.LLC” 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 ”.LLC” 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 Registry is mitigating the significant risks and costs associated with the development of a new system. Highlights of the SRS include:

-State-of-the-art, production proven multi-layer design

-Ability to rapidly and easily scale from low to high volume as a TLD grows

-Fully redundant architecture at two sites

-Support for IDN registrations in compliance with all standards

-Use by over 300 Registrars

-EPP connectivity over IPv6

-Performance being measured using 100% of all production transactions (not sampling).

24.2.2 SRS Systems, Software, Hardware, and Interoperability

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

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

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

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

-The IP address of the client

-Timestamp

-Transaction Details

-Processing Time.

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

24.2.3 SRS Design

The SRS incorporates a multi-layer architecture that is designed to mitigate risks and easily scale as volumes increase. The three layers of the SRS are:

-Protocol Layer

-Business Policy Layer

-Database.

Each of the layers is described below.

24.2.4 Protocol Layer

The first layer is the protocol layer, which includes the EPP interface to registrars. It consists of a high availability farm of load-balanced EPP servers. The servers are designed to be fast processors of transactions. The servers perform basic validations and then feed information to the business policy engines as described below. The protocol layer is horizontally scalable as dictated by volume.

The EPP servers authenticate against a series of security controls before granting service, as follows:

-The registrar’s host exchanges keys to initiates a TLS handshake session with the EPP

server.

-The registrar’s host must provide credentials to determine proper access levels.

-The registrar’s IP address must be preregistered in the network firewalls and traffic-shapers.

24.2.5 Business Policy Layer

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

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

The SRS today processes over 30 million EPP transactions daily.

24.2.6 Database

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

Figure 24-1 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 ".LLC" 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 ".LLC".

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 ".LLC" 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 ".LLC" 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 ".LLC" 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 ".LLC" registry.

25. Extensible Provisioning Protocol (EPP)

25.1 Introduction

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

26. Whois

DOT Registry, 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 Registry, 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 Registry, 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 Registry, LLC's WHOIS services will include:

- Fully compliant with all relevant RFCs including 3912;
- Production proven, highly flexible, and scalable (DOT Registry, 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 Registry, 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 Registry, 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 Registry, LLC's registry services operator currently processes millions of WHOIS queries per day.

In addition to the WHOIS Service on port 43, DOT Registry, LLC will provide a Web-based WHOIS application, which will be located at www.whois.llc. 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 Registry, 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 Registry, 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 Registry, 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 Registry, 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 Registry, LLC's information, DOT Registry, 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

”.LLC” 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 ”.LLC”.

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 ”.LLC” registry per the defined ”.LLC” 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 ”.LLC” 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 ".LLC" 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 ".LLC" registry.

-Hold Removes the domain from the DNS zone.

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

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

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

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

The lifecycle of a domain begins with the registration of the domain. All registrations must follow the EPP standard, as well as the specific business rules described in the response to Question 18 above. Upon registration a domain will either be in an active or inactive state. Domains in an active state are delegated and have their delegation information published to the zone. Inactive domains either have no delegation information or their delegation information in not published in the zone. Following the initial registration of a domain, one of five actions may occur during its lifecycle:

-Domain may be updated

-Domain may be deleted, either within or after the add-grace period

-Domain may be renewed at anytime during the term

-Domain may be auto-renewed by the Registry

-Domain may be transferred to another registrar.

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

27.2 Registration States

27.2.1 Domain Lifecycle Registration States

As described above the ".LLC" 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 serverTranferProhibited status. This will cause the transfer request to fail.The domain goes back to its original state.

-DeleteProhibited: The domain is in clientDeleteProhibited and/or serverDeleteProhibited status.This will cause the delete command to fail.The domain goes back to its original state.

Note: the locked state is not represented as a distinct state on the diagram as a domain may be in a locked state in combination with any of the other states: inactive, active, pending transfer, or pending delete.

27.5.1 EPP RFC Consistency

As described above, the domain lifecycle is determined by ICANN policy and the EPP RFCs. Neustar has been operating ICANN TLDs for the past 10 years consistent and compliant with all the ICANN policies and related EPP RFCs.

27.6 Resources

The registration lifecycle and associated business rules are largely determined by policy and business requirements; as such the Product Management and Policy teams will play a critical role in working Applicant to determine the precise rules that meet the requirements of the TLD. Implementation of the lifecycle rules will be the responsibility of Development/Engineering team, with testing performed by the Quality Assurance team.Neustar's SRS implementation is very flexible and configurable, and in many case development is not required to support business rule changes.

The ".LLC" 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 ".LLC" registry.

28. Abuse Prevention and Mitigation

General Statement of Policy

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

Anti-Abuse Policy

DOT Registry 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 Registry with broad power to suspend, cancel, or transfer domain names that violate the Abuse Policy. DOT Registry will publish the Abuse Policy on its home website at NIC.LLC and clearly provide DOT Registry'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 Registry 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 Registry'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 Registry will catalog all abuse

communications in its CRM software using a ticketing system that maintains records of all abuse complaints indefinitely. Moreover, DOT Registry 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 Registry reserves the right to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary to ; (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 Registry, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) to correct mistakes made by the DOT Registry, 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 Registry'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 Registry will take great care to ensure that trademark and copyright infringement does not occur within the .LLC TLD. DOT Registry 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 Registry;
- 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 Registry

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 Registry will provide a domain name anti-abuse procedure modeled after the DMCA's notice-and-takedown procedure.

At all times, DOT Registry will publish on its home website at NIC.LLC 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 Registry's Legal Team, who will review and if applicable remedy any Complaint regarding an alleged violation of the Abuse Policy. DOT Registry 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 Registry's CRM software and relayed to DOT Registry's Abuse Team. A member of DOT Registry'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 Registry will notify the Complainant of the results of the Complaint within ten (10) days of receiving the Complaint.

DOT Registry'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 Registry considers the matter closed.

If the quick look does not resolve the matter, DOT Registry's Abuse Team will give the Complaint a full review. Any Registrant that has been determined to be in violation of DOT Registry 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 Registry's Abuse Team will alert it's Registry services team to immediately cancel the resolution of the domain name. DOT Registry'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 Registry's Abuse Team for further review. If DOT Registry's Abuse Team is satisfied by the Registrant's response that the use is not abusive, DOT Registry's Abuse Team will submit a request by the registry services provider to reactivate the domain name. DOT Registry'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 Registry 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 Registry's registry services personnel, DOT Registry 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 Registry 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 Registry will place the domain on "serverHold".

Maintenance of Registration Criteria

If a Registrant previously awarded the ".LLC" domain ceases to be registered with a Secretary of State or legally applicable jurisdiction, such Registrant will be required to forfeit the assigned ".LLC" domain at their designated renewal date.
If DOT Registry discovers that a Registrant wrongfully applied for and was awarded a ".LLC" domain, then such ".LLC" will be immediately forfeited to DOT Registry.
If a Registrant previously awarded a ".LLC" domain is dissolved and⁄or forfeited for any reason, then such ".LLC" domain will be forfeited to DOT Registry at their designated renewal time; unless such Registrant takes all reasonable steps to become reinstated and such Registrant is reinstated within six months of being dissolved and⁄or forfeited.
If a Registrant previously awarded the ".LLC" domain is administratively dissolved by the Secretary of State or legally applicable jurisdiction, then such ".LLC" will be forfeited to DOT Registry at their designated renewal time, unless such Registrant is reinstated within six months of being administratively dissolved.
A Registrant's "Active" Status will be verified annually. Any Registrant not considered "Active" by the definition listed above in question 18 will be given a probationary warning, allowing time for the Registrant to restore itself to "Active" Status. If the Registrant is unable to restore itself to "Active" status within the defined probationary period, their previously assigned ".LLC" will be forfeited. In addition, DOT Registry's definition of "Active" may change in accordance with the policies of the Secretaries of State.

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 Registry has written evidence of actual abuse of orphaned glue, DOT Registry will take action to remove those records from the zone to mitigate such malicious conduct.

DOT Registry’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 Registry 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 Registry 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 Registry will offer thick WhoIs services, in which all authoritative WhoIs data—including contact data—is maintained at the registry. DOT Registry 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 Registry’s registrar will provide DOT Registry with an authorization code to verify eligible Registrants provide accurate Registrant contact information.

In order to further promote WhoIs accuracy, DOT Registry will offer a mechanism whereby third parties can submit complaints directly to the DOT Registry (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 Registry 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 Registry reserves the right to cancel or suspend the applicable domain name(s) should DOT Registry determine that the domains are being used in a manner contrary to DOT Registry’s abuse policy.

DOT Registry shall also require authentication and verification of all Registrant data. DOT Registry shall verify the certificates of incorporation, whether a Limited Liability Company 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.

With regard to registrars, DOT Registry shall provide financial incentives for pre-authentication of Registrant data prior to such data being passed to the registry. DOT Registry will provide for lower renewal and bulk registration fees in its RRAs for registrations which have been pre-authenticated and which DOT Registry can rely on as accurate data to be entered into its WhoIs database.

DOT Registry will also maintain historical databases of Registrants and associated information which have provided inaccurate WhoIs information. DOT Registry will endeavor to use this database to uncover patterns of suspicious registrations which DOT Registry 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 Registry's abuse policy.

In addition, DOT Registry'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 Registry 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 Registry 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 Registry reserves the right to suspend the applicable domain name(s) should DOT Registry determine that the Registrant is using the domain in question in a manner contrary to DOT Registry's abuse policy. DOT Registry 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 Registry's registrar. Authentication of modified Registrant information shall be accomplished (48) hours.

29. Rights Protection Mechanisms

DOT Registry 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 Registry will protect the legal rights of others by implementing RPMs and anti-abuse policies backed by robust responsiveness to complaints and requirements of DOT Registry'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 Registry 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 Registry's domain name registration policy, namely, that all registrants be validly registered limited liability companies and all applied-for domains will only be awarded the ".LLC" domain that matches or includes a substantial part of the Registrant's legal name. DOT Registry will assign its Rights Protection Team; which is lead by our Director of Legal and Policy and further supported by two dedicated employees to receive and authenticate all Sunrise Registrations.

DOT Registry'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 Registry 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-served basis and must be active limited liability companies in good standing before they may be awarded the requested domain, or able to proceed to auction. Upon submission of all of the required information and documentation, registrar will forward the information to DOT Registry's [RPM Team] for authentication. DOT Registry's [RPM Team] will review the information and documentation and 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 Registry will notify its registrar and the domain name will be released for registration.
DOT Registry will incorporate a Sunrise Dispute Resolution Policy (SDRP). The SRDP 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 Registry'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 Registry'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 Registry considers the matter closed.

If the domain name is not found to have adequately met the SERs, DOT Registry's [RPM Team] will alert the registrar and registry services provider to immediately suspend the resolution of the domain name. Thereafter, DOT Registry'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 Registry's [RPM Team] to determine if the SERs are met. If DOT Registry's [RPM Team] is satisfied by the registrant's response, DOT Registry's [RPM Team] will submit a request to the registrar and the registry services provider to unsuspend the domain name. DOT Registry'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 Registry. 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: Applicant 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.
Any entity, applying for blocks under Sunrise B as a non-member of the sponsored community cannot apply for names in the TLD.

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 ".LLC" 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 ".LLC" Founder Website, concurrent with the launch of their .INC Founder Website, said press release must be approved by DOT Registry;
c) Founder's websites should be kept good working order, with unique, meaningful content, user-friendly interfaces, and broad user appeal, for the duration of the License Term,
d) Founders are expected to proactively market and promote ".LLC" gTLD in a manner that is likely to produce widespread awareness of the unique advantages gained through the ".LLC" string.
e) Founders are expected to participate in reasonable joint marketing initiatives with DOT Registry or its Agents, these would be discussed and mutually agreed upon, given the unique circumstances of each marketing venture.
f) Founders will allow DOT Registry 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 Registry's marketing, promotional and communications materials.
DOT Registry 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 Registry 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 Registry's registration guidelines or policies.
Registrants participating in the Founders program will receive 25% off their initial registration fees, additional discounts may be offered to founders at the time of renewal, should DOT Registry choose to offer additional discounts to founders or term extensions (not to exceed 5 years) DOT Registry will seek advance approval from ICANN via the specified channels.

Landrush
Landrush is a limited time opportunity for companies that want to secure a high value ".LLC" 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 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. Since ".LLC" is a sponsored community domain for registered limited liability companies, 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 A Applicant chooses to register their name regardless of the

contention, then the Sunrise B Appliant may choose to pursue further action independently of Applciant to contest the name.
c) If two Sunrise A Applicant's apply for the same domain name (i.e., Delta Airlines and Delta Faucet both seek to be awarded the use of DELTA.LLC) then DOT Registry will notify both Applicants of the contention and proceed to an auction process as described in Section 9.
d) If a Sunrise A Applicant and a Landrush Applicant apply for the same domain name, the Sunrise A Applicant, all else being equal will have priority over the Landrush Applicant.
e) 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. LLC), then DOT Registry 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 Registry's rejection. Reconsideration can be requested by completing a reconsideration form and filing a reconsideration fee with DOT Registry. Forms, fee information, and process documentation will be available on the DOT Registry website. Upon receipt of the reconsideration form and the corresponding fee, DOT Registry 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 Registry.

Auctions
Sunrise A names found to be in contention as described above will result in Auction. DOT Registry 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) When your auction account is created, it will be assigned a unique bidder alias in order to ensure confidential bidding. The bidder alias will not reflect any information about your account. You may change your bidder alias to a name of your choosing but once set, it cannot be changed again.
b) All auction participants are expected to keep their account information current, throughout the auction process.
c) Auction participants will receive up to date communication from the auctioneer as the auction progresses, bidding status changes, or issues arise.
d) Bidding
i) Auctions will follow a standard process flow: scheduled (upcoming), open and closed.
ii) 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.
iii) 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.
iv) 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.
e) Extensions
i) 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.
ii) Auction extensions are meant to provide a mechanism that is fair for bidders in all time zones to respond to being outbid.

iii) 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.
iv) 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.
f) 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 .LLC 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 Registry. Participants are encouraged therefore to consider carefully each bid submitted as any bid could be a winning bid.

Trademark Claims Service

DOT Registry will offer a Trademark Claims Service indefinitely to provide maximum protection and value to rights holders. The Trademark Claims Service will be monitored and operated by DOT Registry’s RPM Team that will receive all communications regarding the Trademark Claims Service and catalog them. DOT Registry’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 Registry’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 Registry’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 Registry'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 Registry 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 Registry'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 Registry'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 Registry 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 Registry's RPM Team will receive all UDRP Complaints and decisions, and will notify its registrar to cancel or transfer all registrations determined to by a UDRP panel to be infringing within ten (10) business days of receiving the decision. DOT Registry'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 Registry 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 .LLC 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.

DOT Registry will not permit registrants to use proxy services.

Thick WhoIs

DOT 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.

Grace Period

If a Registrant previously awarded a ".LLC" domain is dissolved and⁄or forfeited for any reason, then such ".LLC" domain will be forfeited to DOT Registry at their designated renewal time; unless such Registrant takes all reasonable steps to become reinstated and such Registrant is reinstated within six months of being dissolved and⁄or forfeited.

If a Registrant previously awarded the ".LLC" domain is administratively dissolved by the Secretary of State or legally applicable jurisdiction, then such ".LLC" will be forfeited to DOT Registry at their designated renewal time, unless such Registrant is reinstated within six months of being administratively dissolved.

Takedown Procedure

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

At all times, DOT Registry will publish on its home website at NIC.LLC 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 Registrys RPM Team who will catalogue and ticket in DOT Registry's CRM software and review as outlined herein. DOT Registry 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 Registry's RPM Team. A member of DOT Registry'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 Registry will notify the Complainant of the results of the Complaint within (10) days of receiving the Complaint.

After sending the confirmation email, DOT Registry's RPM Team will review the Complaint. If DOT Registry or its registrar determines that the registration was in bad faith, DOT Registry 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 Registry's RPM Team If DOT Registry's RPM Team is satisfied by the registrant's response that the content has been taken down or is not infringing, DOT Registry's RPM Team will unsuspend the domain name. DOT Registry'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 Registry 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 Registry's response to Question 28.

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

29.1 Rights Protection Mechanisms

DOT Registry 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. ".LLC" 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 ".LLC"'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, ".LLC" 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, ".LLC" 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, ".LLC"'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.

〈TLD'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 ".LLC".

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 ".LLC" 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 24hours of receipt of the complaint from the URS Provider to restrict all changes to the registration data, including transfer and deletion of the domain names.

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

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

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

29.1.4 Policies Handling Complaints Regarding Abuse

In addition the Rights Protection mechanisms addressed above, DOT Registry will implement a number of measures to handle complaints regarding the abusive registration of domain names in its TLD as described in 〈TLD'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. ".LLC"'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

".LLC" 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.

29.2 Safeguards against Unqualified Registrations

IN THE EVENT, ".LLC" IS VERIFYING INFORMATION SUPPLIED BY REGISTRANTS TO ENSURE THAT A REGISTRANT IS QUALIFIED TO REGISTER A DOMAIN, INFORMATION FROM THE APPLICANT SHOULD BE INSERTED IN THIS SECTION. IT IS NOT REQUIRED BY ICANN IN ORDER TO SCORE A 1 MEETS REQUIREMENTS, BUT MAY BE REQUIRED TO GET A SCORE OF 2 ON THIS QUESTION. THIS IS NOT PART OF NEUSTAR'S REGISTRY SERVICES OFFERING.

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⁄En

New gTLD Application Submitted to ICANN by: Dot Registry LLC

String: llp

Originally Posted: 13 June 2012

Application ID: 1-880-35508

Applicant Information

1. Full legal name

Dot Registry LLC

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact nformation Redacted

4. Fax number

Contact nformation Redacted

5. If applicable, website or URL

Primary Contact

6(a). Name

Ms. Tess Pattison-Wade

6(b). Title

Executive Director

6(c). Address

6(d). Phone Number

Contact nformation 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 nformation Redacted

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Limited Liability Company

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

Kansas

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

Christopher Michael Parrott	Director of Finance
Paul Eugene Spurgeon	COO
Scott Adam Schactman	Director Law & 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

Ecyber Solutions Group Inc	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.

llp

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.

To build confidence, trust, reliance and loyalty for consumers and business owners alike by creating a dedicated gTLD to specifically serve the Community of Registered Limited Liability Partnerships. Through our registry service, we will foster consumer peace of mind with confidence by ensuring that all domains bearing our gTLD string are members of the Community of Registered Limited Liability Partnerships. Our verification process will create an unprecedented level of security for online consumers by authenticating each of our registrant's right to conduct business in the United States. The ".LLP" gTLD will fill a unique void in the current DNS and assist in decreasing the burden on existing domain names by identifying members of the Community of Registered Limited Liability Partnerships

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

With the increased popularity of the Internet as a consumer marketplace and the ease with which individuals are able to access information online, it is essential that safeguards be put in place to validate and identify legitimate businesses.

Businesses representing themselves at Limited Liability Partnerships by including LLP in their business names create an expectation amongst consumers that they have the legal right, to conduct business as a Limited Liability Partnership. Unfortunately, consumers are currently unable to quickly verify the accuracy of this representation. Fraudulent business entities rely on this consumer assumption and the lack of available verification resources to prey on both businesses and consumers. As online commerce replaces the brick-and-mortar businesses there has been a corresponding rise in business identity theft online, which in turn creates a lack of consumer confidence.

In the vast majority of states, the Secretary of State is responsible for overseeing the registration of business entities — from the registration of corporations or the verification of business filings, to the administration of the Uniform Commercial Code, an act which provides for the uniform application of business contracts and practices across the United States. The Secretaries' role is critical to the chartering of businesses (including, but not limited to the formation of Limited Liability Partnerships) that wish to operate in their state. In this regard, the Secretaries of State maintain all records of business activities within the state, and in some states, the Secretary of State has wide-ranging regulatory authority over businesses as well.
The ".LLP" gTLD will be exclusively available to members of the Community of Registered Limited Liability Partnerships, as verified through each applicant's Secretary of States Office. By verifying that an applicant is a registered Limited Liability Partnership, DOT Registry will be able to bring unprecedented clarity and security to consumers and business owners, assuring internet users, registry applicants, and others that web addresses ending in ".LLP" are a hallmark of a valid Limited Liability Partnership recognized by a governmental authority of the United States. This process will decrease the possibility of identity misrepresentation in a cyber setting and assist lesser-known businesses in legitimizing their services to consumers.

In January 2012 after many public forums and contributions from consumer advocates, the Business Services Committee of the National Association of Secretary of States (NASS) released the NASS White Paper on Business Identity Theft, indicating that at least 26 states have reported business identity theft cases resulting from fraudulent business representations online. North Carolina Secretary of State Elaine Marshall, who serves as Co-Chair of the NASS Business Services Committee, indicates that the primary function of

the White Paper is to, “Harness new technology to develop cost-effective solutions, and ultimately make it harder for identity thieves to prey upon state-based businesses.”

With the implementation of the “.LLP” gTLD, consumers would have the ability to quickly identify the presented business as a valid US Limited Liability Partnership. As “.LLP” registrations grow, we will see a reduction in the ease with which criminals are able to hide behind fictitious entities because consumers will be conditioned to look for the appropriate gTLD ending before conducting business online. This simple gTLD extension would provide an efficient and cost effective solution to a growing economic concern in the United States by creating the first ever verifiable online business community network. Through this innovative concept, the DNS system will help to build a stronger more resilient business platform for members of the Community of Registered Limited Liability Partnerships, while fostering user confidence, by ensuring accurate business representation.

It is our goal to provide an efficient and secure application process by minimizing the input required by the registrant and creating a streamlined, efficient evaluation process. We will accomplish this by reviewing the applicant’s proof of business registration with their state. Registry Applicants will only be awarded a domain through DOT Registry if the Registrant is an active member of the Community of Registered Limited Liability Partnerships. “Active” in this context can be defined as any Limited Liability Partnership registered with a Secretary of State in the United States and it’s territories, that is determined to be authorized to conduct business within the state at the time of registration. Registrants “Active” status will be verified on an annual basis to ensure the reputation and validity of the “.LLP” gTLD.

DOT Registry will also ensure that registrants are represented by a web address that is both simple and intuitive allowing for easy recognition by search engines and Internet users. Awarded addresses will identify the registrants company and may be presented in the shortest most memorable way.

At DOT Registry, we believe in complete transparency, consistent with the Secretary of State’s Policy with regard to “Active” members of the Community of Registered Limited Liability Partnerships becoming publicly recorded upon completion of their entity registration process. Further, DOT Registry is informed by the position of the Task Force for Financial Integrity and Economic Development, which was created to advocate for improved levels of transparency and accountability in regards to beneficial ownership, control, and accounts of companies. Over the last decade the Task Force has focused specifically on combatting fraudulent business registrations which result in “fake” entities absorbing, hiding and transferring wealth outside the reach of law enforcement agencies. Because of this DOT Registry will not allow private or proxy registrations.

All approved domain registrants will be made public and available, so as to further validate DOT Registry’s mission of fostering consumer peace of mind by creating a gTLD string dedicated solely to valid members of the Community of Registered Limited Liability Partnerships. These transparency mechanisms will also serve as a deterrent for fraudulent entities by creating an expectation among consumers as to who they are conducting business with.

The social implications of business identity theft and consumer confusion are a paramount concern to DOT Registry. In our currently unstable economy, stimulating economic growth is vital. One means to such growth is by defusing the rampant, legitimate fear caused by online crimes and abuse, which leads to curtailed consumer behavior. By introducing the “.LLP” domain into the DNS, DOT Registry will attempt to reduce the social impact of identity theft on business owners which will in turn reduce consumer fears related to spending and ultimately boost economic growth in regards to consumption and purchase power.

Further, the ".LLP" gTLD will strive to foster competition by presenting members of the Community of Registered Limited Liability Partnerships with a highly valued customized domain name that not only represents their business, but also their validity in the marketplace. Within the current existing top-level domains it is hard for businesses to find naming options that appropriately represent them. One advantage of the ".LLP" gTLD is that it will drive the "right" kind of online registrations by offering a valued alternative to the currently overcrowded and often unrestricted name space. Registrants will be inspired to pursue ".LLP" domains not only because they will be guaranteed a name representative to their business, but also because of the increased validity for their business operations brought about by the ".LLP" verification process. DOT Registry anticipates that the security offered through a ".LLP" extension will increase consumer traffic to websites which in turn will boost advertising revenue online and consumer purchasing.
Successful implementation of the ".LLP" domain will require two registration goals: 1) Capture newly formed corporations and assist them in securing a ".LLP" domain appropriate to their legal business name, and 2) converting existing online members of our community to a ".LLP" domain appropriate to their legal business name. These goals will be accomplished by the following practices:
1) Through our Founders Program, DOT Registry will secure key community tenants in the name space who will act as innovative leaders to assist us in changing the online culture of business representation, by promoting the benefits of the ".LLP" gTLD and shaping economic growth through increased consumer confidence.
2) DOT Registry will work closely with companies such as Legalzoom and CSC (both companies assist in the formation of entities and their registration processes), as well as individual Secretary of State's offices to capture newly admitted members of the community.
3) DOT Registry will educate members of the Community of Registered Limited Liability Partnerships on the benefits and importance of using a ".LLP" gTLD by building a strong relationship with organizations like the Small Business Administration and the Better Business Bureau, which promote business validation and consumer insight. By working closely with these well- known and highly regarded entities DOT Registry will be able to reach a larger majority of community members and enhance our message's validity.
4) DOT Registry will strive to create consumer and Internet user awareness through a strong Internet marketing presence and by developing a relationship with the National Association of Consumer Advocates, which was formed with the intention of curbing consumer abuse through predatory business practices.

At DOT Registry, we strive to meet the exact needs of our registrants and the Internet users who patronize them. This will be accomplished by the creation of a seamless connection and strong communication channel between our organization and the governmental authority charged with monitoring the creation and good standing of Limited Liability Partnerships. DOT Registry will work closely with each Secretary of State's office to tailor our validation process to compliment each office's current information systems and to maximize the benefits of accurate information reporting. These processes are essential in fully assisting consumers in making educated decisions in regards to what businesses to patronize. The reach of the ".LLP" gTLD will not only impact online consumerism, but also offer an additional validation process for consumers to research contractors, businesses, and solicitors before choosing to do business with them in person.

The guidelines listed below were developed through collaborations with both NASS and individual Secretary of State's offices in order to ensure the integrity of the ".LLP" domain. All policies comply with ICANN-developed consensus policies.
In order to maintain the integrity of our mission statement and our relationship with each Secretary of State's office we will implement Registration Guidelines. In order to apply for a domain name ending in ".LLP", a Registrant must be registered with one of the Secretary of State's offices in the United States, the District of Columbia, or any of the U.S. possessions or territories as a Limited Liability Partnership pursuant to that jurisdiction's laws on valid corporate registration. In addition, Applicant will implement

the following Registration Guidelines and naming conventions:
1) A Registrant will only be awarded the ".LLP" domain that matches or includes a substantial part of the Registrant's legal name. For example, Blue Star Partners, LLP. would be able to purchase either BlueStarPartners.LLP or BlueStar.LLP.
2) Registrants will not be allowed to register product line registrations, regardless of the products affiliation to the Limited Liability Partnership. All awarded domains must match or include a substantial part of the Registrant's legal name.
3) If there are registrants applying for the same domain names, which correspond to their legal business names as registered in different states, then the ".LLP" domain will be awarded on a first-come, first-served basis to the first registrant.
4) However, if a registrant has a trademark registered with the United States Patent and Trademark Office (USPTO), then such registrant will have priority over any other registrant to be awarded the applied for ".LLP" domain.
5) If a registrant's ".LLP" domain has already been awarded to another registrant with the same or similar legal name, then DOT Registry will offer to award such registrant a ".LLP" domain with a distinctive denominator including but not limited to a tag, company describer, or name abbreviation. For example, if BlueStar.LLP was awarded to Blue Star Partners, LLP. of California, then Blue Star Partners, LLCP. of Kansas would be offered the opportunity to use BlueStarPartners.LLP.
6) DOT Registry will work closely with the Secretary of State's Offices throughout the United States, with NASS and with a number of other agencies and organizations in maintaining the integrity and security of its domain names. DOT Registry will utilize the Secretary of States' data resources to confirm that companies applying for their ".LLP" domain are in fact registered businesses.
7) All registrants that are awarded the ".LLP" domain will agree to a one-year minimum contract for their domain names that will automatically renew for an additional year on an annual basis if such contract is not terminated prior to the expiration of the renewal date.
8) DOT Registry or it's designated agent will annually verify each registrant's community status in order to determine whether or not the entity is still an "Active" member of the community. Verification will occur in a process similar to the original registration process for each registrant, in which each registrant's "Active" Status and registration information will be validated through the proper state authority. In this regard, the following items would be considered violations of DOT Registry's Registration Guidelines, and may result in dissolution of a registrant's awarded ".LLP" domain:
(a) If a registrant previously awarded the ".LLP" domain ceases to be registered with the State.
(b) If a registrant previously awarded a ".LLP" domain is dissolved and⁄or forfeits the domain for any reason.
(c) If a registrant previously awarded the ".LLP" domain is administratively dissolved by the State.
Any registrant found to be "Inactive," or which falls into scenarios (a) through (c) above, will be issued a probationary warning by DOT Registry, allowing for the registrant to restore its active status or resolve its dissolution with its applicable Secretary of State's office. If the registrant is unable to restore itself to "Active" status within the defined probationary period, their previously assigned ".LLP" will be forfeited. DOT Registry reserves the right to change the definition of "Active" in accordance with the policies of the Secretaries of State.

9) If DOT Registry discovers that a registrant wrongfully applied for and was awarded a ".LLP" domain, then such ".LLP" will be immediately forfeited to DOT Registry. Wrongful application includes but is not limited to: a registrant misrepresenting itself as a member of the Community of Registered Limited Liability Partnerships, a registrant participating in illegal or fraudulent actions, or where a registrant would be in violation of our abuse policies described in Question 28 (including promoting or facilitating spam, trademark or copyright infringement, phishing, pharming, willful distribution of malware, fast flux hosting, botnet command and control, distribution of pornography, illegal access to other

computers or networks, and domain kiting/tasting).
10) In the case of domain forfeiture due to any of the above described options, all payments received by the Registrant for registration services to date or in advance payment will be non-refundable.
11) All registration information will be made publicly available. DOT Registry will not accept blind registration or registration by proxy. DOT Registry'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 Registry will provide a Web-based WHOIS application, which will be located at www.whois.LLP. 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.
12) Awarded names are non-transferrable to entities outside of the designated community, regardless of affiliation to any member of the community. In the event that a registrant's business entity merges, is acquired, or sold, the new entity will be allowed to maintain the previously awarded ".LLP" domain until the domain renewal date, at which point they will be evaluated as described in number seven (7) above. Further, any entity acquiring a ".LLP" domain through the processes described in this guideline that does not meet the registration criteria and wishes to maintain the awarded domain will be allowed a grace period after the renewal verification process to correct any non-compliance issues in order to continue operating their acquired domain. If the said entity is unable to comply with DOT Registry's guidelines, the awarded domain will be revoked.
13) If an application is unable to be verified or does not meet the requirements of the sponsored community, the application will be considered invalid.
14) DOT Registry, LLC will implement a reserved names policy consisting of both names DOT Registry wishes to reserve for our own purposes as the registry operator and names protected by ICANN. DOT Registry will respect all ICANN reserved names including, but not limited to, two letter country codes and existing TLD's. Additionally, DOT Registry 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.

In addition to Applicant's comprehensive eligibility, verification, and policing mechanisms, DOT Registry will implement a series of Rights Protection Mechanisms (RPM), including 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; and stringent take down policies and all required dispute resolution policies.

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

.LLP was proposed for the sole purpose of eliminating business and consumer vulnerability in a cyber setting. In order to maintain the integrity of that mission and minimize the negative consequences to consumers and business owners the following policies will be adhered to:

a) No information collected from any registrant 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 correct data inaccuracies as needed.

e) All data will be kept secure.
DOT Registry will strictly uphold the rules set forth in their registration guidelines in order to accurately service the Community of Registered Limited Liability Partnerships and mitigate any negative consequences to consumers or Internet users.
Price structures for the ".LLP" gTLD are designed to reflect the cost of verification within our community requirements and the ongoing cost of operations. Price escalation will only occur to accommodate rising business costs or fees implemented by the Secretaries of State with regard to verifying the "Active" status of a Registrant. Any price increases would be submitted to ICANN as required in our Registry Agreement and will be compiled in a thoughtful and responsible manner, in order to best reduce the affects on both the registrants and the overall retail market.
DOT Registry 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 Registry 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. With regard to Registrars, DOT Registry shall provide financial incentives for pre-authentication of Registrant data prior to such data being passed to the registry. DOT Registry will provide for lower renewal and bulk registration fees in its RRAs for registrations which have been pre-authenticated and which DOT Registry can rely on as accurate data to be entered into its WhoIs database.
Additionally, DOT Registry , through our founders program will provide a 25% discount to founders participants as a participation incentive. It is possible that DOT Registry 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?

Yes

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

DOT Registry plans to serve the Community of Registered Limited Liability Partnerships. Members of the community are defined as businesses registered as Limited Liability Partnerships with the United States or its territories. Limited Liability Partnerships or (LLP's) as they are commonly abbreviated, are specifically designed to represent professional service businesses in the US . Limited Liability Partnerships are commonly adopted by businesses which focus on: accounting, attorneys, architects, dentists, doctors and other fields treated as professionals under each state's law.

Limited Liability Partnerships (LLP) are a relatively new business structure for the United States. LLP's were first recognized in the state of Texas in the 1980's to offer increased protections to individual partners of businesses and combat potential business losses due to mal-practice claims. In 1996 the National Conference of Commissioners on Uniform State Laws adopted the Revised Uniform Partnership Act; providing for both the definition of an LLP and the governmental standards under which an LLP may be formed. It was through the Revised Uniform Partnership Act that a standard set of policies were created to define, validate, and monitor the operations of LLP's, thus creating a unique and accountable business community in the United States.

A Limited Liability Partnership is defined as a partnership in which some or all partners (depending on jurisdiction) have limited liability. LLP's therefore exhibit qualities of both partnerships and corporations. In an LLP, one partner is not responsible or liable for another partner's misconduct or negligence. This distinction is why the LLP is a popular business entity amongst accountants, doctors, and lawyers; which deal heavily with issues that could inspire mal-practice lawsuits.

Common advantages to forming an LLC include:

1) Pass through income taxation to partners, which avoids the "double taxation" often associated with corporations.
2) Limited Liability to individual members. This feature protects individual partners from being responsible for another partners' misconduct or negligence.
3) Unlike a corporation shareholders can actively participate in managing the business.

LLP's represent a small but prestigious sector of business in the United States. DOT Registry believes that due to the specifically personal nature of business operations conducted by LLP's it is essential for consumers to be able to appropriately identify legitimate LLP's prior to using their services. Through the creation of DOT Registry's .LLP string, consumers can quickly validate that they are working with a member of the Community of Registered Limited Liability Partnerships, providing consumers with brand reassurance and peace of mind. DOT Registry believes that it is essential to identify Limited Liability Partnerships online in order to expand on their creditability and further highlight their privilege to conduct business in the US. Proper representation of this community would allow consumers to make educated choices in choosing businesses to patronize and support.

Limited Liability Partnerships can be formed through all but ten states in the United States. Therefore members of this community exist in close to forty US states. LLP formation guidelines are dictated by state law and can vary based on each state's regulations. Persons form an LLP by filing required documents with the appropriate state authority, usually the Secretary of State. Most states require the filing of Articles of Organization. These are considered public documents and are similar to articles of incorporation, which establish a corporation as a legal entity. At minimum, the articles of organization give a brief description of the intended business purposes, the registered agent, and registered business address. Additionally, many states restrict LLP registrations to professional service companies, making the LLP specifically applicable to industries such as architects, accountants, lawyers, and doctors.
LLP's are expected to conduct business in conjunction with the policies of the state in which they are formed, and the Secretary of State periodically evaluates a LLP's level of good standing based on their commercial interactions with both the state and consumers. DOT Registry or its designated agents would verify membership to the Community of Registered Limited Liability Partnerships by collecting data on each Registrant and cross-referencing the information with their applicable registration state. In order to maintain the reputation of the ".LLP" string and accurately delineate the member to consumers, Registrants would only be awarded a domain that accurately represents their registered legal business name. Additionally, DOT Registry will not allow private or proxy

registrations, therefore DOT Registry's WHOIS service will tie directly back to each member's state registration information and will be publicly available in order to provide complete transparency for consumers.
Entities are required to comply with formation practices in order to receive the right to conduct business in the US. Once formed an LLP must be properly maintained. LLP's are expected to comply with state regulations, submit annual filings, and pay specific taxes and fees. Should a Limited Liability Partnership fail to comply with state statutes it could result in involuntary dissolution by the state in addition to imposed penalties, taxes and fees.
While state statutes vary, the majority of states have adopted the following guidelines in regards to the formation of LLP's:

(1) The name of each Limited Liability Partnership must contain the words "Limited Liability Partnership" or the abbreviation "L.L.P" or the designation "LLP".

(2) In order to form a Limited Liability Partnership, two or more authorized persons must execute the Articles of Organization. Which shall contain: the name of the Limited Liability Partnership; the address of the registered office and the name and address of the registered agent for service of process required to be maintained; and any other matters the members determine to include therein.
(3) A Limited Liability Partnership may be organized to conduct or promote any lawful business or purposes, except as may otherwise be provided by the Constitution or other law of this State.
All entities bearing the abbreviation LLP in their business name create the assumption that they have been awarded the privileges associated to that title such as: the ability to conduct commerce transactions within US borders or territories, the ability to market products, solicit consumers and provide reputable services in exchange for monetary values, and finally to provide jobs or employment incentives to other citizens.
Membership in the Community of Registered Limited Liability Partnerships is established through your business entity registration. In order to maintain your membership to this community you must remain an "Active" member of the community. Active" in this context can be defined as any LLP registered with a Secretary of State in the United States and its territories, that is determined to be authorized to conduct business within that State at the time of their registration. Registrant's "Active" status will be verified on an annual basis as described above in question 18 in order to ensure the reputation and validity of the ".LLP" gTLD.
Since LLP's are not currently delineated on the Internet, the creation of this string would mark a unique advancement in consumer security and confidence in the United States. Essentially, this will create the first ever, clear delineator for the Community of Registered Limited Liability Partnerships.

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

DOT Registry is a corporate affiliate of the National Association of Secretaries of State (NASS), an organization which acts as a medium for the exchange of information between states and fosters cooperation in the development of public policy, and is working to develop individual relationships with each Secretary of State's office in order to ensure our continued commitment to honor and respect the authorities of each state.
DOT Registry is acutely aware of our responsibility to uphold our mission statement of: building confidence, trust, reliance, and loyalty for consumers and business owners alike by creating a dedicated gTLD to specifically serve the Community of Registered Limited Liability Partnerships.DOT Registry has also specifically pledged to various Secretaries of State to responsibly manage this gTLD in a manner that will both protect and promote business development in the US. Further our policies were developed through direct

collaboration with the state offices so as to mitigate any possibility of misrepresenting their regulations.

In order to ensure that we accomplish this goal and preserve the credibility of our operations DOT Registry has taken the following advance actions to ensure compliance and community protection:

1) Developed registration policies that are currently reflective of common state law dictating the creation and retention of Limited Liability Partnerships in the United States.

2) Created a strong partnership with CSC (an ICANN approved registrar also specializing in corporate formation services). Through this partnership DOT Registry was able to develop a streamlined verification process to validate potential Registrants as members of the community and ensure that continued annual verifications are completed in a time sensitive and efficient manner. This process will ensure that consumers are not misled by domains registered with the ".LLP" gTLD. Additionally, this process will create peace of mind amongst community members by ensuring that their integrity is not diminished by falsely identified corporations being represented by a ".LLP" extension.

3) Built a strong relationship with several Secretaries of State in order to receive and give consistent input on policy implementation and state regulation updates. DOT Registry has also notified NASS that we have designed our registration policies and procedures to address NASS' concerns about verification requirements in the TLD.

4) Established an in-house legal and policy director to review, enhance, and ensure compliance and consistency with all registration guidelines and community representations.

As indicated in many of the attached endorsement letters, DOT Registry will be held specifically accountable for protecting the integrity of its restrictions and of the members of this community. DOT Registry will consult directly with NASS and policy advisors in the state offices consistently in order to continue to accurately represent the Community of Registered Limited Liability Partnerships and live up to the vast standards associated to the ".LLP" gTLD.

In furtherance of this goal, DOT Registry has attached letters from critical advocates for and representatives of the proposed community, including:

1) Various Secretary of States Offices: Specifically The Secretary of State of Delaware which is widely regarded as a leader in entity formation and policy in the United States and The Secretary of State of South Dakota, which is working towards combatting business identity theft and fictitious business registration.

2) Members of the community including but not limited to Drinker Biddle & Reath, LLP a national law firm specializing in corporate law. Specifically, partners at Drinker Biddle have consulted on many relevant business protection issues and collaborated with organizations such as NASS to form policy and programs to protect businesses in the United States.

DOT Registry can be viewed as an exemplary community representative not only through its pledged commitment to excellence, but also through its continued commitment to build relationships with the state offices charged with registering and overseeing members of this community. DOT Registry pledges through its registry policies to uphold a common standard of evaluation for all applicants and to add increased integrity to the Community of Limited Liability Partnerships. These pledges are further enforced by the endorsement letters from the above organizations, which call the authentication/verification measures proposed by DOT Registry critical to the success of the proposed community.

Similarly, DOT Registry will adhere to all standards of business operations as described in the Kansas state business statutes and will be equally accountable to consumers to deliver continuously accurate findings and valid registrations.

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

The goal of the ".LLP" gTLD is to build confidence, trust, reliance, and loyalty for consumers and business owners alike by creating a dedicated gTLD to specifically serve the Community of Registered Limited Liability Partnerships. Through our registry service, we will foster consumer peace of mind with confidence by ensuring that all domains bearing our gTLD string are members of the Community of Registered Limited Liability Partnerships. Our verification process will create an unprecedented level of security for online consumers by authenticating each of our registrant's right to conduct business in the United States. The ".LLP" gTLD will fill a unique void in the current DNS and assist in decreasing the burden on existing domain names by identifying members of the Registered Community of Limited Liability Partnerships. The creation of the "LLC" gTLD will bring innovation and unprecedented coordination of this valuable service of verification, a purpose endorsed by many individual Secretary of States and NASS. Additionally, ".LLP" will further promote the importance of accurate business registrations in the US, while assisting in combatting business identity theft by increasing registration visibility through our WHOIS services and strict abuse policies.

The intended registrants of the ".LLP" gTLD would consist of members of the Community of Registered Limited Liability Partnerships. This would be verified by collecting data on each Registrant and cross-referencing the information with their applicable registration state. In order to ensure that this process is accomplished in a secure and time effective manner DOT Registry will develop partnerships with each Secretary of State's office in order to create the applicable applications to securely verify registrant data. DOT Registry or it's agents will be solely responsible for managing the verification process in order to decrease the burden on our registrar partners.

End-users for this TLD would include everyday consumers, members of the community, businesses within the community, and consumers looking for more accurate information with regards to those with whom they may conduct business. DOT Registry plans to initiate a robust marketing campaign geared towards the proposed end-users in order to ensure that consumers are aware of what ".LLP" stands for and its significance throughout the Community of Registered Limited Liability Partnerships. In addition to the vast consumer benefits from the creation of the ".LLP" gTLD, DOT Registry believes that ".LLP" domains would be considerably beneficial to business end users. Since DOT Registry will not allow private or proxy registrations businesses viewing ".LLP" sites would be able to instantly ascertain what businesses operate under the blanket of parent companies, are subsidiaries of other businesses, and of course where a corporation is domiciled. This easily identifiable information not only assists businesses in accurately identifying who they are doing business with, it would also assist in locating sales and use tax information, identifying applicable state records, and tracking an entity's history. These factors could help to determine the outcome of sales, mergers, contract negotiations, and business relationships. Ensuring that this kind of transparency and accountability – qualities previously not attainable in a TLD – shall be at the fingertips of potential business partners or investors.

Our registry policies will be adapted to match any changing state statutes in relation to the definition and creation of Limited Liability Partnerships in the U.S., ensuring the longevity and reputation of our registry services and our commitment to consumers to only represent valid U.S. Limited Liability Partnerships. Much like the perpetuity of the members of the Community of Registered Limited Liability Partnerships, the ".LLP" gTLD will enjoy a similar immortality, for as long as LLP entities continue to exist in the United States the ".LLP" relevance will not diminish. As awareness of the gTLD's mission becomes more widely recognized by end-users expectations to understand who you choose to do business with will increase, making the need for the ".LLP" gTLD more prominent.

In addition, it is our concern that the implementation of the gTLD string ".LLP" as a generic string, without the restrictions and community delineations described in this application and endorsed by NASS and the various Secretaries of State, could promote confusion among consumers and provide clever criminal enthusiasts the tools necessary to misrepresent themselves as a U.S.-based corporation. There is an expectation amongst consumers that entities using the words Limited Liability Partnership in their business name have the legal right and ability to conduct business in the United States. This

representation by non-members of the Community of Registered Limited Liability Partnerships is not only fraudulent, but a great disservice to consumers.

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

".LLP" was chosen as our gTLD string because it is the commonly used abbreviation for the entity type that makes up the membership of our community. In the English language Limited Liability Partnership is primarily shortened to LLP when used to delineate business entity types. For example Red Bridge, LLP could additionally be referred to Red Bridge Limited Liability Partnership. Since all of our community members are Limited Liability Partnerships we believed that ".LLP" would be the simplest, most straight forward way to accurately represent our community.

LLP is a recognized abbreviation in all 50 states and US territories denoting the registration type of a business entity. Our research indicates that LLP. as corporate identifier is used in eleven other jurisdictions (Canada, China, Germany, Greece, India, Japan, Kazakhstan, Poland, Romania, Singapore, and the United Kingdom) though their formation regulations are different from the United States and their entity designations would not fall within the boundaries of our community definition.

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

In order to accurately protect the integrity of our domain name and serve the proposed community the following safeguards will be adapted:

1) All Registrants will be required to submit a minimum of: Their registered business address, State of formation, name and contact information of responsible party, and legally registered business name. DOT Registry or its agents will use this information to cross-reference the applicable state's registration records in order to verify the accuracy of the Registrant's application. Should DOT Registry be unable to verify the legitimacy of the Registrants application additional information might be requested in order to award a domain name.
2)A Registrant will only be awarded the ".LLP" domain that matches or includes a substantial part of the Registrant's legal name. For example, Blue Star Partners, LLP. would be able to purchase either BlueStarPartners.LLP or BlueStar.LLP.
3)Registrants will not be allowed to register product line registrations, regardless of the products affiliation to the LLP. All awarded domains must match or include a substantial part of the Registrant's legal name.
4)If there are registrants applying for the same domain names, which correspond to their legal business names as registered in different states, then the ".LLP" domain will be awarded on a first-come, first-served basis to the first registrant.
5)However, if a registrant has a trademark registered with the United States Patent and Trademark Office (USPTO), then such registrant will have priority over any other registrant to be awarded the applied for ".LLP" domain.
6)If a registrant's ".LLP" domain has already been awarded to another registrant with the same or similar legal name, then DOT Registry will offer to award such registrant a ".LLP" domain with a distinctive denominator including but not limited to a tag, company describer, or name abbreviation. For example, if BlueStar.LLP was awarded to Blue Star

Partners, LLP. of California, then Blue Star Partners, LLP. of Kansas would be offered the opportunity to use BlueStarPartners.LLP.
7)DOT Registry will work closely with the Secretary of State's Offices throughout the United States, with NASS and with a number of other agencies and organizations in maintaining the integrity and security of its domain names. DOT Registry will utilize the Secretary of States' data resources to confirm that companies applying for their ".LLP" domain are in fact registered businesses.
8)DOT Registry or it's designated agent will annually verify each registrants community status in order to determine whether or not the entity is still an "Active" member of the community. Verification will occur in a process similar to the original registration process for each registrant, in which each registrant's "Active" Status and registration information will be validated through the proper state authority. In this regard, the following items would be considered violations of DOT Registry's Registration Guidelines, and may result in dissolution of a registrant's awarded ".LLP" domain:
(a) If a registrant previously awarded the ".LLP" domain ceases to be registered with the State.
(b) If a registrant previously awarded a ".LLP" domain is dissolved and⁄or forfeits the domain for any reason.
(c) If a registrant previously awarded the ".LLP" domain is administratively dissolved by the State.
Any registrant found to be "Inactive," or which falls into scenarios (a) through (c) above, will be issued a probationary warning by DOT Registry, allowing for the registrant to restore its active status or resolve its dissolution with its applicable Secretary of State's office. If the registrant is unable to restore itself to "Active" status within the defined probationary period, their previously assigned ".LLP" will be forfeited. DOT Registry reserves the right to change the definition of "Active" in accordance with the policies of the Secretaries of State.
9)If DOT Registry discovers that a registrant wrongfully applied for and was awarded a ".LLP" domain, then such ".LLP" will be immediately forfeited to DOT Registry. Wrongful application includes but is not limited to: a registrant misrepresenting itself as a member of the Community of Registered Limited Liability Partnerships, a registrant participating in illegal or fraudulent actions, or where a registrant would be in violation of our abuse policies described in Question 28 (including promoting or facilitating spam, trademark or copyright infringement, phishing, pharming, willful distribution of malware, fast flux hosting, botnet command and control, distribution of pornography, illegal access to other computers or networks, and domain kiting⁄tasting).
10)All registration information will be made publicly available. DOT Registry will not accept private or proxy registration. DOT Registry'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 Registry will provide a Web-based WHOIS application, which will be located at www.whois.LLP. 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.
11)Awarded names are non-transferrable to entities outside of the designated community, regardless of affiliation to any member of the community. In the event that a registrant's business entity merges, is acquired, or sold, the new entity will be allowed to maintain the previously awarded ".LLP" domain until the domain renewal date, at which point they will be evaluated as described in number seven (7) above. Further, any entity acquiring a ".LLP" domain through the processes described in this guideline that does not meet the registration criteria and wishes to maintain the awarded domain will be allowed a grace period after the renewal verification process to correct any non-compliance issues in order to continue operating their acquired domain. If the said entity is unable to comply with DOT Registry's guidelines, the awarded domain will be revoked.
12)If an application is unable to be verified or does not meet the requirements of the sponsored community, the application will be considered invalid.
In addition to Applicant's comprehensive eligibility, verification, and policing mechanisms, DOT Registry will implement a series of Rights Protection Mechanisms (RPM),

including 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 policies in order to properly operate the registry; and Applicant shall comply with any RRDRP decision, further reinforcing the fact that Applicant is committed to acting in best interest of the community.
DOT Registry will employ an in house Rights Protection Mechanism Team consisting of our Director of Legal and Policy and two additional support personnel. The RPM team will work to mitigate any RPM complaints, while protecting the general rights and integrity of the ",LLP" gTLD. The RPM team will strictly enforce the rights protection mechanisms described in this application.
Membership verification will be performed via DOT Registry's designated agents that which have software systems in place to efficiently interface with each state's data records. By utilizing the resources of industry leaders in this field, DOT Registry will ensure accurate and timely verification in addition to our ability to meet the needs of such a vast community. "Active" status will be specifically verified by cross referencing an applicant's registration data with state records. If this process is unable to be automated at any given time DOT Registry's agents will manually verify the information by contacting the applicable state agencies. While manual verification will obviously employ a larger pool of resources, DOT Registry believes that its industry partners are sufficiently able to accomplish this task based on their employee pool and past business accomplishments. Registrants will be expected to provide a minimum of their legal registered name, state of organization, registered business address, and administrative contact. All additional information required such as proof of organization or "active" status verification will be the sole responsibility of DOT Registry or its designated agents and will be acquired through the processes described herein.
DOT Registry will not restrict the content of ".LLP" sites other then through the enforcement of our Abuse Mitigation practices or Rights Protection Mechanisms as described in question 28 and 29 of this application. All ".LLP" sites will be expected to adhere to the content restrictions described in DOT Registry's abuse policies. Any sites infringing on the legal rights of other individuals or companies, trademarks, or participating in the practice and promotion of illegal activities will be subject to Applicant's take down procedures.
".LLP" domains are designed for the sole use of community members with the intention of promoting their specific business activities. This purpose implies that site content should be restricted to information, products, and services directly related to the Registrants business practices, any Registrants falsely identifying themselves as a community member or inaccurately representing their intentions could be deemed in non-compliance with our registry policies resulting in the revocation of their awarded domain.

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

-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 ".LLP" 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 Registry 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 ".LLP". 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 Registry 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 ”.LLP” 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 Registry, 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 Registry will not be offering services that are unique to ”.LLP”.

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 Registry has partnered with NeuStar, Inc (”Neustar”), an experienced TLD registry operator, for the operation of the ”.LLP” 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 ”.LLP” 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 Registry is mitigating the significant risks and costs associated with the development of a new system. Highlights of the SRS include:

-State-of-the-art, production proven multi-layer design

-Ability to rapidly and easily scale from low to high volume as a TLD grows

-Fully redundant architecture at two sites

-Support for IDN registrations in compliance with all standards

-Use by over 300 Registrars

-EPP connectivity over IPv6

-Performance being measured using 100% of all production transactions (not sampling).

24.2.2 SRS Systems, Software, Hardware, and Interoperability

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

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

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

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

-The IP address of the client

-Timestamp

-Transaction Details

-Processing Time.

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

24.2.3 SRS Design

The SRS incorporates a multi-layer architecture that is designed to mitigate risks and easily scale as volumes increase. The three layers of the SRS are:

-Protocol Layer

-Business Policy Layer

-Database.

Each of the layers is described below.

24.2.4 Protocol Layer

The first layer is the protocol layer, which includes the EPP interface to registrars. It consists of a high availability farm of load-balanced EPP servers. The servers are designed to be fast processors of transactions. The servers perform basic validations and then feed information to the business policy engines as described below. The protocol layer is horizontally scalable as dictated by volume.

The EPP servers authenticate against a series of security controls before granting service, as follows:

-The registrar’s host exchanges keys to initiates a TLS handshake session with the EPP

server.

-The registrar’s host must provide credentials to determine proper access levels.

-The registrar’s IP address must be preregistered in the network firewalls and traffic-shapers.

24.2.5 Business Policy Layer

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

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

The SRS today processes over 30 million EPP transactions daily.

24.2.6 Database

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

Figure 24-1 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 ".LLP" 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 ".LLP".

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 ".LLP" 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 ".LLP" 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 ".LLP" 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 ".LLP" registry.

25. Extensible Provisioning Protocol (EPP)

25.1 Introduction

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

26. Whois

DOT Registry, 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 Registry, 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 Registry, 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 Registry, LLC's WHOIS services will include:

- Fully compliant with all relevant RFCs including 3912;
- Production proven, highly flexible, and scalable (DOT Registry, 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 Registry, 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 Registry, 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 Registry, LLC's registry services operator currently processes millions of WHOIS queries per day.

In addition to the WHOIS Service on port 43, DOT Registry, LLC will provide a Web-based WHOIS application, which will be located at www.whois.llp. 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 Registry, 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 Registry, 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 Registry, 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 Registry, 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 Registry, LLC's information, DOT Registry, 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

”.LLP” 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 ”.LLP”.

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 ”.LLP” registry per the defined ”.LLP” 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 ”.LLP” 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 ".LLP" 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 ".LLP" registry.

-Hold Removes the domain from the DNS zone.

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

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

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

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

The lifecycle of a domain begins with the registration of the domain. All registrations must follow the EPP standard, as well as the specific business rules described in the response to Question 18 above. Upon registration a domain will either be in an active or inactive state. Domains in an active state are delegated and have their delegation information published to the zone. Inactive domains either have no delegation information or their delegation information in not published in the zone. Following the initial registration of a domain, one of five actions may occur during its lifecycle:

-Domain may be updated

-Domain may be deleted, either within or after the add-grace period

-Domain may be renewed at anytime during the term

-Domain may be auto-renewed by the Registry

-Domain may be transferred to another registrar.

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

27.2 Registration States

27.2.1 Domain Lifecycle Registration States

As described above the ".LLP" 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 serverTranferProhibited status. This will cause the transfer request to fail.The domain goes back to its original state.

-DeleteProhibited: The domain is in clientDeleteProhibited and/or serverDeleteProhibited status.This will cause the delete command to fail.The domain goes back to its original state.

Note: the locked state is not represented as a distinct state on the diagram as a domain may be in a locked state in combination with any of the other states: inactive, active, pending transfer, or pending delete.

27.5.1 EPP RFC Consistency

As described above, the domain lifecycle is determined by ICANN policy and the EPP RFCs. Neustar has been operating ICANN TLDs for the past 10 years consistent and compliant with all the ICANN policies and related EPP RFCs.

27.6 Resources

The registration lifecycle and associated business rules are largely determined by policy and business requirements; as such the Product Management and Policy teams will play a critical role in working Applicant to determine the precise rules that meet the requirements of the TLD. Implementation of the lifecycle rules will be the responsibility of Development/Engineering team, with testing performed by the Quality Assurance team.Neustar's SRS implementation is very flexible and configurable, and in many case development is not required to support business rule changes.

The ".LLP" 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 ".LLP" registry.

28. Abuse Prevention and Mitigation

General Statement of Policy

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

Anti-Abuse Policy

DOT Registry 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 Registry with broad power to suspend, cancel, or transfer domain names that violate the Abuse Policy. DOT Registry will publish the Abuse Policy on its home website at NIC.LLP and clearly provide DOT Registry'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 Registry 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 Registry'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 Registry will catalog all abuse

communications in its CRM software using a ticketing system that maintains records of all abuse complaints indefinitely. Moreover, DOT Registry 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 Registry reserves the right to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary to ; (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 Registry, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) to correct mistakes made by the DOT Registry, 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 Registry'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 Registry will take great care to ensure that trademark and copyright infringement does not occur within the .LLP TLD. DOT Registry 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 Registry;
- 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 Registry

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 Registry will provide a domain name anti-abuse procedure modeled after the DMCA's notice-and-takedown procedure.

At all times, DOT Registry will publish on its home website at NIC.LLP 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 Registry's Legal Time who will review and if applicable remedy any Complaint regarding an alleged violation of the Abuse Policy. DOT Registry 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 Registry's CRM software and relayed to DOT Registry's Abuse Team. A member of DOT Registry'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 Registry will notify the Complainant of the results of the Complaint within ten (10) days of receiving the Complaint.

DOT Registry'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 Registry considers the matter closed.

If the quick look does not resolve the matter, DOT Registry's Abuse Team will give the Complaint a full review. Any Registrant that has been determined to be in violation of DOT Registry 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 Registry's Abuse Team will alert it's Registry services team to immediately cancel the resolution of the domain name. DOT Registry'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 Registry's Abuse Team for further review. If DOT Registry's Abuse Team is satisfied by the Registrant's response that the use is not abusive, DOT Registry's Abuse Team will submit a request by the registry services provider to reactivate the domain name. DOT Registry'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 Registry 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 Registry's registry services personnel, DOT Registry 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 Registry 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 Registry will place the domain on "serverHold".

Maintenance of Registration Criteria

If a Registrant previously awarded the ".LLP" domain ceases to be registered with a Secretary of State or legally applicable jurisdiction, such Registrant will be required to forfeit the assigned ".LLP" domain at their designated renewal date.
If DOT Registry discovers that a Registrant wrongfully applied for and was awarded a ".LLP" domain, then such ".LLP" will be immediately forfeited to DOT Registry.
If a Registrant previously awarded a ".LLP" domain is dissolved and⁄or forfeited for any reason, then such ".LLP" domain will be forfeited to DOT Registry at their designated renewal time; unless such Registrant takes all reasonable steps to become reinstated and such Registrant is reinstated within six months of being dissolved and⁄or forfeited.
If a Registrant previously awarded the ".LLP" domain is administratively dissolved by the Secretary of State or legally applicable jurisdiction, then such ".LLP" will be forfeited to DOT Registry at their designated renewal time, unless such Registrant is reinstated within six months of being administratively dissolved.
A Registrant's "Active" Status will be verified annually. Any Registrant not considered "Active" by the definition listed above in question 18 will be given a probationary warning, allowing time for the Registrant to restore itself to "Active" Status. If the Registrant is unable to restore itself to "Active" status within the defined probationary period, their previously assigned ".LLP" will be forfeited. In addition, DOT Registry's definition of "Active" may change in accordance with the policies of the Secretaries of State.

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 Registry has written evidence of actual abuse of orphaned glue, DOT Registry will take action to remove those records from the zone to mitigate such malicious conduct.

DOT Registry’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 Registry 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 Registry 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 Registry will offer thick WhoIs services, in which all authoritative WhoIs data—including contact data—is maintained at the registry. DOT Registry 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 Registry’s registrar will provide DOT Registry with an authorization code to verify eligible Registrants provide accurate Registrant contact information.

In order to further promote WhoIs accuracy, DOT Registry will offer a mechanism whereby third parties can submit complaints directly to the DOT Registry (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 Registry 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 Registry reserves the right to cancel or suspend the applicable domain name(s) should DOT Registry determine that the domains are being used in a manner contrary to DOT Registry’s abuse policy.

DOT Registry shall also require authentication and verification of all Registrant data. DOT Registry 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.

With regard to registrars, DOT Registry shall provide financial incentives for pre-authentication of Registrant data prior to such data being passed to the registry. DOT Registry will provide for lower renewal and bulk registration fees in its RRAs for registrations which have been pre-authenticated and which DOT Registry can rely on as accurate data to be entered into its WhoIs database.

DOT Registry will also maintain historical databases of Registrants and associated information which have provided inaccurate WhoIs information. DOT Registry will endeavor to use this database to uncover patterns of suspicious registrations which DOT Registry 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 Registry's abuse policy.

In addition, DOT Registry'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 Registry 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 Registry 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 Registry reserves the right to suspend the applicable domain name(s) should DOT Registry determine that the Registrant is using the domain in question in a manner contrary to DOT Registry's abuse policy. DOT Registry 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 Registry's registrar. Authentication of modified Registrant information shall be accomplished 48 Hours.

29. Rights Protection Mechanisms

DOT Registry 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 Registry will protect the legal rights of others by implementing RPMs and anti-abuse policies backed by robust responsiveness to complaints and requirements of DOT Registry'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 Registry 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 Registry's domain name registration policy, namely, that all registrants be validly registered corporations and all applied-for domains will only be awarded the ".LLP" domain that matches or includes a substantial part of the Registrant's legal name. DOT Registry will assign its Rights Protection Team; which is lead by our Director of Legal and Policy and further supported by two dedicated employees to receive and authenticate all Sunrise Registrations.

DOT Registry'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 Registry 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-served basis and must be active corporations in good standing before they may be awarded the requested domain, or able to proceed to auction. Upon submission of all of the required information and documentation, registrar will forward the information to DOT Registry's [RPM Team] for authentication. DOT Registry's [RPM Team] will review the information and documentation and 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 Registry will notify its registrar and

the domain name will be released for registration.
DOT Registry will incorporate a Sunrise Dispute Resolution Policy (SDRP). The SRDP 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 Registry'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 Registry'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 Registry considers the matter closed.

If the domain name is not found to have adequately met the SERs, DOT Registry's [RPM Team] will alert the registrar and registry services provider to immediately suspend the resolution of the domain name. Thereafter, DOT Registry'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 Registry's [RPM Team] to determine if the SERs are met. If DOT Registry's [RPM Team] is satisfied by the registrant's response, DOT Registry's [RPM Team] will submit a request to the registrar and the registry services provider to unsuspend the domain name. DOT Registry'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 Registry. 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: Applicant 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.
Any entity, applying for blocks under Sunrise B as a non-member of the sponsored community

cannot apply for names in the TLD.

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 ".LLP" 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 ".LLP" Founder Website, concurrent with the launch of their .LLP Founder Website, said press release must be approved by DOT Registry;
c) Founder's websites should be kept good working order, with unique, meaningful content, user-friendly interfaces, and broad user appeal, for the duration of the License Term,
d) Founders are expected to proactively market and promote ".LLP" gTLD in a manner that is likely to produce widespread awareness of the unique advantages gained through the ".LLP" string.
e) Founders are expected to participate in reasonable joint marketing initiatives with DOT Registry or its Agents, these would be discussed and mutually agreed upon, given the unique circumstances of each marketing venture.
f) Founders will allow DOT Registry 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 Registry's marketing, promotional and communications materials.
DOT Registry 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 Registry 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 Registry's registration guidelines or policies.
Registrants participating in the Founders program will receive 25% off their initial registration fees, additional discounts may be offered to founders at the time of renewal, should DOT Registry choose to offer additional discounts to founders or term extensions (not to exceed 5 years) DOT Registry will seek advance approval from ICANN via the specified channels.

Landrush
Landrush is a limited time opportunity for companies that want to secure a high value ".LLP" 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 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. Since ".LLP" is a sponsored community domain for registered Corporations, 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 A Applicant chooses to register their name regardless of the contention, then the Sunrise B Applicant may choose to pursue further action independently of DOT Registry to contest the name.

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.LLP) then DOT Registry will notify both Applicants of the contention and proceed to an auction process as described in Section 9.

d) If a Sunrise A Applicant and a Landrush Applicant apply for the same domain name, the Sunrise A Applicant, all else being equal will have priority over the Landrush Applicant.

e) If two Sunrise B Applciants apply for the same domain name (i.e., Delta Airlines and Delta Faucet, both seek to block the use of DELTA. LLP), then DOT Registry 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 Registry's rejection. Reconsideration can be requested by completing a reconsideration form and filing a reconsideration fee with DOT Registry. Forms, fee information, and process documentation will be available on the DOT Registry website. Upon receipt of the reconsideration form and the corresponding fee, DOT Registry 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 Registry.

Auctions

Sunrise A names found to be in contention as described above will result in Auction. DOT Registry 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) When your auction account is created, it will be assigned a unique bidder alias in order to ensure confidential bidding. The bidder alias will not reflect any information about your account. You may change your bidder alias to a name of your choosing but once set, it cannot be changed again.

b) All auction participants are expected to keep their account information current, throughout the auction process.

c) Auction participants will receive up to date communication from the auctioneer as the auction progresses, bidding status changes, or issues arise.

d) Bidding

i) Auctions will follow a standard process flow: scheduled (upcoming), open and closed.

ii) 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.

iii) 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.

iv) 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.

e) Extensions

i) 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.
ii) Auction extensions are meant to provide a mechanism that is fair for bidders in all time zones to respond to being outbid.
iii) 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.
iv) 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.
f) 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 .LLP 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 Registry. Participants are encouraged therefore to consider carefully each bid submitted as any bid could be a winning bid.

Trademark Claims Service

DOT Registry will offer a Trademark Claims Service indefinitely to provide maximum protection and value to rights holders. The Trademark Claims Service will be monitored and operated by DOT Registry’s RPM Team that will receive all communications regarding the Trademark Claims Service and catalog them. DOT Registry’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 Registry’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 Registry'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 Registry'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 Registry 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 Registry'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 Registry'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 Registry 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 Registry's RPM Team will receive all UDRP Complaints and decisions, and will notify its registrar to cancel or transfer all registrations determined to by a UDRP panel to be infringing within ten (10) business days of receiving the decision. DOT Registry'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 Registry 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 .LLP 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.

DOT Registry will not permit registrants to use proxy services.

Thick WhoIs

DOT 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.

Grace Period

If a Registrant previously awarded a ".LLP" domain is dissolved and⁄or forfeited for any reason, then such ".LLP" domain will be forfeited to DOT Registry at their designated renewal time; unless such Registrant takes all reasonable steps to become reinstated and such Registrant is reinstated within six months of being dissolved and⁄or forfeited.

If a Registrant previously awarded the ".LLP" domain is administratively dissolved by the Secretary of State or legally applicable jurisdiction, then such ".LLP" will be forfeited to DOT Registry at their designated renewal time, unless such Registrant is reinstated within six months of being administratively dissolved.

Takedown Procedure

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

At all times, DOT Registry will publish on its home website at NIC.LLP 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 Registrys RPM Team who will catalogue and ticket in DOT Registry's CRM software and review as outlined herein. DOT Registry 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 Registry's RPM Team. A member of DOT Registry'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 Registry will notify the Complainant of the results of the Complaint within (10) days of receiving the Complaint.

After sending the confirmation email, DOT Registry's RPM Team will review the Complaint. If DOT Registry or its registrar determines that the registration was in bad faith, DOT Registry 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 Registry's RPM Team If DOT Registry's RPM Team is satisfied by the registrant's response that the content has been taken down or is not infringing, DOT Registry's RPM Team will unsuspend the domain name. DOT Registry'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 Registry 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 Registry's response to Question 28.

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

30.(a).1 Security Policies

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

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 ".LLP" 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 ".LLP". 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 ".LLP" 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

Governmental Advisory Committee

Beijing, People's Republic of China – 11 April 2013

GAC Communiqué – Beijing, People's Republic of China[1]

I. Introduction

The Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) met in Beijing during the week of 4 April 2013. Sixty-one (61) GAC Members participated in the meetings and eight (8) Observers. The GAC expresses warm thanks to the local hosts China Internet Network Information Center (CNNIC), China Organizational Name Administration Center (CONAC), and Internet Society of China for their support.

II. Internal Matters

1. New Members and Observers

The GAC welcomes Belarus, Cape Verde, Côte d'Ivoire, Lebanon, and the Republic of the Marshall Islands to the Committee as members, and The World Meteorological Organisation as an Observer.

2. GAC Secretariat

Following a request for proposals, the GAC received presentations from two organizations and agreed that one such candidate should be providing secretariat services to the GAC, with the aim of becoming operational as soon as possible. Negotiations with such organization will start immediately after the Beijing meeting.

[1] To access previous GAC advice, whether on the same or other topics, past GAC communiqués are available at: https://gacweb.icann.org/display/gacweb/GAC+Recent+Meetings and older GAC communiqués are available at: https://gacweb.icann.org/display/gacweb/GAC+Meetings+Archive.

3. GAC Leadership

The GAC warmly thanks the outgoing Vice-Chairs, Kenya, Singapore, and Sweden and welcomes the incoming Vice-Chairs, Australia, Switzerland and Trinidad & Tobago.

III. Inter-constituencies Activities

1. Meeting with the Accountability and Transparency Review Team 2 (ATRT 2)

The GAC met with the ATRT 2 and received an update on the current activities of the ATRT 2. The exchange served as an information gathering session for the ATRT 2 in order to hear GAC member views on the Review Team processes and areas of interest for governments. The GAC provided input on governmental processes and the challenges and successes that arose during the first round of reviews, and implementation of the GAC related recommendations of the first Accountability and Transparency Review Team.

2. Board/GAC Recommendation Implementation Working Group (BGRI-WG)

The Board–GAC Recommendation Implementation Working Group (BGRI–WG) met to discuss further developments on ATRT1 recommendations relating to the GAC, namely recommendations 11 and 12. In the context of Recommendation 11, the GAC and the Board have concluded the discussion and agreed on the details of the consultation process mandated per ICANN Bylaws, should the Board decide not to follow a GAC advice. With respect to Recommendation 12, on GAC Early Engagement, the BGRI-WG had a good exchange with the GNSO on mechanisms for the GAC to be early informed and provide early input to the GNSO PDP. The BGRI–WG intends to continue this discussion intersessionally and at its next meeting in Durban.

3. Brand Registry Group

The GAC met with the Brand Registry Group and received information on its origins, values and missions.

4. Law Enforcement

The GAC met with law enforcement representatives and received an update from Europol on the Registrar Accreditation Agreement (RAA).

***

The GAC warmly thanks the Accountability and Transparency Review Team 2, the Brand Registry Group, Law Enforcement, and the ICANN Board who jointly met with the GAC as well

as all those among the ICANN community who have contributed to the dialogue with the GAC in Beijing.

IV. GAC Advice to the ICANN Board[2]

1. New gTLDs

a. GAC Objections to Specific Applications

i. The GAC Advises the ICANN Board that:

i. The GAC has reached consensus on GAC Objection Advice according to Module 3.1 part I of the Applicant Guidebook on the following applications:[3].

1. The application for .africa (Application number 1-1165-42560)
2. The application for .gcc (application number: 1-1936-2101)

ii. With regard to Module 3.1 part II of the Applicant Guidebook[4]:

1. The GAC recognizes that Religious terms are sensitive issues. Some GAC members have raised sensitivities on the applications that relate to Islamic terms, specifically .islam and .halal. The GAC members concerned have noted that the applications for .islam and .halal lack community involvement and support. It is the view of these GAC members that these applications should not proceed.

b. Safeguard Advice for New gTLDs

To reinforce existing processes for raising and addressing concerns the GAC is providing safeguard advice to apply to broad categories of strings (see Annex I).

c. Strings for Further GAC Consideration

In addition to this safeguard advice, that GAC has identified certain gTLD strings where further GAC consideration may be warranted, including at the GAC meetings to be held in Durban.

i. Consequently, **the GAC advises the ICANN Board** to: not proceed beyond Initial Evaluation with the following strings : .shenzhen (IDN in Chinese), .persiangulf, .guangzhou (IDN in Chinese), .amazon (and IDNs in Japanese and Chinese), .patagonia, .date, .spa, . yun, .thai, .zulu, .wine, .vin

---

[2] To track the history and progress of GAC Advice to the Board, please visit the GAC Advice Online Register available at: https://gacweb.icann.org/display/gacweb/GAC+Recent+Meetings

[3] Module 3.1: "The GAC advises ICANN that it is the consensus of the GAC that a particular application should not proceed. This will create a strong presumption for the ICANN Board that the application should not be approved.

[4] Module 3.1: "The GAC advises ICANN that there are concerns about a particular application "dot-example." The ICANN Board is expected to enter into dialogue with the GAC to understand the scope of concerns. The ICANN Board is also expected to provide a rationale for its decision.

d. The GAC requests:

i. a written briefing about the ability of an applicant to change the string applied for in order to address concerns raised by a GAC Member and to identify a mutually acceptable solution.

e. Community Support for Applications

The GAC advises the Board:

i. that in those cases where a community, which is clearly impacted by a set of new gTLD applications in contention, has expressed a collective and clear opinion on those applications, such opinion should be duly taken into account, together with all other relevant information.

f. Singular and plural versions of the same string as a TLD

The GAC believes that singular and plural versions of the string as a TLD could lead to potential consumer confusion.

Therefore **the GAC advises the ICANN Board to:**

i. Reconsider its decision to allow singular and plural versions of the same strings.

g. Protections for Intergovernmental Organisations

The GAC stresses that the IGOs perform an important global public mission with public funds, they are the creations of government under international law, and their names and acronyms warrant special protection in an expanded DNS. Such protection, which the GAC has previously advised, should be a priority.

This recognizes that IGOs are in an objectively different category to other rights holders, warranting special protection by ICANN in the DNS, while also preserving sufficient flexibility for workable implementation.

The GAC is mindful of outstanding implementation issues and commits to actively working with IGOs, the Board, and ICANN Staff to find a workable and timely way forward.

Pending the resolution of these implementation issues, the **GAC reiterates its advice to the ICANN Board that:**

i. appropriate preventative initial protection for the IGO names and acronyms on the provided list be in place before any new gTLDs would launch.

2. Registrar Accreditation Agreement (RAA)

Consistent with previous communications to the ICANN Board

a. **the GAC advises the ICANN Board that:**

i. the 2013 Registrar Accreditation Agreement should be finalized before any new gTLD contracts are approved.

The GAC also strongly supports the amendment to the new gTLD registry agreement that would require new gTLD registry operators to use only those registrars that have signed the 2013 RAA.

The GAC appreciates the improvements to the RAA that incorporate the 2009 GAC-Law Enforcement Recommendations.

The GAC is also pleased with the progress on providing verification and improving accuracy of registrant data and supports continuing efforts to identify preventative mechanisms that help deter criminal or other illegal activity. Furthermore the GAC urges all stakeholders to accelerate the implementation of accreditation programs for privacy and proxy services for WHOIS.

3. WHOIS

The GAC urges the ICANN Board to:

a. ensure that the GAC Principles Regarding gTLD WHOIS Services, approved in 2007, are duly taken into account by the recently established Directory Services Expert Working Group.

The GAC stands ready to respond to any questions with regard to the GAC Principles.

The GAC also expects its views to be incorporated into whatever subsequent policy development process might be initiated once the Expert Working Group concludes its efforts.

4. International Olympic Committee and Red Cross /Red Crescent

Consistent with its previous communications, **the GAC advises the ICANN Board to:**

a. amend the provisions in the new gTLD Registry Agreement pertaining to the IOC/RCRC names to confirm that the protections will be made permanent prior to the delegation of any new gTLDs.

5. Public Interest Commitments Specifications

The GAC requests:

b. more information on the Public Interest Commitments Specifications on the basis of the questions listed in annex II.

V. Next Meeting

The GAC will meet during the period of the 47th ICANN meeting in Durban, South Africa.

ANNEX I

Safeguards on New gTLDs

The GAC considers that Safeguards should apply to broad categories of strings. For clarity, this means any application for a relevant string in the current or future rounds, in all languages applied for**.**

The GAC advises the Board that all safeguards highlighted in this document as well as any other safeguard requested by the ICANN Board and/or implemented by the new gTLD registry and registrars should:

- be implemented in a manner that is fully respectful of human rights and fundamental freedoms as enshrined in international and, as appropriate, regional declarations, conventions, treaties and other legal instruments – including, but not limited to, the UN Universal Declaration of Human Rights.
- respect all substantive and procedural laws under the applicable jurisdictions.
- be operated in an open manner consistent with general principles of openness and non-discrimination.

Safeguards Applicable to all New gTLDs

The GAC Advises that the following six safeguards should apply to all new gTLDs and be subject to contractual oversight.

1. **WHOIS verification and checks** —Registry operators will conduct checks on a statistically significant basis to identify registrations in its gTLD with deliberately false, inaccurate or incomplete WHOIS data at least twice a year. Registry operators will weight the sample towards registrars with the highest percentages of deliberately false, inaccurate or incomplete records in the previous checks. Registry operators will notify the relevant registrar of any inaccurate or incomplete records identified during the checks, triggering the registrar's obligation to solicit accurate and complete information from the registrant.

2. **Mitigating abusive activity**—Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.

3. **Security checks**— While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.

4. **Documentation**—Registry operators will maintain statistical reports that provide the number of inaccurate WHOIS records or security threats identified and actions taken as a result of its periodic WHOIS and security checks. Registry operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request in connection with contractual obligations.

5. **Making and Handling Complaints** – Registry operators will ensure that there is a mechanism for making complaints to the registry operator that the WHOIS information is inaccurate or that the domain name registration is being used to facilitate or promote malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.

6. **Consequences** – Consistent with applicable law and any related procedures, registry operators shall ensure that there are real and immediate consequences for the demonstrated provision of false WHOIS information and violations of the requirement that the domain name should not be used in breach of applicable law; these consequences should include suspension of the domain name.

The following safeguards are intended to apply to particular categories of new gTLDs as detailed below.

Category 1

Consumer Protection, Sensitive Strings, and Regulated Markets:

The GAC Advises the ICANN Board:

- Strings that are linked to regulated or professional sectors should operate in a way that is consistent with applicable laws. These strings are likely to invoke a level of implied trust from consumers, and carry higher levels of risk associated with consumer harm. The following safeguards should apply to strings that are related to these sectors:

    1. Registry operators will include in its acceptable use policy that registrants comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.
    2. Registry operators will require registrars at the time of registration to notify registrants of this requirement.
    3. Registry operators will require that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law and recognized industry standards.
    4. Establish a working relationship with the relevant regulatory, or industry self-regulatory, bodies, including developing a strategy to mitigate as much as possible the risks of fraudulent, and other illegal, activities.

5. Registrants must be required by the registry operators to notify to them a single point of contact which must be kept up-to-date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self-regulatory, bodies in their main place of business.

In the current round the GAC has identified the following non-exhaustive list of strings that the above safeguards should apply to:

- **Children:**
  - .kid, .kids, .kinder, .game, .games, .juegos, .play, .school, .schule, .toys
- **Environmental:**
  - .earth, .eco, .green, .bio, .organic
- **Health and Fitness:**
  - .care, .diet, .fit, .fitness, .health, .healthcare, .heart, .hiv, .hospital,, .med, .medical, .organic, .pharmacy, .rehab, .surgery, .clinic, .healthy (IDN Chinese equivalent), .dental, .dentist .doctor, .dds, .physio
- **Financial:**
  - capital, . cash, .cashbackbonus, .broker, .brokers, .claims, .exchange, .finance, .financial, .fianancialaid, .forex, .fund, .investments, .lease, .loan, .loans, .market, . markets, .money, .pay, .payu, .retirement, .save, .trading, .autoinsurance, .bank, .banque, .carinsurance, .credit, .creditcard, .creditunion,.insurance, .insure, ira, .lifeinsurance, .mortgage, .mutualfunds, .mutuelle, .netbank, .reit, .tax, .travelersinsurance, .vermogensberater, .vermogensberatung and .vesicherung.
- **Gambling:**
  - .bet, .bingo, .lotto, .poker, and .spreadbetting, .casino
- **Charity:**
  - .care, .gives, .giving, .charity (and IDN Chinese equivalent)
- **Education:**
  - degree, .mba, .university
- **Intellectual Property**
  - .audio, .book (and IDN equivalent), .broadway, .film, .game, .games, .juegos, .movie, .music, .software, .song, .tunes, .fashion (and IDN equivalent), .video, .app, .art, .author, .band, .beats, .cloud (and IDN equivalent), .data, .design, .digital, .download, .entertainment, .fan, .fans, .free, .gratis, .discount, .sale, .hiphop, .media, .news, .online, .pictures, .radio, .rip, .show, .theater, .theatre, .tour, .tours, .tvs, .video, .zip
- **Professional Services:**
  - .abogado, .accountant, .accountants, .architect, .associates, .attorney, .broker, .brokers, .cpa, .doctor, .dentist, .dds, .engineer, .lawyer, .legal, .realtor, .realty, .vet
- **Corporate Identifiers:**
  - .corp, .gmbh, .inc, .limited, .llc, .llp, .ltda, .ltd, .sarl, .srl, .sal
- **Generic Geographic Terms:**
  - .town, .city, .capital

- .reise, .reisen[5]
- .weather
- .engineering
- .law
- **Inherently Governmental Functions**
    - .army, .navy, .airforce
- In addition, applicants for the following strings should develop clear policies and processes to minimise the risk of cyber bullying/harassment
    - .fail, .gripe, .sucks, .wtf

The GAC further advises the Board:

1. In addition, some of the above strings may require further targeted safeguards, to address specific risks, and to bring registry policies in line with arrangements in place offline. In particular, a limited subset of the above strings are associated with market sectors which have clear and/or regulated entry requirements (such as: financial, gambling, professional services, environmental, health and fitness, corporate identifiers, and charity) in multiple jurisdictions, and the additional safeguards below should apply to some of the strings in those sectors:

6. At the time of registration, the registry operator must verify and validate the registrants' authorisations, charters, licenses and/or other related credentials for participation in that sector.

7. In case of doubt with regard to the authenticity of licenses or credentials, Registry Operators should consult with relevant national supervisory authorities, or their equivalents.

8. The registry operator must conduct periodic post-registration checks to ensure registrants' validity and compliance with the above requirements in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve.

Category 2

<u>Restricted Registration Policies</u>

The GAC advises the ICANN Board:

1. **Restricted Access**
    - As an exception to the general rule that the gTLD domain name space is operated in an open manner registration may be restricted, in particular for strings mentioned under category 1

[5] Austria, Germany, and Switzerland support requirements for registry operators to develop registration policies that allow only travel-related entities to register domain names. Second Level Domains should have a connection to travel industries and/or its customers

above. In these cases, the registration restrictions should be appropriate for the types of risks associated with the TLD. The registry operator should administer access in these kinds of registries in a transparent way that does not give an undue preference to any registrars or registrants, including itself, and shall not subject registrars or registrants to an undue disadvantage.

2. Exclusive Access

- For strings representing generic terms, exclusive registry access should serve a public interest goal.

  - In the current round, the GAC has identified the following non-exhaustive list of strings that it considers to be generic terms, where the applicant is currently proposing to provide exclusive registry access

    - .antivirus, .app, .autoinsurance, .baby, .beauty, .blog, .book, .broker, .carinsurance, .cars, .cloud, .courses, .cpa, .cruise, .data, .dvr, .financialaid, .flowers, .food, .game, .grocery, .hair, .hotel, .hotels .insurance, .jewelry, .mail, .makeup, .map, .mobile, .motorcycles, .movie, .music, .news, .phone, .salon, .search, .shop, .show, .skin, .song, .store, .tennis, .theater, .theatre, .tires, .tunes, .video, .watches, .weather, .yachts, .クラウド [cloud], .ストア [store], .セール [sale], .ファッション [fashion], .家電 [consumer electronics], .手表 [watches], .書籍 [book], .珠宝 [jewelry], .通販 [online shopping], .食品 [food]

ANNEX II

List of questions related to Public Interest Commitments Specifications

1. Could a third party intervene or object if it thinks that a public interest commitment is not being followed? Will governments be able to raise those sorts of concerns on behalf of their constituents?

2. If an applicant does submit a public interest commitment and it is accepted are they able to later amend it? And if so, is there a process for that?

3. What are ICANN's intentions with regard to maximizing awareness by registry operators of their commitments?

4. Will there be requirements on the operators to maximize the visibility of these commitments so that stakeholders, including governments, can quickly determine what commitments were made?

5. How can we follow up a situation where an operator has not made any commitments? What is the process for amending that situation?

6. Are the commitments enforceable, especially later changes? Are they then going into any contract compliance?

7. How will ICANN decide whether to follow the sanctions recommended by the PIC DRP? Will there be clear and transparent criteria? Based on other Dispute Resolution Procedures what is the expected fee level?

8. If serious damage has been a result of the past registration policy, will there be measures to remediate the harm?