Annex 1.

Little Birch, LLC
Contact Information Redacted

Mr. Jon Nevett
Ms. Crystal Ondo
Contact Information Redacted

Minds + Machines Group Limited
Contact Information Redacted

Ms. Reg Levy
Contact Information Redacted

THIS DOCUMENT IS IMPORTANT AND REQUIRES YOUR IMMEDIATE ATTENTION. If you are in any doubt about the contents of this Document, or the action you should take, you should consult a person authorised under the Financial Services and Markets Act 2000 who specialises in advising on the acquisition of shares and other securities in the United Kingdom before taking any action.

Defined terms in this Document have the meanings given on pages 8 to 13, unless the context requires otherwise. Application will be made for the Shares to be readmitted to trading on AIM. **AIM is a market designed primarily for emerging or smaller companies to which a higher investment risk tends to be attached than to larger or more established companies. AIM securities are not admitted to the Official List of the United Kingdom Listing Authority. A prospective investor should be aware of the risks of investing in such companies and should make the decision to invest only after careful consideration and, if appropriate, consultation with an independent financial advisor. The London Stock Exchange Plc has not itself examined or approved the contents of this Document. Each AIM company is required pursuant to the AIM Rules for Companies to have a nominated adviser. The nominated adviser is required to make a declaration to the London Stock Exchange on admission to the market in the form set out in Schedule Two to the AIM Rules for Companies.** Admission is expected to become effective and dealings in the Ordinary Shares to recommence on AIM on or around 20 March 2014.

This Document, which comprises an AIM admission document, has been drawn up in accordance with the AIM Rules. This document does not constitute an offer to the public in accordance with the provisions of section 85 of FSMA. Accordingly, this Document has not been prepared in accordance with the Prospectus Rules, nor has it been approved by the FCA pursuant to section 85 of FSMA and a copy has not been delivered to the FCA under rule 3.2 of the Prospectus Rules.

The Directors, whose names appear on page 6 of this Document, accept full responsibility, collectively and individually, for the Company's compliance with the AIM Rules and the Company and the Directors accept responsibility for the information contained in this Document. To the best of the knowledge and belief of the Company and the Directors (who have taken all reasonable care to ensure that such is the case) the information contained in this Document is in accordance with the facts and contains no omission likely to affect its import.

Top Level Domain Holdings Limited

(Incorporated and registered in the British Virgin Islands with registered number 1412814)

Readmission of the Shares to trading on AIM

and

Change of name to

Minds + Machines Group Limited

Nominated Adviser	***Broker***
Beaumont Cornish Limited	N+1 Singer

Shares immediately following Readmission

Issued and fully paid Shares of no par value

825,558,522

The Shares will not be registered under the United States Securities Act of 1933, as amended, or under the securities legislation of, or with any securities regulatory authority of, any state or other jurisdiction of the United States or under the applicable securities laws of the Republic of South Africa, Australia, Canada, Republic of Ireland or Japan. The distribution of this Document in certain jurisdictions may be restricted by law. In particular, this Document should not be distributed, published, reproduced or otherwise made available in whole or in part, or disclosed by recipients to any other person, and in particular, should not be distributed to persons with addresses in the United States of America, the Republic of South Africa, Australia, Canada, Republic of Ireland or Japan and, subject to certain exceptions, the Shares may not be offered or sold, directly or indirectly, or to or for the account or benefit of any national, resident or citizen in or into those jurisdictions. This document does not constitute an offer to issue or sell, or the solicitation of an offer to subscribe for or buy, any of the Shares to any person in any jurisdiction to whom it is unlawful to make such offer or solicitation in such jurisdiction. No action has been taken by the Company or by Beaumont Cornish that would permit an offer of any of the Shares or possession or distribution of this Document where action for that purpose is required. Persons into whose possession this Document comes should inform themselves about, and observe, any such restrictions. Any failure to comply with these restrictions may constitute a violation of the securities laws of such jurisdictions.

Beaumont Cornish is authorised and regulated in the United Kingdom by the FCA and is acting as Nominated Adviser for the purposes of the AIM Rules exclusively for the Company and no one else in connection with the matters described herein and will not be responsible to any other person for providing the protections afforded to customers of Beaumont Cornish, or for advising any other person on the contents of this Document or any matter referred to herein. The responsibilities of Beaumont Cornish, as Nominated Adviser, are owed solely to the London Stock Exchange and are not owed to the Company or to any Director or Shareholder or to any other subsequent purchaser of any of the Shares and accordingly no duty of care is accepted in relation to them. No representation or warranty, express or implied, is made by Beaumont Cornish as to, and no liability whatsoever is accepted by Beaumont Cornish in respect of, any of the contents of this Document (without limiting the statutory rights of any person to whom this Document is issued).

N+1 Singer, which is authorised and regulated in the United Kingdom by the FCA, is the Company's broker for the purposes of the AIM Rules. N+1 Singer are acting for the Company and no one else and will not be responsible to any other person for providing the protections afforded to customers of N+1 Singer nor for providing advice in relation to the contents of this Document or any matter referred to herein. No representation or warranty, express or implied is made by N+1 Singer for the accuracy of any information or opinions contained in this Document or for the omission of any material information, for which it is not responsible.

Copies of this Document will be available free of charge during normal business hours on any Business Day at the offices of Beaumont Cornish, 2nd Floor, Bowman House, 29 Wilson Street, London EC2M 2SJ from the date of this Document and for a period of at least one month following Admission.

Notice of a Meeting of Shareholders to be held at 10.00 a.m. GMT at the office of Kerman & Co. Solicitors, Fitzwilliam Hall, Fitzwilliam Place, Dublin 2, Ireland on 19 March 2014 is set out at the end of this Document. A Form of Proxy for holders of Shares for use in connection with the Meeting of Shareholders accompanies this Document and, to be valid, must be completed and lodged with Computershare Investor Services (Jersey) Limited, c/o Computershare Investor Services PLC, The Pavilions, Bridgwater Road, Bristol BS99 6ZY or sent by fax to 00 44 870 703 6322 as soon as possible but in any event to be received not later than 10.00 a.m. GMT on 17 March 2014 or 48 hours before any adjourned meeting. A Form of Instruction for holders of Depositary Interests for use in connection with the Meeting of Shareholders accompanies this Document and, to be valid, must be completed and lodged with Computershare Investor Services PLC, The Pavilions, Bridgwater Road, Bristol BS99 6ZY or sent by fax to 00 44 870 703 6322 as soon as possible but in any event to be received not later than 10.00 a.m. GMT on 16 March 2014 or 72 hours before any adjourned meeting. Completion of a Form of Proxy or a Form of Instruction will not preclude a Shareholder from attending and voting at the Meeting of Shareholders in person save that in each case the Shareholder should contact Computershare Investor Services PLC in advance to confirm what identity documents they should bring with them and to complete a form of representation (available on request from Computershare Company Nominees Limited) if necessary.

You should read the whole text of this Document. An investment in the Company involves a significant degree of risk, may result in the loss of the entire investment and may not be suitable for all recipients of this Document. Your attention is drawn to Part III of this Document which sets out certain risk factors relating to any investment in the Company. All statements regarding the Company's business, financial position and prospects should be viewed in the light of the risk factors set out in Part III of this Document.

FORWARD LOOKING STATEMENTS

Certain statements in this Document are "Forward Looking Statements." These Forward Looking Statements are not based on historical facts but rather on the Directors' expectations regarding the Company's future growth, results of operations, performance, future capital and other expenditures (including the amount, nature and sources of funding thereof), competitive advantages, business prospects and opportunities. Such Forward Looking Statements reflect management's current beliefs and assumptions and are based on information currently available to management. Forward Looking Statements involve significant known and unknown risks and uncertainties. A number of factors could cause actual results to differ materially from the results discussed in the Forward Looking Statements including risks associated with vulnerability to general economic market and business conditions, competition, environmental and other regulatory changes, actions by governmental authorities, the availability of capital markets, reliance on key personnel, uninsured and underinsured losses and other factors, many of which are beyond the control of the Company. Although the Forward Looking Statements contained in this Document are based upon what management believes to be reasonable assumptions the Company cannot assure investors that actual results will be consistent with these Forward Looking Statements.

NOTICE TO RESIDENTS OF THE UNITED STATES

This Document is in respect of securities of a British Virgin Islands company filing an application for all of the issued and to be issued Shares to be readmitted to trading on AIM, and has been created under the disclosure regime provided by the AIM Rules for Companies, which is materially different to disclosure prepared in accordance with US law. As noted above, because this Document does not constitute an offer to the public in accordance with UK provisions, this Document has not been prepared under the retail investor oriented Prospectus Rules made under section 73 of FSMA. If you are a US investor you should not use this Document to assess whether to make an investment in the Company.

An application for the registration of securities on AIM is not subject to the rules governing the registration of securities under the United States Securities Act of 1933, as amended, nor those of the US states. Neither the Securities and Exchange Commission nor any other US or state securities commission nor regulatory authority has approved of or passed an opinion on the accuracy or adequacy of this Document. Any representation to the contrary is a criminal offence. Any financial information regarding the Company or its subsidiaries included in this Document has been prepared in accordance with

International Financial Reporting Standards ("IFRS") that may not be comparable to the financial statements of US companies. US generally accepted accounting principles differ in many respects from IFRS. None of the financial information included in this Document has been audited in accordance with auditing standards generally accepted in the United States or the auditing standards of the Public Company Accounting Oversight Board (United States). Shareholders who are US persons may have difficulty in enforcing any rights or claims that they may have arising under US federal or state securities laws in respect of the document or their holding of any Shares, as the Company is located in a country other than the United States and many of its officers and directors are residents of countries other than the United States. US holders of Shares may not be able to sue a non-US company or its officers or directors in a non-US court for violations of US securities laws. Further, to compel a non-US company and its affiliates to subject themselves to a US court's judgment may be difficult.

Holders subject to tax in the United States are strongly urged to contact their tax advisers about the consequences of holding Shares including the potential applicability of special rules concerning US shareholders of non-US corporations. You should note that, at this time, the Company does not intend to make special accommodations regarding its financial information to assist holders with their US tax obligations. This present intention may cause additional difficulty to US holders when attempting to assess the tax profile of the Shares.

Annex 2.

New gTLD Application Submitted to ICANN by: Little Birch, LLC

String: eco

Originally Posted: 13 June 2012

Application ID: 1-1434-1370

Applicant Information

1. Full legal name

Little Birch, LLC

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact Information Redacted

4. Fax number

Contact Information Redacted

5. If applicable, website or URL

Primary Contact

6(a). Name

Daniel Schindler

6(b). Title

EVP, Donuts Inc.

6(c). Address

6(d). Phone Number

Contact Information Redacted

6(e). Fax Number

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Jonathon Nevett

7(b). Title

EVP, Donuts Inc.

7(c). Address

7(d). Phone Number

Contact Information Redacted

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Limited Liability Company

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

Delaware.

http://delcode.delaware.gov/title6/c018/sc01/index.shtml

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

Attachments are not displayed on this form.

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

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

Covered TLD, LLC

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

Applicant Background

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

N/A	N/A

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

N/A	N/A

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

Covered TLD, LLC	N/A

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

Paul Stahura	CEO, Donuts Inc.

Applied-for gTLD string

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

eco

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

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

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

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

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

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

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

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

Attachments are not displayed on this form.

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

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

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

Donuts has conducted technical analysis on the applied-for string, and concluded that there are no known potential operational or rendering issues associated with the string.

The following sections discuss the potential operational or rendering problems that can arise, and how Donuts mitigates them.

## Compliance and Interoperability

The applied-for string conforms to all relevant RFCs, as well as the string requirements set forth in Section 2.2.1.3.2 of the Applicant Guidebook.

## Mixing Scripts

If a domain name label contains characters from different scripts, it has a higher likelihood of encountering rendering issues. If the mixing of scripts occurs within the top-level label, any rendering issue would affect all domain names registered under it. If occurring within second level labels, its ill-effects are confined to the domain names with such labels.

All characters in the applied-for gTLD string are taken from a single script. In addition, Donuts's IDN policies are deliberately conservative and compliant with the ICANN Guidelines for the Implementation of IDN Version 3.0. Specifically, Donuts does not allow mixed-script labels to be registered at the second level, except for languages with established orthographies and conventions that require the commingled use of multiple scripts, e.g. Japanese.

## Interaction Between Labels

Even with the above issue appropriately restricted, it is possible that a domain name composed of labels with different properties such as script and directionality may introduce unintended rendering behaviour.

Donuts adopts a conservative strategy when offering IDN registrations. In particular, it ensures that any IDN language tables used for offering IDN second level registrations involve only scripts and characters that would not pose a risk when combined with the top level label.

## Immature Scripts

Scripts or characters added in Unicode versions newer than 3.2 (on which IDNA2003 was based) may encounter interoperability issues due to the lack of software support.

Donuts does not currently plan to offer registration of labels containing such scripts or characters.

## Other Issues

To further contain the risks of operation or rendering problems, Donuts currently does not offer registration of labels containing combining characters or characters that require IDNA contextual rules handling. It may reconsider this decision in cases where a language has a clear need for such characters.

Donuts understands that the following may be construed as operational or rendering issues, but considers them out of the scope of this question. Nevertheless, it will take reasonable steps to protect registrants and Internet users by working with vendors and relevant language communities to mitigate such issues.

- missing fonts causing string to fail to render correctly; and
- universal acceptance of the TLD;

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

Mission/Purpose

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

Q18A CHAR: 6671

ABOUT DONUTS
Donuts Inc. is the parent applicant for this and multiple other TLDs. The company intends to increase competition and consumer choice at the top level. It will operate these carefully selected TLDs safely and securely in a shared resources business model. To achieve its objectives, Donuts has recruited seasoned executive management with proven track records of excellence in the industry. In addition to this business and operational experience, the Donuts team also has contributed broadly to industry policymaking and regulation, successfully launched TLDs, built industry-leading companies from the ground up, and brought innovation, value and choice to the domain name marketplace.

THE .ECO TLD
This TLD is attractive and useful to end-users as it better facilitates search,

self-expression, information sharing and the provision of legitimate goods and services. Along with the other TLDs in the Donuts family, this TLD will provide Internet users with opportunities for online identities and expression that do not currently exist. In doing so, the TLD will introduce significant consumer choice and competition to the Internet namespace – the very purpose of ICANN’s new TLD program.

This TLD is a generic term and its second level names will be attractive to a variety of Internet users. Making this TLD available to a broad audience of registrants is consistent with the competition goals of the New TLD expansion program, and consistent with ICANN’s objective of maximizing Internet participation. Donuts believes in an open Internet and, accordingly, we will encourage inclusiveness in the registration policies for this TLD. In order to avoid harm to legitimate registrants, Donuts will not artificially deny access, on the basis of identity alone (without legal cause), to a TLD that represents a generic form of activity and expression.

.ECO is a versatile and attractive string that appeals to a broad and diverse group of registrants and users. This includes individuals and organizations interested in issues relating to the natural environment, scientific research, and environmental protection. The term also is useful to those involved in fundraising, publishing, information sharing, and other functions related to environmental causes. Many who are interested in environmental issues are not members of formal or organized groups, and thus the term is very broadly applicable to those who are interested in using .ECO registrations as a forum of expression or other function. The term ECO, further, has dozens of alternate and established meanings, including acronyms and other means of usage. Accordingly, we would operate this TLD inclusively and with this diverse group of users in mind, and in a secure and legitimate manner on behalf of all registrants.

DONUTS’ APPROACH TO PROTECTIONS

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

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

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

OUR PROTECTIONS

Donuts has consulted with and evaluated the ideas of international law enforcement, consumer privacy advocacy organizations, intellectual property interests and other Internet industry groups to create a set of protections that far exceed those in existing TLDs, and bring to the Internet namespace nearly two dozen new rights and protection mechanisms to raise user safety and protection to a new level.

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

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

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

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

DONUTS’ INTENTION FOR THIS TLD
As a senior government authority has recently said, “a successful applicant is entrusted with operating a critical piece of global Internet infrastructure.” Donuts’ plan and intent is for this TLD to serve the international community by bringing new users online through opportunities for economic growth, increased productivity, the exchange of ideas and information and greater self-expression.

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

Q18B CHAR: 8712

DONUTS’ PLACE WITHIN ICANN’S MISSION
ICANN and the new TLD program share the following purposes:
1. to make sure that the Internet remains as safe, stable and secure as possible, while
2. helping to ensure there is a vibrant competitive marketplace to efficiently bring the benefits of the namespace to registrants and users alike.

ICANN harnesses the power of private enterprise to bring forth these public benefits. While pursuing its interests, Donuts helps ICANN accomplish its objectives by:

1. Significantly widening competition and choice in Internet identities with hundreds of new top-level domain choices;

2. Providing innovative, robust, and easy-to-use new services, names and tools for users, registrants, registrars, and registries while at the same time safeguarding the rights of others;
3. Designing, launching, and securely operating carefully selected TLDs in multiple languages and character sets; and
4. Providing a financially robust corporate umbrella under which its new TLDs will be protected and can thrive.

ABOUT DONUTS’ RESOURCES
Donuts’ financial resources are extensive. The company has raised more than US$100 million from a number of capital sources including multiple multi-billion dollar venture capital and private equity funds, a top-tier bank, and other well-capitalized investors. Should circumstances warrant, Donuts is prepared to raise additional funding from current or new investors. Donuts also has in place pre-funded, Continued Operations Instruments to protect future registrants. These resource commitments mean Donuts has the capability and intent to launch, expand and operate its TLDs in a secure manner, and to properly protect Internet users and rights-holders from potential abuse.

Donuts firmly believes a capable and skilled organization will operate multiple TLDs and benefit Internet users by:

1. Providing the operational and financial stability necessary for TLDs of all sizes, but particularly for those with smaller volume (which are more likely to succeed within a shared resources and shared services model);
2. Competing more powerfully against incumbent gTLDs; and
3. More thoroughly and uniformly executing consumer and rights holder protections.

Donuts will be the industry leader in customer service, reputation and choice. The reputation of this, and other TLDs in the Donuts portfolio, will be built on:
1. Our successful launch and marketplace reach;
2. The stability of registry operations; and
3. The effectiveness of our protection mechanisms.

THE GOAL OF THIS TLD

This and other Donuts TLDs represent discrete segments of commerce and human interest, and will give Internet users a better vehicle for reaching audiences. In reviewing potential strings, we deeply researched discrete industries and sectors of human activity and consulted extensive data sources relevant to the online experience. Our methodology resulted in the selection of this TLD – one that offers a very high level of user utility, precision in content delivery, and ability to contribute positively to economic growth.

SERVICE LEVELS

Donuts will endeavor to provide a service level that is higher than any existing TLD. Donuts’ commitment is to meet and exceed ICANN-mandated availability requirements, and to provide industry-leading services, including non-mandatory consumer and rights protection mechanisms (as described in answers to Questions 28, 29, and 30) for a beneficial customer experience.

REPUTATION

As noted, Donuts management enjoys a reputation of excellence as domain name industry contributors and innovators. This management team is committed to the successful expansion of the Internet, the secure operation of the DNS, and the creation of a new segment of the web that will be admired and respected.

The Donuts registry and its operations are built on the following principles:

1. More meaningful product choice for registrants and users;
2. Innovative services;
3. Competitive pricing; and
4. A more secure environment with better protections.

These attributes will flow to every TLD we operate. This string’s reputation will develop as a compelling product choice, with innovative offerings, competitive pricing, and safeguards for consumers, businesses and other users.

Finally, the Donuts team has significant operational experience with registrars, and will collaborate knowledgeably with this channel to deliver new registration opportunities to end-users in way that is consistent with Donuts principles.

NAMESPACE COMPETITION

This TLD will contribute significantly to the current namespace. It will present multiple new domain name alternatives compared to existing generic and country code TLDs. The DNS today offers very limited addressing choices, especially for registrants who seek a specific identity.

INNOVATION

Donuts will provide innovative registration methods that allow registrants the opportunity to secure an important identity using a variety of easy-to-use tools that fit individual needs and preferences.

Consistent with our principle of innovation, Donuts will be a leader in rights protection, shielding those that deserve protection and not unfairly limiting or directing those that don’t. As detailed in this application, far-reaching protections will be provided in this TLD. Nevertheless, the Donuts approach is inclusive, and second level registrations in this TLD will be available to any responsible registrant with an affinity for this string. We will use our significant protection mechanisms to prevent and eradicate abuse, rather than attempting to do so by limiting registrant eligibility.

This TLD will contribute to the user experience by offering registration alternatives that better meet registrants’ identity needs, and by providing more intuitive methods for users to locate products, services and information. This TLD also will contribute to marketplace diversity, an important element of user experience. In addition, Donuts will offer its sales channel a suite of innovative registration products that are inviting, practical and useful to registrants.

As noted, Donuts will be inclusive in its registration policies and will not limit registrant eligibility at the second level at the moment of registration. Restricting access to second level names in this broadly generic TLD would cause more harm than benefit by denying domain access to legitimate registrants. Therefore, rather than artificially limiting registrant access, we will control abuse by carefully and uniformly implementing our extensive range of user and rights protections.

Donuts will not limit eligibility or otherwise exclude legitimate registrants in second level names. Our primary focus will be the behavior of registrants, not their identity.

Donuts will specifically adhere to ICANN-required registration policies and will comply with all requirements of the Registry Agreement and associated specifications regarding registration policies. Further, Donuts will not tolerate abuse or illegal activity in this TLD, and will have strict registration policies that provide for remediation and takedown as necessary.

Donuts TLDs will comply with all applicable laws and regulations regarding privacy and data protection. Donuts will provide a highly secure registry environment for registrant and user data (detailed information on measures to protect data is available in our technical response).

Donuts will permit the use of proxy and privacy services for registrations in this TLD, as there are important, legitimate uses for such services (including free speech rights and the avoidance of spam). Donuts will limit how such proxy and privacy services are offered (details on these limitations are provided in our technical response). Our approach balances the needs of legitimate and responsible registrants with the need to identify registrants who illegally use second level domains.

Donuts will build on ICANN's outreach and media coverage for the new TLD Program and will initiate its own effort to educate Internet users and rights holders about the launch of this TLD. Donuts will employ three specific communications efforts. We will:

1. Communicate to the media, analysts, and directly to registrants about the Donuts enterprise.
2. Build on existing relationships to create an open dialogue with registrars about what to expect from Donuts, and about the protections required by any registrar selling this TLD.
3. Communicate directly to end-users, media and third parties interested in the attributes and benefits of this TLD.

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

Q18C Standard CHAR: 1440

Generally, during the Sunrise phase of this TLD, Donuts will conduct an auction if there are two or more competing applications from validated trademark holders for the same second level name. Alternatively, if there is a defined trademark classification reflective of this TLD, Donuts may give preference to second-level applicants with rights in that classification of goods and services. Post-Sunrise, requests for registration will generally be on a first-come, first-served basis.

Donuts may offer reduced pricing for registrants interested in long-term registration, and potentially to those who commit to publicizing their use of the TLD. Other advantaged pricing may apply in selective cases, including bulk purchase pricing.

Donuts will comply with all ICANN-related requirements regarding price increases: advance notice of any renewal price increase (with the opportunity for existing registrants to renew for up to ten years at their current pricing); and advance notice of any increase in initial registration pricing.

The company does not otherwise intend, at this time, to make contractual commitments regarding pricing. Donuts has made every effort to correctly price its offerings for end-user value prior to launch. Our objective is to avoid any disruption to our customers after they have registered. We do not plan or anticipate significant price increases over time.

Community-based Designation

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

No

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

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

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

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

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

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

Attachments are not displayed on this form.

Geographic Names

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

No

Protection of Geographic Names

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

Q22 CHAR: 4979

As previously discussed (in our response to Q18: Mission ⁄ Purpose) Donuts believes in an open Internet. Consistent with this we also believe in an open DNS, where second level domain names are available to all registrants who act responsibly.

The range of second level names protected by Specification 5 of the Registry Operator contract is extensive (approx. 2,000 strings are blocked). This list resulted from a lengthy process of collaboration and compromise between members of the ICANN community, including the Governmental Advisory Committee. Donuts believes this list represents a healthy balance between the protection of national naming interests and free speech on the Internet.

Donuts does not intend to block second level names beyond those detailed in Specification 5. Should a geographic name be registered in this TLD and used for illegal or abusive activity Donuts will remedy this by applying the array of protections implemented in this TLD. (For details about these protections please see our responses to Questions 18, 28, 29 and 30).

Donuts will strictly adhere to the relevant provisions of Specification 5 of the New gTLD Agreement. Specifically:

1. All two-character labels will be initially reserved, and released only upon agreement between Donuts and the relevant government and country code manager.
2. At the second level, country and territory names will be reserved at the second and other levels according to these standards:
2.1. Short form (in English) of country and territory names documented in the ISO 3166-1 list;
2.2. Names of countries and territories as documented by the United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World; and
2.3. The list of United Nations member states in six official UN languages, as prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names.
Donuts will initially reserve country and territory names at the second level and at all other levels within the TLD. Donuts supports this requirement by using the

following internationally recognized lists to develop a comprehensive master list of all geographic names that are initially reserved:

1. The short form (in English) of all country and territory names contained on the ISO 3166-1 list, including the European Union, which is exceptionally reserved on the ISO 3166-1 List, and its scope extended in August 1999 to any application needing to represent the name European Union [http:⁄⁄www.iso.org⁄iso⁄support⁄country_codes⁄iso_3166_code_lists⁄iso-3166-1_decoding_table.htm#EU].

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

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

4. The 2-letter alpha-2 code of all country and territory names contained on the ISO 3166-1 list, including all reserved and unassigned codes

This comprehensive list of names will be ineligible for registration. Only in consultation with the GAC and ICANN would Donuts develop a proposal for release of these reserved names, and seek approval accordingly. Donuts understands governmental processes require time-consuming, multi-department consultations. Accordingly, we will apportion more than adequate time for the GAC and its members to review any proposal we provide.

Donuts recognizes the potential use of country and territory names at the third level. We will address and mitigate attempted third-level use of geographic names as part of our operations.

Donuts’ list of geographic names will be transmitted to Registrars as part of the onboarding process and will also be made available to the public via the TLD website. Changes to the list are anticipated to be rare; however, Donuts will regularly review and revise the list as changes are made by government authorities.

For purposes of clarity the following will occur for a domain that is reserved by the registry:
1. An availability check for a domain in the reserved list will result in a “not available” status. The reason given will indicate that the domain is reserved.
2. An attempt to register a domain name in the reserved list will result in an error.
3. An EPP info request will result in an error indicating the domain name was not found.
4. Queries for a reserved name in the WHOIS system will display information indicating the reserved status and indicate it is not registered nor is available for registration.
5. Reserved names will not be published or used in the zone in any way.
6. Queries for a reserved name in the DNS will result in an NXDOMAIN response.

Registry Services

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

Q23 CHAR: 22971

TLD Applicant is applying to become an ICANN accredited Top Level Domain (TLD) registry. TLD Applicant meets the operational, technical, and financial capability requirements to pursue, secure and operate the TLD registry. The responses to technical capability questions were prepared to demonstrate, with confidence, that the technical capabilities of TLD Applicant meet and substantially exceed the requirements proposed by ICANN.

The following response describes our registry services, as implemented by Donuts and our partners. Such partners include Demand Media Europe Limited (DMEL) for back-end registry services; AusRegistry Pty Ltd. (ARI) for Domain Name System (DNS) services and Domain Name Service Security Extensions (DNSSEC); an independent consultant for abuse mitigation and prevention consultation; Equinix and SuperNap for datacenter facilities and infrastructure; and Iron Mountain Intellectual Property Management, Inc. (Iron Mountain) for data escrow services. For simplicity, the term “company” and the use of the possessive pronouns “we”, “us”, “our”, “ours”, etc., all refer collectively to Donuts and our subcontracted service providers.

DMEL is a wholly-owned subsidiary of DMIH Limited, a well-capitalized Irish corporation whose ultimate parent company is Demand Media, Inc., a leading content and social media company listed on the New York Stock Exchange (ticker: DMD). DMEL is structured to operate a robust and reliable Shared Registration System by leveraging the infrastructure and expertise of DMIH and Demand Media, Inc., which includes years of experience in the operation side for domain names in both gTLDs and ccTLDs for over 10 years.

1.0. EXECUTIVE SUMMARY

We offer all of the customary services for proper operation of a gTLD registry using an approach designed to support the security and stability necessary to ensure continuous uptime and optimal registry functionality for registrants and Internet users alike.

2.0. REGISTRY SERVICES

2.1. Receipt of Data from registrars

The process of registering a domain name and the subsequent maintenance involves interactions between registrars and the registry. These interactions are facilitated by the registry through the Shared Registration System (SRS) through two interfaces:

- EPP: A standards-based XML protocol over a secure network channel.
- Web: A web based interface that exposes all of the same functionality as EPP yet accessible through a web browser.

Registrants wishing to register and maintain their domain name registrations must do so through an ICANN accredited registrar. The XML protocol, called the

Extensible Provisioning Protocol (EPP) is the standard protocol widely used by registrars to communicate provisioning actions. Alternatively, registrars may use the web interface to create and manage registrations.

The registry is implemented as a “thick” registry meaning that domain registrations must have contact information associated with each. Contact information will be collected by registrars and associated with domain registrations.

2.1.1. SRS EPP Interface

The SRS EPP Interface is provided by a software service that provides network based connectivity. The EPP software is highly compliant with all appropriate RFCs including:

- RFC 5730 Extensible Provisioning Protocol (EPP)
- RFC 5731 Extensible Provisioning Protocol (EPP) Domain Name Mapping
- RFC 5732 Extensible Provisioning Protocol (EPP) Host Mapping
- RFC 5733 Extensible Provisioning Protocol (EPP) Contact Mapping
- RFC 5734 Extensible Provisioning Protocol (EPP) Transport over TCP
- RFC 5910 Domain Name System (DNS) Security Extensions for Extensible Provisioning Protocol (EPP)
- RFC 3915 Domain Registry Grace Period Mapping for EPP

2.1.1.1. SRS EPP Interface Security Considerations

Security precautions are put in place to ensure transactions are received only from authorized registrars in a private, secure manner. Registrars must provide the registry with narrow subnet ranges, allowing the registry to restrict network connections that originate only from these pre-arranged networks. The source IP address is verified against the authentication data received from the connection to further validate the source of the connection. Registrars may only establish a limited number of connections and the network traffic is rate limited to ensure that all registrars receive the same quality of service. Network connections to the EPP server must be secured with TLS. The revocation status and validity of the certificate are checked.

Successful negotiation of a TLS session begins the process of authentication using the protocol elements of EPP. Registrars are not permitted to continue without a successful EPP session establishment. The EPP server validates the credential information passed by the registrar along with validation of:

- Certificate revocation status
- Certificate chain
- Certificate Common Name matches the Common Name the registry has listed for the source IP address
- User name and password are correct and match those listed for the source IP address

In the event a registrar creates a level of activity that threatens the service quality of other registrars, the service has the ability to rate limit individual registrars.

2.1.1.2. SRS EPP Interface Stability Considerations

To ensure the stability of the EPP Interface software, strict change controls and access controls are in place. Changes to the software must be approved by management and go through a rigorous testing and staged deployment procedure.

Additional stability is achieved by carefully regulating the available computing resources. A policy of conservative usage thresholds leaves an equitable amount of computing resources available to handle spikes and service management.

2.1.2. SRS Web Interface

The SRS web interface is an alternative way to access EPP functionality using a web interface, providing the features necessary for effective operations of the registry. This interface uses the HTTPS protocol for secure web communication. Because users can be located worldwide, as with the EPP interface, the web interface is available to all registrars over multiple network paths. Additional functionality is available to registrars to assist them in managing their account. For instance, registrars are able to view their account balance in near real time as well as the status of the registry services. In addition, notifications that are sent out in email are available for viewing.

2.1.2.1. Web Interface Security Considerations

Only registrars are authorized to use the SRS web interface, and therefore the web interface has several security measures to prevent abuse. The web interface requires an encrypted network channel using the HTTPS protocol. Attempts to access the interface through a clear channel are redirected to the encrypted channel.

The web interface restricts access by requiring each user to present authentication credentials before proceeding. In addition to the typical user name and password combinations, the web interface also requires the user to possess a hardware security key as a second factor of authentication.

Registrars are provided a tool to create and manage users that are associated with their account. With these tools, they can set access and authorization levels for their staff.

2.1.2.2. Web Interface Stability Considerations

Both the EPP interface and web interface use a common service provider to perform the work required to fulfill their requests. This provides consistency across both interfaces and ensures all policies and security rules are applied.

The software providing services for both interfaces executes on a farm of servers, distributing the load more evenly ensuring stability is maintained.

2.2. Dissemination of TLD Zone Files

2.2.1. Communication of Status Information of TLD Zone Servers to Registrars

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

Normal operations are:

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

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

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

2.2.2. Communication Policy

We maintain close communication with registrars regarding the performance and consistency of the TLD zone servers.

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

Communication using the registrar contact information discussed above will occur prior to any maintenance that has the potential to effect the access to, consistency of, or reliability of the TLD zone servers. If such maintenance is required within a short timeframe, immediate communication occurs using the above contact information. In either case, the nature of the maintenance and how it affects the consistency or accessibility of the TLD zone servers, and the estimated time for full restoration, are included within the communication.

That being said, the TLD zone server infrastructure has been designed in such a way that we expect no downtime. Only individual sites will potentially require downtime for maintenance; however the DNS service itself will continue to operate with 100% availability.

2.2.3. Security and Stability Considerations

We restrict zone server status communication to registrars, thereby limiting the scope for malicious abuse of any maintenance window. Additionally, we ensure registrars have effective operational procedures to deal with any status change of the TLD nameservers and will seek to align its communication policy to those procedures.

2.3. Zone File Access Provider Integration

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

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

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

2.4. Zone File Update

To ensure changes within the SRS are reflected in the zone file rapidly and securely, we update the zone file on the TLD zone servers following a staged but rapid propagation of zone update information from the SRS, outwards to the TLD zone servers - which are visible to the Internet. As changes to the SRS data occur, those changes are updated to isolated systems which act as the authoritative primary server for the zone, but remain inaccessible to systems outside our network. The primary servers notify the designated secondary servers, which service queries for the TLD zone from the public. Upon notification, the secondary servers transfer the incremental changes to the zone and publicly present those changes.

The mechanisms for ensuring consistency within and between updates are fully implemented in our TLD zone update procedures. These mechanisms ensure updates are quickly propagated while the data remains consistent within each incremental update, regardless of the speed or order of individual update transactions.

2.5. Operation of Zone Servers

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

2.5.1. Security and Operational Considerations of Zone Server Operations

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

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

The TLD zone servers are protected from accessibility loss by malicious intent or misadventure, via the provision of significant over-capacity of resources and access paths. Multiple independent network paths are provided to each TLD zone server and the query servicing capacity of the network exceeds the extremely conservatively anticipated peak load requirements by at least 10 times, to prevent loss of service should query loads significantly increase.

As well as the authentication, authorization and consistency checks carried out by the registrar access systems and DNS update mechanisms, ARI reduces the scope for alteration of DNS data by following strict DNS operational practices:

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

2.6. Dissemination of Domain Registration Information

Domain name registration information is required for a variety of purposes. Our registry provides this information through the required WHOIS service through a standard text based network protocol on port 43. Whois also is provided on the registry’s web site using a standard web interface. Both interfaces are publically available at no cost to the user and are reachable worldwide.

The information displayed by the Whois service consists not only of the domain name but also of relevant contact information associated with the domain. It also identifies nameserver delegation and the registrar of record. This service is available to any Internet user, and use of it does not require prior authorization or permission.

2.6.1. Whois Port 43 Interface

The Whois port 43 interface consists of a standard Transmission Control Protocol (TCP) server that answers requests for information over port 43 in compliance with IETF RFC 3912. For each query, the TCP server accepts the connection over port 43 and then waits for a set time for the query to be sent. This communication occurs via clear, unencrypted ASCII text. If a properly formatted and valid query is received, the registry database is queried for the registration data. If registration data exists, it is returned to the service where it is then formatted and delivered to the requesting client. Each query connection is short-lived. Once the output is transmitted, the server closes the connection.

2.6.2. Whois Web Interface

The Whois web interface also uses clear, unencrypted text. The web interface is in an HTML format suitable for web browsers. This interface is also available over an encrypted channel on port 43 using the HTTPS protocol.

2.6.3. Security and Stability Considerations

Abuse of the Whois system through data mining is a concern as it can impact system performance and reduce the quality of service to legitimate users. The Whois system mitigates this type of abuse by detecting and limiting bulk query access from single sources. It does this in two ways: 1) by rate limiting queries by non-authorized parties; and 2) by ensuring all queries result in responses that do not include data sets representing significant portions of the registration database. In addition, the Whois web interface adds a simple challenge-response CAPCHA that requires a user to type in the characters displayed in image format.
Both systems have blacklist functionality to provide a complete block to individual IPs or IP ranges.

2.7. Internationalized Domain Names (IDNs)

An Internationalized Domain Name (IDN) contains at least one label that is displayed in a specific language script in IDN aware software. We will offer registration of second level IDN labels at launch,
IDNs are published into the TLD zone. The SRS EPP and Web Interfaces also support IDNs.
The IDN implementation is fully compliant with the IDNA 2008 suite of standards (RFC 5890, 5891, 5892 and 5893) as well as the ICANN Guidelines for the Implementation of IDN Version 3.0
〈http:⁄⁄www.icann.org⁄en⁄resources⁄idn⁄implementation-guidelines〉 . To ensure stability and security, we have adopted a conservative approach in our IDN registration policies, as well as technical implementation.

All IDN registrations must be requested using the A-label form, and accompanied by an RFC 5646 language tag identifying the corresponding language table published by the registry. The candidate A-label is processed according to the registration protocol as specified in Section 4 of RFC 5891, with full U-label validation. Specifically, the “Registry Restrictions” steps specified in Section 4.3 of RFC 5891 are implemented by validating the U-label against the identified language table to ensure that the set of characters in the U-label is a proper subset of the character repertoire listed in the language table.

2.7.1. IDN Stability Considerations

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

Domains registered within a particular language are restricted to only the characters of that language. This avoids the use of visually similar characters within one language which mimic the appearance of a label within another language, regardless of whether that label is already within the DNS or not.
Child domains are restricted to a specific language and registrations are prevented in one language being confused with a registration in another language; for example Cyrillic a (U+0430) and Latin a (U+0061).

2.8. DNSSEC

DNSSEC provides a set of extensions to the DNS that allow an Internet user (normally the resolver acting on a user's behalf) to validate that the DNS responses they receive were not manipulated en-route.
This type of fraud, commonly called 'man in the middle', allows a malicious party to misdirect Internet users. DNSSEC allows a domain owner to sign their domain and to publish the signature, so that all DNS consumers who visit that domain can validate that the responses they receive are as the domain owner intended.

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

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

2.8.1. Stability and Operational Considerations for DNSSEC

2.8.1.1. DNSSEC Practice Statement

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

2.8.1.2. Resolution Stability

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

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

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

3.0. APPROACH TO SECURITY AND STABILITY

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

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

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

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

Q24 CHAR: 19964

TLD Applicant is applying to become an ICANN accredited Top Level Domain (TLD) registry. TLD Applicant meets the operational, technical, and financial capability requirements to pursue, secure and operate the TLD registry. The responses to technical capability questions were prepared to demonstrate, with confidence, that the technical capabilities of TLD Applicant meet and substantially exceed the requirements proposed by ICANN.

1.0. INTRODUCTION

Our Shared Registration System (SRS) complies fully with Specification 6, Section 1.2 and the SLA Matrix provided with Specification 10 in ICANN’s Registry Agreement and is in line with the projections outlined in our responses to Questions 31 and 46. The services provided by the SRS are critical to the proper functioning of a TLD registry.

We will adhere to these commitments by operating a robust and reliable SRS founded on best practices and experience in the domain name industry.

2.0. TECHNICAL OVERVIEW

A TLD operator must ensure registry services are available at all times for both registrants and the Internet community as a whole. To meet this goal, our SRS was specifically engineered to provide the finest levels of service derived from a long pedigree of excellence and experience in the domain name industry. This pedigree of excellence includes a long history of technical excellence providing long running, highly available and high-performing services that help thousands of companies derive their livelihoods.

Our SRS services will give registrars standardized access points to provision and manage domain name registration data. We will provide registrars with two interfaces: an EPP protocol over TCP⁄IP and a web site accessible from any web browser (note: throughout this document, references to the SRS are inclusive of both these interfaces).

Initial registration periods will comply with Specification 6 and will be in one (1) year increments up to a maximum of ten (10) years. Registration terms will not be allowed to exceed ten (10) years. In addition, renewal periods also will be in one-year increments and renewal periods will only allow an extension of the registration period of up to ten years from the time of renewal.

The performance of the SRS is critical for the proper functioning of a TLD. Poor performance of the registration systems can adversely impact registrar systems that depend on its responsiveness. Our SRS is committed to exceeding the performance specifications described in Specification 10 in all cases. To ensure that we are well within specifications for performance, we will test our system on a regular basis during development to ensure that changes have not impacted performance in a material way. In addition, we will monitor production systems to ensure compliance. If internal thresholds are exceeded, the issue will be escalated, analyzed and addressed.

Our SRS will offer registry services that support Internationalized Domain Names (IDNs). Registrations can be made through both the EPP and web interfaces.

3.0. ROBUST AND RELIABLE ARCHITECTURE
To ensure quality of design, the SRS software was designed and written by seasoned and experienced software developers. This team designed the SRS using modern software architecture principles geared toward ensuring flexibility in its design not only to meet business needs but also to make it easy to understand, maintain and test.

A classic 3-tier design was used for the architecture of the system. 3-tier is a well-proven architecture that brings flexibility to the system by abstracting the application layer from the protocol layer. The data tier is isolated and only accessible by the services tier. 3-tier adds an additional layer of security by minimizing access to the data tier through possible exploits of the protocol layer.

The protocol and services layers are fully redundant. A minimum of three physical servers is in place in both the protocol and services layers. Communications are balanced across the servers. Load balancing is accomplished with a redundant load balancer pair.

4.0. SOFTWARE QUALITY

The software for the SRS, as well as other registry systems, was developed using an approach that ensures that every line of source code is peer reviewed and source code is not checked into the source code repository without the accompanying automated tests that exercise the new functionality. The development team responsible for building the SRS and other registry software applies continuous integration practices to all software projects; all developers work on an up-to-date code base and are required to synchronize their code base with the master code base and resolve any incompatibilities before checking in. Every source code check-in triggers an automated build and test process to ensure a minimum level of quality. Each day an automated “daily build” is created, automatically deployed to servers and a fully-automated test suite run against it. Any failures are automatically assigned to developers to resolve in the morning when they arrive.

When extensive test passes are in order for release candidates, these developers use a test harness designed to run usability scenarios that exercise the full gamut of use cases, including accelerated full registration life cycles. These scenarios can be entered into the system using various distributions of activity. For instance, the test harness can be run to stress the system by changing the distribution of scenarios or to stress the system by exaggerating particular scenarios to simulate land rushes or, for long running duration scenarios, a more common day-to-day business distribution.

5.0. SOFTWARE COMPLIANCE

The EPP interface to our SRS is compliant with current RFCs relating to EPP protocols and best practices. This includes RFCs 5910, 5730, 5731, 5732, 5733 and 5734. Since we are also supporting Registry Grace Period functionality, we are also compliant with RFC 3915. Details of our compliance with these specifications are provided in our response to Question 25. We are also committed to maintaining compliance with future RFC revisions as they apply as documented in Section 1.2 of Specification 6 of the new gTLD Agreement.

We strive to be forward-thinking and will support the emerging standards of both IPv6 and DNSSEC on our SRS platform. The SRS was designed and has been tested to accept IPv6 format addresses for nameserver glue records and provision them to the gTLD zone. In addition, key registry services will be accessible over both IPv4 and IPv6. These include both the SRS EPP and SRS web-based interfaces, both port 43 and web-based WHOIS interfaces and DNS, among others. For details regarding our IPv6 reachability plans, please refer to our response to Question 36.

DNSSEC services are provided, and we will comply with Specification 6. Additionally, our DNSSEC implementation complies with RFCs 4033, 4034, 4035, and 4509; and we commit to complying with the successors of these RFCs and following the best practices described in RFC 4641. Additional compliance and commitment details on our DNSSEC services can be found in our response to Question 43.

6.0. DATABASE OPERATIONS

The database for our gTLD is Microsoft SQL Server 2008 R2. It is an industry-leading database engine used by companies requiring the highest level of security, reliability and trust. Case studies highlighting SQL Server’s reliability and use indicate its successful application in many industries, including major financial institutions such as Visa, Union Bank of Israel, KeyBank, TBC Bank, Paymark, Coca-Cola, Washington State voter registration and many others. In addition, Microsoft SQL Server provides a number of features that ease the management and maintenance of the system. Additional details about our database system can be found in our response to Question 33.

Our SRS architecture ensures security, consistency and quality in a number of ways. To prevent eavesdropping, the services tier communicates with the database over a secure channel. The SRS is architected to ensure all data written to the database is atomic. By convention, leave all matters of atomicity are left to the database. This ensures consistency of the data and reduces the chance of error. So that we can examine data versions at any point in time, all changes to the database are written to an audit database. The audit data contains all previous and new values and the date⁄time of the change. The audit data is saved as part of each atomic transaction to ensure consistency.

To minimize the chance of data loss due to a disk failure, the database uses an array of redundant disks for storage. In addition, maintain an exact duplicate of the primary site is maintained in a secondary datacenter. All hardware is fully duplicated and set up to take over operations at any time. All database operations are replicated to the secondary datacenter via synchronous replication. The secondary datacenter always maintains an exact copy of our live data as the transactions occur.

7.0. REDUNDANT HARDWARE

The SRS is composed of several pieces of hardware that are critical to its proper functioning, reliability and scale. At least two of each hardware component comprises the SRS, making the service fully redundant. Any component can fail, and the system is designed to use the facility of its pair. The EPP interface to the SRS will operate with more than two servers to provide the capacity required to meet our projected scale as described in Question 46: Projections Template.

8.0. HORIZONTALLY SCALABLE

The SRS is designed to scale horizontally. That means that, as the needs of the registry grow, additional servers can be easily added to handle additional loads.

The database is a clustered 2-node pair configured for both redundancy and performance. Both nodes participate in serving the needs of the SRS. A single node can easily handle the transactional load of the SRS should one node fail. In addition, there is an identical 2-node cluster in our backup datacenter. All data from the primary database is continuously replicated to the backup datacenter.

Not only is the registry database storage medium specified to provide the excess of capacity necessary to allow for significant growth, it is also configured to use techniques, such as data sharing, to achieve horizontal scale by distributing logical groups of data across additional hardware. For further detail on the scalability of our SRS, please refer to our response to Question 31.

9.0. REDUNDANT HOT FAILOVER SITE

We understand the need for maximizing uptime. As such, our plan includes maintaining at all times a warm failover site in a separate datacenter for the SRS and other key registry services. Our planned failover site contains an exact replica of the hardware and software configuration contained in the primary site. Registration data will be replicated to the failover site continuously over a secure connection to keep the failover site in sync.

Failing over an SRS is not a trivial task. In contrast, web site failover can be as simple as changing a DNS entry. Failing over the SRS, and in particular the EPP interface, requires careful planning and consideration as well as training and a well-documented procedure. Details of our failover procedures as well as our testing plans are detailed in our response to Question 41.

10.0. SECURE ACCESS

To ensure security, access to the EPP interface by registrars is restricted by IP⁄subnet. Access Control Lists (ACLs) are entered into our routers to allow access only from a restricted, contiguous subnet from registrars. Secure and private communication over mutually authenticated TLS is required. Authentication credentials and certificate data are exchanged in an out-of-band mechanism. Connections made to the EPP interface that successfully establish an EPP session are subject to server policies that dictate connection maximum lifetime and minimal activity to maintain the session.

To ensure fair and equal access for all registrars, as well as maintain a high level of service, we will use traffic shaping hardware to ensure all registrars receive an equal number of resources from the system.

To further ensure security, access to the SRS web interface is over the public

Internet via an encrypted HTTPS channel. Each registrar will be issued master credentials for accessing the web interface. Each registrar also will be required to use 2-factor authentication when logging in. We will issue a set of Yubikey (http:⁄⁄yubico.com) 2-factor, one-time password USB keys for authenticating with the web site. When the SRS web interface receives the credentials plus the one-time password from the Yubikey, it communicates with a RADIUS authentication server to check the credentials.

11.0. OPERATING A ROBUST AND RELIABLE SRS

11.1. AUTOMATED DEPLOYMENT

To minimize human error during a deployment, we use a fully-automated package and deployment system. This system ensures that all dependencies, configuration changes and database components are included every time. To ensure the package is appropriate for the system, the system also verifies the version of system we are upgrading.

11.2. CHANGE MANAGEMENT

We use a change management system for changes and deployments to critical systems. Because the SRS is considered a critical system, it is also subject to all change management procedures. The change management system covers all software development changes, operating system and networking hardware changes and patching. Before implementation, all change orders entered into the system must be reviewed with careful scrutiny and approved by appropriate management. New documentation and procedures are written; and customer service, operations, and monitoring staff are trained on any new functionality added that may impact their areas.

11.3. PATCH MANAGEMENT

Upon release, all operating system security patches are tested in the staging environment against the production code base. Once approved, patches are rolled out to one node of each farm. An appropriate amount of additional time is given for further validation of the patch, depending on the severity of the change. This helps minimize any downtime (and the subsequent roll back) caused by a patch of poor quality. Once validated, the patch is deployed on the remaining servers.

11.4. REGULAR BACKUPS

To ensure that a safe copy of all data is on hand in case of catastrophic failure of all database storage systems, backups of the main database are performed regularly. We perform full backups on both a weekly and monthly basis. We augment these full backups with differential backups performed daily. The backup process is monitored and any failure is immediately escalated to the systems engineering team. Additional details on our backup strategy and procedures can be found in our response to Question 37.

11.5. DATA ESCROW

Data escrow is a critical registry function. Escrowing our data on a regular basis ensures that a safe, restorable copy of the registration data is available should all other attempts to restore our data fail. Our escrow process is performed in accordance with Specification 2. Additional details on our data escrow procedures can be found in our response to Question 38.

11.6. REGULAR TRAINING

Ongoing security awareness training is critical to ensuring users are aware of security threats and concerns. To sustain this awareness, we have training programs in place designed to ensure corporate security policies pertaining to registry and other operations are understood by all personnel. All employees must pass a proficiency exam and sign the Information Security Policy as part of their employment. Further detail on our security awareness training can be found in our response to Question 30a.

We conduct failover training regularly to ensure all required personnel are up-to-date on failover process and have the regular practice needed to ensure successful failover should it be necessary. We also use failover training to validate current policies and procedures. For additional details on our failover training, please refer to our response to Question 41.

11.7. ACCESS CONTROL

User authentication is required to access any network or system resource. User accounts are granted the minimum access necessary. Access to production resources is restricted to key IT personnel. Physical access to production resources is extremely limited and given only as needed to IT-approved personnel. For further details on our access control policies, please refer to our response to Question 30a.

11.8. 24⁄7 MONITORING AND REGISTRAR TECHNICAL SUPPORT

We employ a full-time staff trained specifically on monitoring and supporting the services we provide. This staff is equipped with documentation outlining our processes for providing first-tier analysis, issue troubleshooting, and incident handling. This team is also equipped with specialty tools developed specifically to safely aid in diagnostics. On-call staff second-tier support is available to assist when necessary. To optimize the service we provide, we conduct ongoing training in both basic and more advanced customer support and conduct additional training, as needed, when new system or tool features are introduced or solutions to common issues are developed.

12.0. SRS INFRASTRUCTURE

As shown in Attachment A, Figure 1, our SRS infrastructure consists of two identically provisioned and configured datacenters with each served by multiple bandwidth providers.

For clarity in Figure 1, connecting lines through the load balancing devices between the Protocol Layer and the Services Layer are omitted. All hardware connecting to the Services Layer goes through a load-balancing device. This device distributes the load across the multiple machines providing the services. This detail is illustrated more clearly in subsequent diagrams in Attachment A.

13.0 RESOURCING PLAN

Resources for the continued development and maintenance of the SRS and ancillary services have been carefully considered. We have a significant portion of the required personnel on hand and plan to hire additional technical resources, as indicated below. Resources on hand are existing full time employees whose primary responsibility is the SRS.

For descriptions of the following teams, please refer to the resourcing section of our response to Question 31, Technical Review of Proposed Registry. Current and planned allocations are below.

Software Engineering:

- Existing Department Personnel: Project Manager, Development Manager, two Sr. Software Engineers, two, Sr. Database Engineer, Quality Assurance Engineer
- First Year New Hires: Web Developer, Database Engineer, Technical Writer, Build⁄Deployment Engineer

Systems Engineering:

- Existing Department Personnel: Sr. Director IT Operations, two Sr. Systems Administrators, two Systems Administrators, two Sr. Systems Engineers, two Systems Engineers
- First Year New Hires: Systems Engineer

Network Engineering:

- Existing Department Personnel: Sr. Director IT Operations, two Sr. Network Engineers, two Network Engineers
- First Year New Hires: Network Engineer

Database Operations:

- Existing Department Personnel: Sr. Database Operations Manager, 2 Database Administrators

Information Security Team:

- Existing Department Personnel: Director of Information Security, Sr. Information Security Specialist, Information Security Specialists, Sr. Information Security Engineer, Information Security Engineer
- First Year New Hires: Information Security Engineer

Network Operations Center (NOC):

- Existing Department Personnel: Manager, two NOC Supervisors, 12 NOC Analysts
- First Year New Hires: Eight NOC Analysts

25. Extensible Provisioning Protocol (EPP)

Q25 CHAR: 20820

TLD Applicant is applying to become an ICANN accredited Top Level Domain (TLD) registry. TLD Applicant meets the operational, technical, and financial capability requirements to pursue, secure and operate the TLD registry. The responses to technical capability questions were prepared to demonstrate, with confidence, that the technical capabilities of TLD Applicant meet and substantially exceed the requirements proposed by ICANN.

1.0. INTRODUCTION

Our SRS EPP interface is a proprietary network service compliant with RFC 3735 and RFCs 5730-4. The EPP interface gives registrars a standardized programmatic access point to provision and manage domain name registrations.

2.0. IMPLEMENTATION EXPERIENCE

The SRS implementation for our gTLD leverages extensive experience implementing long-running, highly available network services accessible. Our EPP interface was written by highly experienced engineers focused on meeting strict requirements developed to ensure quality of service and uptime. The development staff has extensive experience in the domain name industry.

3.0. TRANSPORT

The EPP core specification for transport does not specify that a specific transport method be used and is, thus, flexible enough for use over a variety of transport methods. However, EPP is most commonly used over TCP⁄IP and secured with a Transport Layer Security (TLS) layer for domain registration purposes. Our EPP interface uses the industry standard TCP with TLS.

4.0. REGISTRARS' EXPERIENCE

Registrars will find our EPP interface familiar and seamless. As part of the account creation process, a registrar provides us with information we use to authenticate them. The registrar provides us with two subnets indicating the connection's origination. In addition, the registrar provides us with the Common Name specified in the certificate used to identify and validate the connection.

Also, as part of the account creation process, we provide the registrar with authentication credentials. These credentials consist of a client identifier and an initial password and are provided in an out-of-band, secure manner. These credentials are used to authenticate the registrar when starting an EPP session.

Prior to getting access to the production interfaces, registrars have access to an Operational Test and Evaluation (OT&E) environment. This environment is an isolated area that allows registrars to develop and test against registry systems without any impact to production. The OT&E environment also provides registrars the opportunity to test implementation of custom extensions we may require.

Once a registrar has completed testing and is prepared to go live, the registrar is provided a Scripted Server Environment. This environment contains an EPP interface and database pre-populated with known data. To verify that the registrar's implementations are correct and minimally suitable for the production environment, the registrar is required to run through a series of exercises. Only after successful performance of these exercises is a registrar allowed access to production services.

5.0. SESSIONS

The only connections that are allowed are those from subnets previously communicated during account set up. The registrar originates the connection to the SRS and must do so securely using a Transport Layer Security (TLS) encrypted channel over TCP⁄IP using the IANA assigned standard port of 700.

The TLS protocol establishes an encrypted channel and confirms the identity of each machine to its counterpart. During TLS negotiation, certificates are exchanged to mutually verify identities. Because mutual authentication is required, the registrar certificate must be sent during the negotiation. If it is not sent, the connection is terminated and the event logged.

The SRS first examines the Common Name (CN). The SRS then compares the Common Name to the one provided by the registrar during account set up. The SRS then validates the certificate by following the signature chain, ensures that the chain is complete, and terminates against our store of root Certificate Authorities (CA). The SRS also verifies the revocation status with the root CA. If these fail, the connection is terminated and the event logged.

Upon successful completion of the TLS handshake and the subsequent client validation, the SRS automatically sends the EPP greeting. Then the registrar initiates a new session by sending the login command with their authentication credentials. The SRS passes the credentials to the database for validation over an encrypted channel. Policy limits the number of failed login attempts. If the registrar exceeds the maximum number of attempts, the connection to the server is closed. If authentication was successful, the EPP session is allowed to proceed and a response is returned indicating that the command was successful.

An established session can only be maintained for a finite period. EPP server policy specifies the timeout and maximum lifetime of a connection. The policy requires the registrar to send a protocol command within a given timeout period. The maximum lifetime policy for our registry restricts the connection to a finite overall timespan. If a command is not received within the timeout period or the connection lifetime is exceeded, the connection is terminated and must be reestablished. Connection lifecycle details are explained in detail in our Registrar Manual.

The EPP interface allows pipelining of commands. For consistency, however, the server only processes one command at a time per session and does not examine the next command until a response to the previous command is sent. It is the registrar’s responsibility to track both the commands and their responses.

6.0. EPP SERVICE SCALE

Our EPP service is horizontally scalable. Its design allows us to add commodity-grade hardware at any time to increase our capacity. The design employs a 3-tier architecture which consists of protocol, services and data tiers. Servers for the protocol tier handle the loads of SSL negotiation and protocol validation and parsing. These loads are distributed across a farm of numerous servers balanced by load-balancing devices. The protocol tier connects to the services tier through load-balancing devices.

The services tier consists of a farm of servers divided logically based on the services provided. Each service category has two or more servers. The services tier is responsible for registry policy enforcement, registration lifecycle and provisioning, among other services. The services tier connects to the data tier which consists of Microsoft SQL Server databases for storage.

The data tier is a robust SQL Server installation that consists of a 2-node cluster in an active⁄active configuration. Each node is designed to handle the entire load of the registry should the alternate node go offline.

Additional details on scale and our plans to service the load we anticipate are described in detail on questions 24: SRS Performance and 32: Architecture.

7.0. COMPLIANCE WITH CORE AND EPP EXTENSION RFCs

The EPP interface is highly compliant with the following RFCs:

- RFC 5730 Extensible Provisioning Protocol
- RFC 5731 EPP Domain Name Mapping
- RFC 5732 EPP Host Mapping
- RFC 5733 EPP Contact Mapping
- RFC 5734 EPP Transport over TCP
- RFC 3915 Domain Registry Grace Period Mapping
- RFC 5910 Domain Name System (DNS) Security Extensions Mapping

The implementation is fully compliant with all points in each RFC. Where an RFC specifies optional details or service policy, they are explained below.

7.1. RFC 5730 EXTENSIBLE PROVISIONING PROTOCOL

Section 2.1 Transport Mapping Considerations - ack.
Transmission Control Protocol (TCP) in compliance with RFC 5734 with TLS.

Section 2.4 Greeting Format – compliant
The SRS implementation responds to a successful connection and subsequent TLS handshake with the EPP Greeting. The EPP Greeting is also transmitted in response to a 〈hello⁄〉 command. The server includes the EPP versions supported which at this time is only 1.0. The Greeting contains namespace URIs as 〈objURI⁄〉 elements representing the objects the server manages.

The Greeting contains a 〈svcExtension〉 element with one 〈extURI〉 element for each extension namespace URI implemented by the SRS.

Section 2.7 Extension Framework – compliant
Each mapping and extension, if offered, will comply with RFC 3735 Guidelines for Extending EPP.

Section 2.9 Protocol Commands – compliant

Login command’s optional 〈options〉 element is currently ignored. The 〈version〉 is verified and 1.0 is currently the only acceptable response. The 〈lang〉 element is also ignored because we currently only support English (en). This server policy is reflected in the greeting.

The client mentions 〈objURI〉 elements that contain namespace URIs representing objects to be managed during the session inside 〈svcs〉 element of Login request. Requests with unknown 〈objURI〉 values are rejected with error information in the response. A 〈logout〉 command ends the client session.

Section 4 Formal syntax - compliant
All commands and responses are validated against applicable XML schema before acting on the command or sending the response to the client respectively. XML schema validation is performed against base schema (epp-1.0), common elements schema (eppcom-1.0) and object-specific schema.

Section 5 Internationalization Considerations - compliant
EPP XML recognizes both UTF-8 and UTF-16. All date-time values are presented in Universal Coordinated Time using Gregorian calendar.

7.2. RFC 5731 EPP DOMAIN NAME MAPPING

Section 2.1 Domain and Host names – compliant
The domain and host names are validated to meet conformance requirements mentioned in RFC 0952, 1123 and 3490.

Section 2.2 Contact and Client Identifiers – compliant
All EPP contacts are identified by a server-unique identifier. Contact identifiers conform to “clIDType” syntax described in RFC 5730.

Section 2.3 Status Values – compliant
A domain object always has at least one associated status value. Status value can only be set by the sponsoring client or the registry server where it resides. Status values set by server cannot be altered by client. Certain combinations of statuses are not permitted as described by RFC.

Section 2.4 Dates and Times – compliant
Date and time attribute values are represented in Universal Coordinated Time (UTC) using Gregorian calendar, in conformance with XML schema.

Section 2.5 Validity Periods - compliant
Our SRS implementation supports validity periods in unit year ("y"). The default period is 1y.

Section 3.1.1 EPP 〈check〉 Command - compliant
A maximum of 5 domains can be checked in a single command request as defined by server policy.

Section 3.1.2 EPP 〈info〉 Command - compliant
EPP 〈info〉 command is used to retrieve information associated with a domain object. If the querying Registrar is not the sponsoring registrar and the registrar does not provide valid authorization information, the server does not send any domain elements in response per server policy.

Section 3.1.3 EPP 〈transfer〉 Query Command - compliant
EPP 〈transfer〉 command provides a query operation that allows a client to determine the real-time status of pending and completed transfer requests. If the authInfo element is not provided or authorization information is invalid, the command is rejected for authorization.

Section 3.2.4 EPP 〈transfer〉 Command - compliant
All subordinate host objects to the domain are transferred along with the domain object.

7.3. RFC 5732 EPP HOST MAPPING

Section 2.1 Host Names - compliant
The host names are validated to meet conformance requirements mentioned in RFC 0952, 1123 and 3490.

Section 2.2 Contact and Client Identifiers - compliant
All EPP clients are identified by a server-unique identifier. Client identifiers conform to "clIDType" syntax described in RFC 5730.

Section 2.5 IP Addresses - compliant
The syntax for IPv4 addresses conform to RFC0791. The syntax for IPv6 addresses conform to RFC4291.

Section 3.1.1 EPP 〈check〉 Command - compliant
Maximum of five host names can be checked in a single command request set by server policy.

Section 3.1.2 EPP 〈info〉 Command - compliant
If the querying client is not a sponsoring client, the server does not send any host object elements in response and the request is rejected for authorization according to server policy.

Section 3.2.2 EPP 〈delete〉 Command - compliant
A delete is permitted only if the host is not delegated.

Section 3.2.2 EPP 〈update〉 Command - compliant
Any request to change host name of an external host that has associations with objects that are sponsored by a different client fails.

7.4. RFC 5733 EPP CONTACT MAPPING

Section 2.1 Contact and Client Identifiers - compliant
Contact identifiers conform to "clIDType" syntax described in RFC 5730.

Section 2.6 Email Addresses – compliant
Email address validation conforms to syntax defined in RFC5322.

Section 3.1.1 EPP 〈check〉 Command – compliant
Maximum of 5 contact id can be checked in a single command request.

Section 3.1.2 EPP 〈info〉 Command – compliant
If querying client is not sponsoring client, server does not send any contact object elements in response and the request is rejected for authorization.

Section 3.2.2 EPP 〈delete〉 Command – compliant
A delete is permitted only if the contact object is not associated with other known objects.

7.5. RFC 5734 EPP TRANSPORT OVER TCP

Section 2 Session Management – compliant
The SRS implementation conforms to the required flow mentioned in the RFC for initiation of a connection request by a client, to establish a TCP connection. The client has the ability to end the session by issuing an EPP 〈logout〉 command, which ends the session and closes the TCP connection. Maximum life span of an established TCP connection is defined by server policy. Any connections remaining open beyond that are terminated. Any sessions staying inactive beyond the timeout policy of the server are also terminated similarly. Policies regarding timeout and lifetime values are clearly communicated to registrars in documentation provided to them.

Section 3 Message Exchange – compliant
With the exception of EPP server greeting, EPP messages are initiated by EPP client in the form of EPP commands. Client-server interaction works as a command-response exchange where the client sends one command to the server and the server returns one response to the client in the exact order as received by the server.

Section 8 Security considerations – ack.
TLS 1.0 over TCP is used to establish secure communications from IP restricted clients. Validation of authentication credentials along with the certificate common name, validation of revocation status and the validation of the full certificate chain are performed. The ACL only allows connections from subnets prearranged with the Registrar.

Section 9 TLS Usage Profile – ack.
The SRS uses TLS 1.0 over TCP and matches the certificate common name. The full certificate chain, revocation status and expiry date is validated. TLS is implemented for mutual client and server authentication.

8.0. EPP EXTENSIONS

8.1. STANDARDIZED EXTENSIONS

Our implementation includes extensions that are accepted standards and fully documented. These include the Registry Grace Period Mapping and DNSSEC.

8.2. COMPLIANCE WITH RFC 3735

RFC 3735 are the Guidelines for Extending the Extensible Provisioning Protocol. Any custom extension implementations follow the guidance and recommendations given in RFC 3735.

8.3. COMPLIANCE WITH DOMAIN REGISTRY GRACE PERIOD MAPPING RFC 3915

Section 1 Introduction – compliant
Our SRS implementation supports all specified grace periods particularly, add grace period, auto-renew grace period, renew grace period, and transfer grace period.

Section 3.2 Registration Data and Supporting Information – compliant
Our SRS implementation supports free text and XML markup in the restore report.

Section 3.4 Client Statements – compliant
Client can use free text or XML markup to make 2 statements regarding data included in a restore report.

Section 5 Formal syntax - compliant
All commands and responses for this extension are validated against applicable XML schema before acting on the command or sending the response to the client respectively. XML schema validation is performed against RGP specific schema (rgp-1.0).

8.4. COMPLIANCE WITH DOMAIN NAME SYSTEM (DNS) SECURITY EXTENSIONS MAPPING RFC 5910

RFC 5910 describes an Extensible Provisioning Protocol (EPP) extension mapping for the provisioning and management of Domain Name System Security Extensions (DNSSEC) for domain names stored in a shared central repository. Our SRS and DNS implementation supports DNSSEC.

The information exchanged via this mapping is extracted from the repository and used to publish DNSSEC Delegate Signer (DS) resource records (RR) as described in RFC 4034.

Section 4 DS Data Interface and Key Data Interface – compliant
Our SRS implementation supports only DS Data Interface across all commands applicable with DNSSEC extension.

Section 4.1 DS Data Interface – compliant
The client can provide key data associated with the DS information. The collected key data along with DS data is returned in an info response, but may not be used in our systems.

Section 4.2 Key Data Interface – compliant
Since our gTLD’s SRS implementation does not support Key Data Interface, when a client sends a command with Key Data Interface elements, it is rejected with error code 2306.

Section 5.1.2 EPP 〈info〉 Command – compliant
This extension does not add any elements to the EPP 〈info〉 command. When an 〈info〉 command is processed successfully, the EPP 〈resData〉 contains child elements for EPP domain mapping. In addition, it contains a child 〈secDNS:infData〉 element that identifies extension namespace if the domain object has data associated with this extension. It is conditionally based on whether or the client added the 〈extURI〉 element for this extension in the 〈login〉 command. Multiple DS data elements are supported.

Section 5.2.1 EPP 〈create〉 Command – compliant
The client must add an 〈extension〉 element, and the extension element MUST contain a child 〈secDNS:create〉 element if the client wants to associate data defined in this extension to the domain object. Multiple DS data elements are supported. Since the SRS implementation does not support maxSigLife, it returns a 2102 error code if the command included a value for maxSigLife.

Section 5.2.5 EPP 〈update〉 Command – compliant

Since the SRS implementation does not support the 〈secDNS:update〉 element’s optional “urgent” attribute, an EPP error result code of 2102 is returned if the “urgent” attribute is specified in the command with value of Boolean true.

8.5. PROPRIETARY EXTENSION DOCUMENTATION

We are not proposing any proprietary EPP extensions for this TLD.

8.6. EPP CONSISTENT WITH THE REGISTRATION LIFECYCLE DESCRIBED IN QUESTION 27

Our EPP implementation makes no changes to the industry standard registration lifecycle and is consistent with the lifecycle described in Question 27.

9.0. RESOURCING PLAN

For descriptions of the following teams, please refer to our response to Question 31. Current and planned allocations are below.

Software Engineering:

- Existing Department Personnel: Project Manager, Development Manager, 2 Sr. Software Engineers, Sr. Database Engineer, Quality Assurance Engineer
- First Year New Hires: Web Developer, Database Engineer, Technical Writer, Build⁄Deployment Engineer

Systems Engineering:

- Existing Department Personnel: Sr. Director IT Operations, two Sr. Systems Administrators, two Systems Administrators, two Sr. Systems Engineers, two Systems Engineers
- First Year New Hires: Systems Engineer

Network Engineering:

- Existing Department Personnel: Sr. Director IT Operations, two Sr. Network Engineers, two Network Engineers
- First Year New Hires: Network Engineer

Database Operations:

- Existing Department Personnel: Sr. Database Operations Manager, two Database Administrators

Information Security Team:

- Existing Department Personnel: Director of Information Security, Sr. Information Security Specialist, Information Security Specialists, Sr. Information Security Engineer, Information Security Engineer
- First Year New Hires: Information Security Engineer

Network Operations Center (NOC):

- Existing Department Personnel: Manager, two NOC Supervisors, 12 NOC Analysts
- First Year New Hires: Eight NOC Analysts

26. Whois

Q26 CHAR: 19908

1.0. INTRODUCTION

Our registry provides a publicly available Whois service for registered domain names in the top-level domain (TLD). Our planned registry also offers a searchable Whois service that includes web-based search capabilities by domain name, registrant name, postal address, contact name, registrar ID and IP addresses without an arbitrary limit. The Whois service for our gTLD also offers Boolean search capabilities, and we have initiated appropriate precautions to avoid abuse of the service. This searchable Whois service exceeds requirements and is eligible for a score of 2 by providing the following:

- Web-based search capabilities by domain name, registrant name, postal address, contact names, registrar IDs, and Internet Protocol addresses without arbitrary limit.
- Boolean search capabilities.
- Appropriate precautions to avoid abuse of this feature (e.g., limiting access to legitimate authorized users).
- Compliance with any applicable privacy laws or policies.

The Whois service for our planned TLD is available via port 43 in accordance with RFC 3912. Also, our planned registry includes a Whois web interface. Both provide free public query-based access to the elements outlined in Specification 4 of the Registry Agreement. In addition, our registry includes a searchable Whois service. This service is available to authorized entities and accessible from a web browser.

2.0. HIGH-LEVEL WHOIS SYSTEM DESCRIPTION

The Whois service for our registry provides domain registration information to the public. This information consists not only of the domain name but also of relevant contact information associated with the domain. It also identifies nameserver delegation and the registrar of record. This service is available to any Internet user, and use does not require prior authorization or permission. To maximize accessibility to the data, Whois service is provided over two mediums, as described below. Where the medium is not specified, any reference to Whois pertains to both mediums. We describe our searchable Whois solution in Section 11.0.

One medium used for our gTLD’s Whois service is port 43 Whois. This consists of a standard Transmission Control Protocol (TCP) server that answers requests for information over port 43 in compliance with IETF RFC 3912. For each query, the TCP server accepts the connection over port 43 and then waits for a set time for the query to be sent. This communication occurs via clear, unencrypted text. If no query is received by the server within the allotted time or a malformed query is detected, the connection is closed. If a properly formatted and valid query is received, the registry database is queried for the registration data. If registration data exists, it is returned to the service where it is then formatted and delivered to the requesting client. Each query connection is short-lived. Once the output is transmitted, the server closes the connection.

The other medium used for Whois is via web interface using clear, unencrypted text. The web interface is in an HTML format suitable for web browsers. This interface is also available over an encrypted channel on port 443 using the HTTPS protocol.

The steps for accessing the web-based Whois will be prominently displayed on the registry home page. The web-based Whois is for interactive use by individual users while the port 43 Whois system is for automated use by computers and lookup clients.

Both Whois service offerings comply with Specification 4 of the New GTLD Agreement. Although the Whois output is free text, it follows the output format as described for domain, registrar and nameserver data in Sections 1.4, 1.5 and 1.6 of Specification 4 of the Registry Agreement.

Our gTLD's WHOIS service is mature, and its current implementation has been in continuous operation for seven years. A dedicated support staff monitors this service 24⁄7. To ensure high availability, multiple redundant servers are maintained to enable capacity well above normal query rates.

Most of the queries sent to the port 43 Whois service are automated. The Whois service contains mechanisms for detecting abusive activity and, if abuse is detected, reacts appropriately. This capability contributes to a high quality of service and availability for all users.

2.1. PII POLICY

The services and systems for this gTLD do not collect, process or store any personally identifiable information (PII) as defined by state disclosure and privacy laws. Registry systems collect the following Whois data types: first name, last name, address and phone numbers of all billing, administration and technical contacts. Any business conducted where confidential PII consisting of customer payment information is collected uses systems that are completely separate from registry systems and segregated at the network layer.

3.0. RELEVANT NETWORK DIAGRAM(S)

Our network diagram (Q 26 - Attachment A, Figure 1) provides a quick-reference view of the Whois system. This diagram reflects the Whois system components and compliance descriptions and explanations that follow in this section.

3.1. NARRATIVE FOR Q26 - FIGURE 1 OF 1 (SHOWN IN ATTACHMENT A)

The Whois service for our gTLD operates from two datacenters from replicated data. Network traffic is directed to either of the datacenters through a global load balancer. Traffic is directed to an appropriate server farm, depending on the service interface requested. The load balancer within the datacenter monitors the load and health of each individual server and uses this information to select an appropriate server to handle the request.

The protocol server handling the request communicates over an encrypted channel with the Whois service provider through a load-balancing device. The WHOIS service provider communicates directly with a replicated, read-only copy of the appropriate data from the registry database. The Whois service provider is passed a sanitized and verified query, such as a domain name. The database attempts to locate the appropriate records, then format and return them. Final output formatting is performed by the requesting server and the results are returned back to the original client.

4.0. INTERCONNECTIVITY WITH OTHER REGISTRY SYSTEMS

The Whois port 43 interface runs as an unattended service on servers dedicated to this task. As shown in Attachment A, Figure 1, these servers are delivered network traffic by redundant load-balancing hardware, all of which is protected by access control methods. Balancing the load across many servers helps distribute the load and allows for expansion. The system’s design allows for the rapid addition of new servers, typically same-day, should load require them.

Both our port 43 Whois and our web-based Whois communicate with the Whois service provider in the middle tier. Communication to the Whois service provider is distributed by a load balancing pair. The Whois service provider calls the appropriate procedures in the database to search for the registration records.

The Whois service infrastructure operates from both datacenters, and the global load balancer distributes Whois traffic evenly across the two datacenters. If one datacenter is not responding, the service sends all traffic to the remaining datacenter. Each datacenter has sufficient capacity to handle the entire load.

To avoid placing an abnormal load on the Shared Registration System (SRS), both service installations read from replicated, read-only database instances (see Figure 1). Because each instance is maintained via replication from the primary SRS database, each replicated database contains a copy of the authoritative data. Having the Whois service receive data from this replicated database minimizes the impact of services competing for the same data and enables service redundancy. Data replication is also monitored to prevent detrimental impact on the primary SRS.

5.0. FREQUENCY OF SYNCHRONIZATION BETWEEN SERVERS

As shown in Figure 1, the system replicates WHOIS services data continuously from the authoritative database to the replicated database. This persistent connection is maintained between the databases, and each transaction is queued and published as an atomic unit. Delays, if any, in the replication of registration information are minimal, even during periods of high load. At no time will the system prioritize replication over normal operations of the SRS.

6.0. POTENTIAL FORMS OF ABUSE

Potential forms of abuse of this feature, and how they are mitigated, are outlined below. For additional information on our approach to preventing and mitigating Whois service abuse, please refer to our response to Question 28.

6.1. DATA MINING ABUSE

This type of abuse consists primarily of a user using queries to acquire all or a significant portion of the registration database.

The system mitigates this type of abuse by detecting and limiting bulk query access from single sources. It does this in two ways: 1) by rate-limiting queries by non-authorized parties; and 2) by ensuring all queries result in responses that do not include data sets representing significant portions of the registration database.

6.2. INVALID DATA INJECTION

This type of abuse is mitigated by 1) ensuring that all Whois systems are strictly read-only; and 2) ensuring that any input queries are properly sanitized to prevent data injection.

6.3. DISCLOSURE OF PRIVATE INFORMATION

The Whois system mitigates this type of abuse by ensuring all responses, while complete, only contain information appropriate to Whois output and do not contain any private or non-public information.

7.0. COMPLIANCE WITH WHOIS SPECIFICATIONS FOR DATA OBJECTS, BULK ACCESS, AND LOOKUPS

Whois specifications for data objects, bulk access, and lookups for our gTLD are fully compliant with Specifications 4 and 10 to the Registry Agreement, as explained below.

7.1. COMPLIANCE WITH SPECIFICATION 4

Compliance of Whois specifications with Specification 4 is as follows:

- Registration Data Directory Services Component: Specification 4.1 is implemented as described. Formats follow the outlined semi-free text format. Each data object is represented as a set of key⁄value pairs with lines beginning with keys followed by a colon and a space as delimiters, followed by the value. Fields relevant to RFCs 5730-4 are formatted per Section 1.7 of Specification 4.
- Searchability compliance is achieved by implementing, at a minimum, the specifications in section 1.8 of specification 4. We describe this searchability feature in Section 11.0.
- Co-operation, ICANN Access and Emergency Operator Access: Compliance with these specification components is assured.
- Bulk Registration Data Access to ICANN: Compliance with this specification component is assured.

Evidence of Whois system compliance with this specification consists of:

- Matching existing Whois output with specification output to verify that it is equivalent.

7.2. COMPLIANCE WITH SPECIFICATION 10 FOR WHOIS

Our gTLD’s Whois complies fully with Specification 10. With respect to Section 4.2, the approach used ensures that Round-Trip Time (RTT) remains below five times the corresponding Service Level Requirement (SLR).

7.2.1. Emergency Thresholds

To achieve compliance with this Specification 10 component, several measures are used to ensure emergency thresholds are never reached:

1) Provide staff training as necessary on Registry Transition plan components that prevent Whois service interruption in case of emergency (see the Question 40 response for details).
2) Conduct regular failover testing for Whois services as outlined in the Question 41 response.
3) Adhere to recovery objectives for Whois as outlined in the Question 39 response.

7.2.2. Emergency Escalation

Compliance with this specification component is achieved by participation in escalation procedures as outlined in this section.

8.0. COMPLIANCE WITH RFC 3912

Whois service for our gTLD is fully compliant with RFC 3912 as follows:

- RFC 3912 Element, “A Whois server listens on TCP port 43 for requests from Whois clients”: This requirement is properly implemented, as described in Section 1 above. Further, running Whois on ports other than port 43 is an option.

- RFC 3912 Element, “The Whois client makes a text request to the Whois server, then the Whois server replies with text content”: The port 43 Whois service is a text-based query and response system. Thus, this requirement is also properly implemented.
- RFC 3912 Element, “All requests are terminated with ASCII CR and then ASCII LF. The response might contain more than one line of text, so the presence of ASCII CR or ASCII LF characters does not indicate the end of the response”: This requirement is properly implemented for our TLD.
- RFC 3912 Element, “The Whois server closes its connection as soon as the output is finished”: This requirement is properly implemented for our TLD, as described in Section 1 above.
- RFC 3912 Element, “The closed TCP connection is the indication to the client that the response has been received”: This requirement is properly implemented.

9.0. RESOURCING PLAN

Resources for the continued development and maintenance of the Whois have been carefully considered. Many of the required personnel are already in place. Where gaps exist, technical resource addition plans are outlined below as “First Year New Hires.” Resources now in place, shown as “Existing Department Personnel”, are employees whose primary responsibility is the registry system.

Software Engineering:

- Existing Department Personnel: Project Manager, Development Manager, two Sr. Software Engineers, Sr. Database Engineer, Quality Assurance Engineer
- First Year New Hires: Web Developer, Database Engineer, Technical Writer, Build⁄Deployment Engineer

Systems Engineering:

- Existing Department Personnel: Sr. Director IT Operations, two Sr. Systems Administrators, two Systems Administrators, two Sr. Systems Engineers, two Systems Engineers
- First Year New Hires: Systems Engineer

Network Engineering:

- Existing Department Personnel: Sr. Director IT Operations, two Sr. Network Engineers, two Network Engineers
- First Year New Hires: Network Engineer

Database Operations:

- Existing Department Personnel: Sr. Database Operations Manager, two Database Administrators

Information Security Team:

- Existing Department Personnel: Director of Information Security, Sr. Information Security Specialist, Information Security Specialists, Sr. Information Security Engineer, Information Security Engineer
- First Year New Hires: Information Security Engineer

Network Operations Center (NOC):

- Existing Department Personnel: Manager, two NOC Supervisors, 12 NOC Analysts
- First Year New Hires: Eight NOC Analysts

11.0. PROVISION FOR SEARCHABLE WHOIS CAPABILITIES

The searchable Whois service for our gTLD provides flexible and powerful search ability for users through a web-based interface. This service is provided only to entities with a demonstrated need for it. Where access to registration data is critical to the investigation of cybercrime and other potentially unlawful activity, we authorize access for fully vetted law enforcement and other entities as appropriate. Search capabilities for our gTLD's searchable Whois meet or exceed the requirements indicated in section 1.8 of specification 4.

Once authorized to use the system, a user can perform exact and partial match searches on the following fields:

- Domain name
- Registrant name
- Postal address including street, city and state, etc., of all registration contacts
- Contact names
- Registrant email address
- Registrar name and ID
- Nameservers
- Internet Protocol addresses

In addition, all other EPP Contact Object fields and sub-fields are searchable as well. The following Boolean operators are also supported: AND, OR, NOT. These operators can be used for joining or excluding results.

Certain types of registry related abuse are unique to the searchable Whois function. Providing searchable Whois warrants providing protection against this abuse. Potential problems include:

- Attempts to abuse Whois by issuing a query that essentially returns the entire database in the result set.
- Attempts to run large quantities of queries sufficient to reduce the performance of the registry database.

Precautions for preventing and mitigating abuse of the Whois search service include:

- Limiting access to authorized users only.
- Establishing legal agreements with authorized users that clearly define and prohibit system abuse.
- Queuing search queries into a job processing system.
- Executing search queries against a replicated read-only copy of the database.
- Limiting result sets when the query is clearly meant to cause a wholesale dump of registration data.

Only authorized users with a legitimate purpose for searching registration data are permitted to use the searchable Whois system. Examples of legitimate purpose include the investigation of terrorism or cybercrime by authorized officials, or any of many other official activities that public officials must conduct to fulfill their respective duties. We grant access for these and other purposes on a case-by-case basis.

To ensure secure access, a two-factor authentication device is issued to each authorized user of the registry. Subsequent access to the system requires the user name, password and a one-time generated password from the issued two-factor device.

Upon account creation, users are provided with documentation describing our terms of service and policies for acceptable use. Users must agree to these terms to use the system. These terms clearly define and illustrate what constitutes legitimate use and what constitutes abuse. They also inform the user that abuse of the system is grounds for limiting or terminating the user’s account.

For all queries submitted, the searchable Whois system first sanitizes the query to deter potential harm to our internal systems. The system then submits the query to a queue for job processing. The system processes each query one by one and in the order received. The number of concurrent queries executed varies, depending on the current load.

To ensure Whois search capabilities do not affect other registry systems, the system executes queries against a replicated read-only version of the database. The system updates this database frequently as registration transactions occur. These updates are performed in a manner that ensures no detrimental load is placed on the production SRS.

To process successfully, each query must contain the criteria needed to filter its results down to a reasonable result set (one that is not excessively large). If the query does not meet this, the user is notified that the result set is excessive and is asked to verify the search criteria. If the user wishes to continue without making the indicated changes, the user must contact our support team to verify and approve the query. Each successful query submitted results in immediate execution of the query.

Query results are encrypted using the unique shared secret built into each 256-bit Advanced Encryption Standard (AES) two-factor device. The results are written to a secure location dedicated for result storage and retrieval. Each result report has a unique file name in the user’s directory. The user’s directory is assigned the permissions needed to prevent unauthorized access to report files. For the convenience of Registrars and other users, each query result is stored for a minimum of 30 days. At any point following this 30-day period, the query result may be purged by the system.

27. Registration Life Cycle

Q27 CHAR: 19951

1.0. INTRODUCTION
To say that the lifecycle of a domain name is complex would be an understatement. A domain name can traverse many states throughout its lifetime and there are many and varied triggers that can cause a state transition. Some states are triggered simply by the passage of time. Others are triggered by an explicit action taken by the registrant or registrar. Understanding these is critical to the proper operation of a gTLD registry. To complicate matters further, a domain name can contain one or more statuses. These are set by the registrar or registry and have a variety of uses.

When this text discusses EPP commands received from registrars, with the exception of a transfer request, the reader can assume that the command is received from the sponsoring registrar and successfully processed. The transfer request originates from the potential gaining registrar. Transfer details are explicit for clarity.

2.0. INDUSTRY STANDARDS
The registration life cycle approach for our gTLD follows industry standards for registration lifecycles and registration statuses. By implementing a registration life cycle that adheres to these standards, we avoid compounding an already

confusing topic for registrants. In addition, since registrar systems are already designed to manage domain names in a standard way, a standardized registration lifecycle also lowers the barrier to entry for registrars.

The registration lifecycle for our gTLD follows core EPP RFCs including RFC 5730 and RFC 5731 and associated documentation of lifecycle information. To protect registrants, EPP Grace Period Mapping for domain registrations is implemented, which affects the registration lifecycle and domain status. EPP Grace Period Mapping is documented in RFC 3915.

3.0. REGISTRATION STATES
For a visual guide to this registration lifecycle discussion, please refer to the attachment, Registration Lifecycle Illustrations. Please note that this text makes many references to the status of a domain. For brevity, we do not distinguish between the domain mapping status 〈domain:status〉 and the EPP Grace Period Mapping status 〈rgp:rgpStatus〉 as making this differentiation in every case would make this document more difficult to read and in this context does not improve understanding.

4.0. AVAILABILITY
The lifecycle for any domain registration begins with the Available state. This is not necessarily a registration state, per se, but indicates the lack of domain registration implied and provides an entry and terminal point for the state diagram provided. In addition to the state diagram, please refer to Fig. 2 - Availability Check for visual representation of the process flow.

Before a user can register a new domain name, the registry performs an availability check. Possible outcomes of this availability check include:
1. Domain name is available for registration.
2. Domain name is already registered, regardless of the current state and not available for registration.
3. Domain name has been reserved by the registry.
4. Domain name string has been blocked because of a trademark claim.

5.0. INITIAL REGISTRATION
The first step in domain registration is the availability check as described above and shown in Fig. 2 - Availability Check. A visual guide to the description for domain registration in this section can be found in Fig. 3 - Domain Registration. If the domain is available for registration, a registrar submits a registration request.

With this request, the registrar can include zero or more nameserver hosts for zone delegation. If the registrar includes zero or one nameserver host(s), the domain is registered but the EPP status of the domain is set to inactive. If the registrar includes two or more, the EPP status of the domain is set to ok.

The request may also include a registration period (the number of years the registrar would like the domain registered). If this time period is omitted, the registry may use a default initial registration period. The policy for this aligns with the industry standard of one year as the default period. If the registrar includes a registration period, the value must be between one and ten years as specified in the gTLD Registry Agreement.

Once the registration process is complete within the registry, the domain registration is considered to be in the REGISTERED state but within the Add Grace Period.

6.0. REGISTERED STATE - ADD GRACE PERIOD
The Add Grace Period is a status given to a new domain registration. The EPP

status applied in this state is addPeriod. The Add Grace Period is a state in which the registrar is eligible for a refund of the registration price should the registration be deleted while this status is applied. The status is removed and the registration transitions from the Add Grace Period either by an explicit delete request from the registrar or by the lapse of five days. This is illustrated in Fig. 1 and Fig. 3 of the illustrations attachment.

If the registrar deletes the domain during the Add Grace Period, the domain becomes immediately available for registration. The registrar is refunded the original cost of the registration.

If the five-day period lapses without receiving a successful delete command, the addPeriod status is removed from the domain.

7.0. REGISTERED STATE

A domain registration spends most of its time in the REGISTERED state. A domain registration period can initially be between one year and ten years in one-year increments as specified in the new gTLD Registry Agreement. At any time during the registration's term, several things can occur to either affect the registration period or transition the registration to another state. The first three are the auto-renew process, an explicit renew EPP request and a successful completion of the transfer process.

8.0. REGISTRATION PERIOD EXTENSION

The registration period for a domain is extended either through a successful renew request by the registrar, through the successful completion of the transfer process or through the auto-renew process. This section discusses each of these three options.

8.1. EXTENSION VIA RENEW REQUEST

One way that a registrar can extend the registration period is by issuing a renew request. Each renew request includes the number of years desired for extension of the registration up to ten years. Please refer to the flow charts found in both Fig. 4 – Renewal and Fig. 5 – Renewal Grace Period for a visual representation of the following.

Because the registration period cannot extend beyond ten years, any request for a registration period beyond ten years fails. The domain must not contain the status renewProhibited. If this status exists on the domain, the request for a renewal fails.

Upon a successful renew request, the registry adds the renewPeriod status to the domain. This status remains on the domain for a period of five days. The number of years in the renew request is added to the total registration period of the domain. The registrar is charged for each year of the additional period.

While the domain has the renewPeriod status, if the sponsoring registrar issues a successful delete request, the registrar receives a credit for the renewal. The renewPeriod status is removed and the domain enters the Redemption Grace Period (RGP) state. The status redemptionPeriod is added to the status of the domain.

8.2. EXTENSION VIA TRANSFER PROCESS

The second way to extend the registration is through the Request Transfer process. A registrar may transfer sponsorship of a domain name to another registrar. The exact details of a transfer are explained in the Request Transfer section below. The successful completion of the Request Transfer process automatically extends the registration for one year. The registrar is not charged separately for the addition of the year; it comes automatically with the successful transfer. The transferPeriod status is added to the domain.

If the gaining registrar issues a successful delete request during the transferPeriod, the gaining registrar receives a credit for the transfer. The status redemptionPeriod is added to the status of the domain and transferPeriod is removed. The domain then enters the RGP state.

8.3. EXTENSION VIA AUTO-RENEW
The last way a registration period can be extended is passive and is the simplest way because it occurs without any action by the Registrar. When the registration period expires, for the convenience of the registrar and registrant, the registration renews automatically for one year. The registrar is charged for the renewal at this time. This begins the Auto Renew Grace Period. The autoRenewPeriod status is added to the domain to represent this period.

The Auto Renew Grace Period lasts for 45 days. At any time during this period, the Registrar can do one of four things: 1) passively accept the renewal; 2) actively renew (to adjust renewal options); 3) delete the registration; or 4) transfer the registration.

To passively accept the renewal, the registrar need only allow the 45-day time span to pass for the registration to move out of the Auto Renew Grace Period.

Should the registrar wish to adjust the renewal period in any way, the registrar can submit a renew request via EPP to extend the registration period up to a maximum of ten years. If the renew request is for a single year, the registrar is not charged. If the renew request is for more than a single year, the registrar is charged for the additional years that the registration period was extended. If the command is a success, the autoRenewPeriod status is removed from the domain.

Should the registrar wish to delete the registration, the registrar can submit a delete command via EPP. Once a delete request is received, the autoRenewPeriod status is removed from the domain and the redemptionPeriod status is added. The registrar is credited for the renewal fees. For illustration of this process, please refer to Fig. 6 – Auto Renew Grace Period.

The last way move a domain registration out of the Auto Renew state is by successful completion of the Request Transfer process, as described in the following section. If the transfer completes successfully, the autoRenewPeriod status is removed and the transferPeriod status is added.

9.0. REQUEST TRANSFER

A customer can change the sponsoring registrar of a domain registration through the Request Transfer process. This process is an asynchronous, multi-step process that can take many as five days but may occur faster, depending on the level of support from participating Registrars.

The initiation of the transfer process is illustrated in Fig. 8 – Request Transfer. The transfer process begins with a registrar submitting a transfer request. To succeed, the request must meet several criteria. First, the domain status must not contain transferProhibited or pendingTransfer. Second, the initial domain registration must be at least 60 days old or, if transferred prior to the current transfer request, must not have been transferred within the last 60 days. Lastly, the transfer request must contain the correct authInfo (authorization information) value. If all of these criteria are met, the transfer request succeeds and the domain moves into the Pending Transfer state and the pendingTransfer status is added to the domain.

There are four ways to complete the transfer (and move it out of Pending Transfer

status):
1. The transfer is auto-approved.
2. The losing registrar approves the transfer.
3. The losing registrar rejects the transfer.
4. The requesting registrar cancels the transfer.

After a successful transfer request, the domain continues to have the pendingTransfer status for up to five days. During this time, if no other action is taken by either registrar, the domain successfully completes the transfer process and the requesting registrar becomes the new sponsor of the domain registration. This is illustrated in Fig. 9 – Auto Approve Transfer.

At any time during the Pending Transfer state, either the gaining or losing registrar can request the status of a transfer provided they have the correct domain authInfo. Querying for the status of a transfer is illustrated in Fig. 13 – Query Transfer.

During the five-day Pending Transfer state, the losing registrar can accelerate the process by explicitly accepting or rejecting the transfer. If the losing registrar takes either of these actions, the pendingTransfer status is removed. Both of these actions are illustrated in Fig. 10 – Approve Transfer and Fig. 11 – Reject Transfer.

During the five-day Pending Transfer state, the requesting registrar may cancel the transfer request. If the registrar sends a cancel transfer request, the pendingTransfer status is removed. This is shown in Fig. 12 – Cancel Transfer.

If the transfer process is a success, the registry adds the transferPeriod status and removes the pendingTransfer status. If the domain was in the Renew Period state, upon successful completion of the transfer process, this status is removed.

The transferPeriod status remains on the domain for five days. This is illustrated in Fig. 14 – Transfer Grace Period. During this period, the gaining Registrar may delete the domain and obtain a credit for the transfer fees. If the gaining registrar issues a successful delete request during the transferPeriod, the gaining registrar receives a credit for the transfer. The status redemptionPeriod is added to the status of the domain and transferPeriod is removed. The domain then enters the RGP state.

10.0. REDEMPTION GRACE PERIOD

The Redemption Grace Period (RGP) is a service provided by the registry for the benefit of registrars and registrants. The RGP allows a registrar to recover a deleted domain registration. The only way to enter the RGP is through a delete command sent by the sponsoring registrar. A domain in RGP always contains a status of redemptionPeriod. For an illustrated logical flow diagram of this, please refer to Fig. 15 – Redemption Grace Period.

The RGP lasts for 30 days. During this time, the sponsoring registrar may recover the domain through a two-step process. The first step is to send a successful restore command to the registry. The second step is to send a restore report to the registry.

Once the restore command is processed, the registry adds the domain status of pendingRestore to the domain. The domain is now in the Pending Restore state, which lasts for seven days. During this time, the registry waits for the restore report from the Registrar. If the restore report is not received within seven days, the domain transitions back to the RGP state. If the restore report is successfully processed by the registry, the domain registration is restored back to the REGISTERED state. The statuses of pendingRestore and redemptionPeriod are removed from the domain.

After 30 days in RGP, the domain transitions to the Pending Delete state. A status of pendingDelete is applied to the domain and all other statuses are removed. This state lasts for five days and is considered a quiet period for the domain. No commands or other activity can be applied for the domain while it is in this state. Once the five days lapse, the domain is again available for registration.

11.0. DELETE
To delete a domain registration, the sponsoring registrar must send a delete request to the registry. If the domain is in the Add Grace Period, deletion occurs immediately. In all other cases, the deleted domain transitions to the RGP. For a detailed visual diagram of the delete process flow, please refer to Fig. 7 – Delete.

For domain registration deletion to occur successfully, the registry must first ensure the domain is eligible for deletion by conducting two checks. The registry first checks to verify that the requesting registrar is also the sponsoring registrar. If this is not the case, the registrar receives an error message.

The registry then checks the various domain statuses for any restrictions that might prevent deletion. If the domain's status includes either the transferPending or deleteProhibited, the name is not deleted and an error is returned to the registrar.

If the domain is in the Add Grace Period, the domain is immediately deleted and any registration fees paid are credited back to the registrar. The domain is immediately available for registration.

If the domain is in the Renew Grace Period, the Transfer Grace Period or the Auto Renew Grace Period, the respective renewPeriod, transferPeriod or autoRenewPeriod statuses are removed and the corresponding fees are credited to the Registrar. The domain then moves to the RGP as described above.

12.0. ADDITIONAL STATUSES
There are additional statuses that the registry or registrar can apply to a domain registration to limit what actions can be taken on it or to limit its usefulness. This section addresses such statuses that have not already addressed in this response.

Some statuses are applied by the registrar and others are exclusively applied by the registry. Registry-applied statuses cannot be altered by registrars. Status names that registrars can add or remove begin with "client". Status names that only the registry can add or remove begin with "server". These statuses can be applied by a registrar using the EPP domain update request as defined in RFC 5731.

To prevent a domain registration from being deleted, the status values of clientDeleteProhibited or serverDeleteProhibited may be applied by the appropriate party.

To withhold delegation of the domain to the DNS, clientHold or serverHold is applied. This prevents the domain name from being published to the zone file. If it is already published, the domain name is removed from the zone file.

To prevent renewal of the domain registration clientRenewProhibited or serverRenewProhibited is applied by the appropriate party.

To prevent the transfer of sponsorship of a registration, the states clientTransferProhibited or serverTransferProhibited is applied to the domain.

When this is done, all requests for transfer are rejected by the registry.

If a domain registration contains no host objects, the registry applies the status of inactive. Since there are no host objects associated with the domain, by definition, it cannot be published to the zone. The inactive status cannot be applied by registrars.

If a domain has no prohibitions, restrictions or pending operations and the domain also contains sufficient host object references for zone publication, the registry assigns the status of ok if there is no other status set.

There are a few statuses defined by the domain mapping RFC 5731 that our registry does not use. These statuses are: pendingCreate, pendingRenew and pendingUpdate. RFC 5731 also defines some status combinations that are invalid. We acknowledge these and our registry system disallows these combinations.

13.0. RESOURCING
Software Engineering:
- Existing Department Personnel: Project Manager, Development Manager, two Sr. Software Engineers, Sr. Database Engineer, Quality Assurance Engineer
- New Hires: Web Developer, Database Engineer, Technical Writer, Build⁄Deployment Engineer
Systems Engineering:
- Existing Department Personnel: Sr. Director IT Operations, 2 Sr. Systems Administrators, 2 Systems Administrators, 2 Sr. Systems Engineers, 2 Systems Engineers
- New Hires: Systems Engineer
Network Engineering:
- Existing Department Personnel: Sr. Director IT Operations, two Sr. Network Engineers, 2 Network Engineers
- New Hires: Network Engineer
Database Operations:
- Existing Department Personnel: Sr. Database Operations Manager, 2 Database Administrators
Network Operations Center:
- Existing Department Personnel: Manager, 2 NOC Supervisors, 12 NOC Analysts
- New Hires: Eight NOC Analysts

28. Abuse Prevention and Mitigation

Q28 Standard CHAR: 29543

1.0. INTRODUCTION

Donuts will employ strong policies and procedures to prevent and mitigate abuse. Our intention is to ensure the integrity of this top-level domain (TLD) and maintain it as a trusted space on the Internet. We will not tolerate abuse and will use professional, consistent, and fair policies and procedures to identify and address abuse in the legal, operational, and technical realms

Our approach to abuse prevention and mitigation includes the following:

– An Anti-Abuse Policy that clearly defines malicious and abusive behaviors;
– An easy-to-use single abuse point of contact (APOC) that Internet users can use to report the malicious use of domains in our TLD;
– Procedures for investigating and mitigating abuse;
– Procedures for removing orphan glue records used to support malicious

activities;
- Dedicated procedures for handling legal requests, such as inquiries from law enforcement bodies, court orders, and subpoenas;
- Measures to deter abuse of the Whois service; and
- Policies and procedures to enhance Whois accuracy, including compliance and monitoring programs.

Our abuse prevention and mitigation solution leverages our extensive domain name industry experience and was developed based on extensive study of existing gTLDs and ccTLDs for best registry practices. This same experience will be leveraged to manage the new TLD.

2.0. ANTI-ABUSE POLICY

The Anti-Abuse Policy for our registry will be enacted under the Registry-Registrar Agreement, with obligations from that agreement passed on to and made binding upon all registrants, registrars, and resellers. This policy will also be posted on the registry web site and accompanied by abuse point-of-contact contact information (see below). Internet users can report suspected abuse to the registry and sponsoring registrar, and report an orphan glue record suspected of use in connection with malicious conduct (see below).

The policy is especially designed to address the malicious use of domain names. Its intent is to:

1. Make clear that certain types of behavior are not tolerated;
2. Deter both criminal and non-criminal but harmful use of domain names; and
3. Provide the registry with clearly stated rights to mitigate several types of abusive behavior when found.

This policy does not take the place of the Uniform Dispute Resolution Policy (UDRP) or the Uniform Rapid Suspension System (URS), and it is not to be used as an alternate form of dispute resolution or as a brand protection mechanism.

Below is a policy draft based on the anti-abuse policies of several existing TLD registries with exemplary practices (including .ORG, .CA, and .INFO). We plan to adopt the same, or a substantially similar version, after the conclusion of legal reviews.

3.0. TLD ANTI-ABUSE POLICY

The registry reserves the right, at its sole discretion and at any time and without limitation, to deny, suspend, cancel, redirect, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status as it determines necessary for any of the following reasons:

(1) to protect the integrity and stability of the registry;
(2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process;
(3) to avoid any liability, civil or criminal, on the part of the registry operator, its affiliates, subsidiaries, officers, directors, or employees;
(4) to comply with the terms of the registration agreement and the registry’s Anti-Abuse Policy;
(5) registrant fails to keep Whois information accurate and up-to-date;
(6) domain name use violates the registry’s acceptable use policies, or a third party’s rights or acceptable use policies, including but not limited to the infringement of any copyright or trademark;
(7) to correct mistakes made by the registry operator or any registrar in connection with a domain name registration; or
(8) as needed during resolution of a dispute.

Abusive use of a domain is an illegal, malicious, or fraudulent action and includes, without limitation, the following:

- Distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include computer viruses, worms, keyloggers, trojans, and fake antivirus products;
- Phishing: attempts to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication;
- DNS hijacking or poisoning;
- Spam: The use of electronic messaging systems to send unsolicited bulk messages. This includes but is not limited to email spam, instant messaging spam, mobile messaging spam, and the spamming of Internet forums;
- Use of botnets, including malicious fast-flux hosting;
- Denial-of-service attacks;
- Child pornography⁄child sexual abuse images;
- The promotion, encouragement, sale, or distribution of prescription medication without a valid prescription in violation of applicable law; and
- Illegal access of computers or networks.

4.0. SINGLE ABUSE POINT OF CONTACT

Our prevention and mitigation plan includes use of a single abuse point of contact (APOC). This contact will be a role-based e-mail address in the form of “abuse@registry.tld”. This e-mail address will allow multiple staff members to monitor abuse reports. This role-based approach has been used successfully by ISPs, e-mail service providers, and registrars for many years, and is considered an Internet abuse desk best practice.

The APOC e-mail address will be listed on the registry web site. We also will provide a convenient web form for complaints. This form will prompt complainants to provide relevant information. (For example, complainants who wish to report spam will be prompted to submit the full header of the e-mail.) This will help make their reports more complete and accurate.

Complaints from the APOC e-mail address and web form will go into a ticketing system, and will be routed to our abuse handlers (see below), who will evaluate the tickets and execute on them as needed.

The APOC is mainly for complaints about malicious use of domain names. Special addresses may be set up for other legal needs, such as civil and criminal subpoenas, and for Sunrise issues.

5.0. ABUSE INVESTIGATION AND MITIGATION

Our designated abuse handlers will receive and evaluate complaints received via the APOC. They will decide whether a particular issue merits action, and decide what action is appropriate.

Our designated abuse handlers have domain name industry experience receiving, investigating and resolving abuse reports. Our registry implementation plan will leverage this experience and deploy additional resources in an anti-abuse program tailored to running a registry.

We expect that abuse reports will be received from a wide variety of parties, including ordinary Internet users; security researchers and Internet security companies; institutions, such as banks; and law enforcement agencies.

Some of these parties typically provide good forensic data or supporting evidence of the alleged malicious behavior. In other cases, the party reporting an issue may not be familiar with how to provide evidence. It is not unusual, in the Internet industry, that a certain percentage of abuse reports are not actionable because there is insufficient evidence to support the complaint, even after additional investigation.

The abuse handling function will be staffed with personnel who have experience handling abuse complaints. This group will function as an abuse desk to "triage" and investigate reports. Over the past several years, this group has investigated allegations about a variety of problems, including malware, spam, phishing, and child pornography⁄child sexual abuse images.

6.0. POLICIES, PROCEDURES, AND SERVICE LEVELS

Our abuse prevention and mitigation plan includes development of an internal manual for assessing and acting upon abuse complaints. Our designated abuse handlers will use this to ensure consistent and fair processes. To prevent exploitation of internal procedures by malefactors, these procedures will not be published publicly.

Assessing abuse reports requires great care. The goals are accuracy, a zero false-positive rate to prevent harm to innocent registrants, and good documentation.

Different types of malicious activities require different methods of investigation and documentation. The procedures we deploy will address all the abuse types listed in our Anti-Abuse Policy (above). This policy will also contain procedures for assessing complaints about orphan nameservers used for malicious activities.

One of the first steps in addressing abusive or harmful activities is to determine the type of domain involved. Two types of domains may be involved: 1) a "compromised domain"; and⁄or 2) a maliciously registered domain.

A "compromised" domain is one that has been hacked or otherwise compromised by criminals; the registrant is not responsible for the malicious activity taking place on the domain. For example, most domain names that host phishing sites are compromised. The goal in such cases is to inform the registrant of the problem via the registrar. Ideally, such domains are not suspended, since suspension disrupts legitimate activity on the domain.

The second type of potentially harmful domain, the maliciously registered domain, is one registered by a bad actor for the purpose of abuse. Since it has no legitimate use, this type of domain is a candidate for suspension.

In general, we see the registry as the central entity responsible for monitoring abuse of the TLD and passing any complaints received to the domains' sponsoring registrars. In an alleged (though credible) case of malicious use, the case will be communicated to the domain's sponsoring registrar requesting that the registrar investigate, act appropriately, and report on it within a defined time period. Our abuse handlers will also provide any evidence they collect to the registrar.

There are several good reasons for passing a case of malicious domain name use on to the registrar. First, the registrar has a direct relationship and contract with the registrant. It is important to respect this relationship as it pertains both to business in general and any legal perspectives involved. Second, the registrar holds a better position to evaluate and act because the registrar typically has vital information the registry operator does not, including domain purchase details and payment method (i.e., credit card, etc.); the identity of a proxy-protected registrant; the IP address from which the domain purchase was made; and whether a reseller is involved. Finally, it is important the registrar know if a registrant is in violation of registry or registrar policies and terms—the registrar may wish to suspend the registrant's account, or investigate other domains the registrar has registered in this TLD or others.

The registrar is also often best for determining if questionable registrant activity violates the registrar's legal terms of service or the registry Anti-Abuse Policy, and deciding whether to take any action. Registrars will be required to include language in their registrar-registrant contracts that indemnifies the registrar if it takes action and allows the registrar to suspend or cancel a domain name.

If a registrar does not take action within the time indicated by us in the report (i.e., 24 hours), we may take action ourselves. In some cases, we may suspend the domain name(s), and we reserve the right to act directly and immediately. We plan to take action directly if time is of the essence, such as with a malware attack that may cause significant harm to Internet users.

It is important to note that strict service level agreements (SLAs) for abuse response and mitigation are not always appropriate, additional tailoring of any SLAs may be required, depending on the problem. For example, suspending a domain within 24 hours may not be the best course of action when working with law enforcement or a national clearinghouse to address reports of child pornography. Officials may need more than 24 hours to investigate and gather evidence.

7.0. ABUSE MONITORING AND METRICS

In addition to addressing abuse complaints, we will actively monitor the overall abuse status of the TLD, gather intelligence and track abuse metrics to address criminal use of domains in the TLD.

To enable active reporting of problems to the sponsoring registrars, our plan includes proactive monitoring for malicious use of the domains in the TLD. Our goal is to keep malicious activity at an acceptably low level, and mitigate it actively when it occurs—we may do so by using professional blocklists of domain names. For example, professional advisors such as LegitScript (www.legitscript.com) may be used to identify and close down illegal "rogue" Internet pharmacies.

Our approach also incorporates recordkeeping and metrics regarding abuse and abuse reports. These may include:

- The number of abuse reports received by the registry's abuse point of contact described above and the domains involved;
- The number of cases and domains referred to registrars for resolution;
- The number of cases and domains for which the registry took direct action;
- Resolution times (when possible or relevant, as resolution times for compromised domains are difficult to measure).

We expect law enforcement to be involved in only a small percentage of abuse cases and will call upon relevant law enforcement as needed.

8.0. HANDLING REPORTS FROM LAW ENFORCEMENT, COURT ORDERS

The new gTLD Registry Agreement contains this requirement: "Registry Operator shall take reasonable steps to investigate and respond to any reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD. In responding to such reports, Registry Operator will not be required to take any action in contravention of applicable law." (Article 2.8)

We will be responsive as required by Article 2.8. Our abuse handling team will comply with legal processes and leverage both experience and best practices to work effectively with law enforcement and other government agencies. The registry will post a Criminal Subpoena Policy and Procedure page, which will detail how law enforcement and government agencies may submit criminal and civil subpoenas. When we receive valid court orders or seizure warrants from courts or law enforcement agencies of relevant jurisdiction, we will expeditiously review and comply with them.

9.0. PROHIBITING DOMAIN HIJACKINGS AND UNAPPROVED UPDATES

Our abuse prevention and mitigation plan also incorporates registrars that offer domain protection services and high-security access and authentication controls. These include services designed to prevent domain hijackings and inhibit unapproved updates (such as malicious changes to nameserver settings). Registrants will then have the opportunity to obtain these services should they so elect.

10.0. ABUSE POLICY: ADDRESSING INTELLECTUAL PROPERTY INFRINGEMENT

Intellectual property infringement involves three distinct but sometimes intertwined problems: cybersquatting, piracy, and trademark infringement:

- Cybersquatting is about the presence of a trademark in the domain string itself.
- Trademark infringement is the misuse or misappropriation of trademarks – the violation of the exclusive rights attached to a trademark without the authorization of the trademark owner or any licensees. Trademark infringement sometimes overlaps with piracy.
- Piracy involves the use of a domain name to sell unauthorized goods, such as copyrighted music, or trademarked physical items, such as fake brand-name handbags. Some cases of piracy involve trademark infringement.

The Uniform Dispute Resolution Process (UDRP) and the new Uniform Rapid Suspension System (URS) are anti-cybersquatting policies. They are mandatory and all registrants in the new TLD will be legally bound to them. Please refer to our response to Question #29 for details on our plans to respond to URS orders.

The Anti-Abuse Policy for our gTLD will be used to address phishing cases that involve trademarked strings in the domain name. The Anti-Abuse Policy prohibits violation of copyright or trademark; such complaints will be routed to the sponsoring Registrar.

11.0. PROPOSED MEASURES FOR REMOVAL OF ORPHAN GLUE RECORDS

Below are the policies and procedures to be used for our registry in handling orphan glue records. The anti-abuse documentation for our gTLD will reflect these procedures.

By definition, a glue record becomes an "orphan" when the delegation point Name Server (NS) record referencing it is removed without also removing the corresponding glue record. The delegation point NS record is sometimes referred to as the parent NS record.

As ICANN's SSAC noted in its Advisory SAC048 "SSAC Comment on Orphan Glue Records in the Draft Applicant
Guidebook" (http://www.icann.org/en/committees/security/sac048.pdf), "Orphaned glue can be used for abusive purposes; however, the dominant use of orphaned glue supports the correct and ordinary operation of the Domain Name System (DNS)." For example, orphan glue records may be created when a domain (example.tld) is placed on Extensible Provisioning Protocol (EPP) ServerHold or ClientHold status. This use of Hold status is an essential tool for suspending malicious domains. When

placed on Hold, the domain is removed from the zone and will stop resolving. However, any child nameservers (now orphan glue) of that domain (e.g., ns1.example.tld) are left in the zone. It is important to keep these orphan glue records in the zone so that any innocent sites using that nameserver will continue to resolve.

We will use the following procedure—used by several existing registries and considered a generally accepted DNS practice—to manage orphan glue records.. When a registrar submits a request to delete a domain, the registry first checks for the existence of glue records. If glue records exist, the registry checks to see if other domains in the registry are using the glue records. If other domains in the registry are using the glue records, then registrar EPP requests to delete the domain will fail until no other domains are using the glue records. (This functionality is currently in place for the .ORG registry.) However, if a registrar submits a complaint that orphan glue is being used maliciously and the malicious conduct is confirmed, the registry operator will remove the orphan glue record from the zone file via an exceptional process.

12.0. METHODS TO PROMOTE WHOIS ACCURACY

12.1. ENFORCING REQUIRED CONTACT DATA FIELDS

We will offer a “thick” registry system. In this model, all key contact details for each domain name will be stored in a central location by the registry. This allows for better access to domain data and provides uniformity in storing the information.

As per the EPP specification, certain contact data fields are mandatory. Our registry will enforce those, plus certain other fields as necessary. This ensures that registrars are providing required domain registration data. The following fields (indicated as “MANDATORY”) will be mandatory at a minimum:

Contact Name [MANDATORY]
Street1 [MANDATORY]
City [MANDATORY]
State⁄Province [optional]
Country [MANDATORY]
Postal Code [optional]
Registrar Phone [MANDATORY]
Phone Ext [optional]
Fax [optional]
Fax Ext [optional]
Email [MANDATORY]

In addition, our registry will verify formats for relevant individual data fields (e.g. e-mail, and phone⁄fax numbers) and will reject any improperly formatted submissions. Only valid country codes will be allowed, as defined by the ISO 3166 code list.

We will reject entries that are clearly invalid. For example, a contact that contains phone numbers such as 555.5555, or registrant names that consist only of hyphens, will be rejected.

12.2. POLICIES AND PROCEDURES TO ENHANCE WHOIS ACCURACY COMPLIANCE

We generally will rely on registrars to enforce WHOIS accuracy measures, but will also rely on review and audit procedures to enhance compliance.

As part of our RRA (Registry-Registrar Agreement), we will require each registrar to be responsible for ensuring the input of accurate Whois data by its registrants. The Registrar⁄Registered Name Holder Agreement will include specific clauses to ensure accuracy of Whois data, as per ICANN requirements, and to give the registrar the right to cancel or suspend registrations if the registered name holder fails to respond to the registrar's query regarding accuracy of data. In addition, the Anti-Abuse Policy for our registry will give the registry the right to suspend, cancel, etc., domains that have invalid Whois data.

As part of our RRA (Registry-Registrar Agreement), we will include a policy similar to the one below, currently used by the Canadian Internet Registration Authority (CIRA), the operator of the .CA registry. It will require the registrar to help us verify contact data.

"CIRA is entitled at any time and from time to time during the Term…to verify: (a) the truth, accuracy and completeness of any information provided by the Registrant to CIRA, whether directly, through any of the Registrars of Record or otherwise; and (b) the compliance by the Registrant with the provisions of the Agreement and the Registry PRP. The Registrant shall fully and promptly cooperate with CIRA in connection with such verification and shall give to CIRA, either directly or through the Registrar of Record such assistance, access to and copies of, such information and documents as CIRA may reasonably require to complete such verification. CIRA and the Registrant shall each be responsible for their own expenses incurred in connection with such verification."
http:⁄⁄www.cira.ca⁄assets⁄Documents⁄Legal⁄Registrants⁄registrantagreement.pdf

On a periodic basis, we will perform spot audits of the accuracy of Whois data in the registry. Questionable data will be sent to the sponsoring registrars as per the above policy.

All accredited registrars have agreed with ICANN to obtain contact information from registrants, and to take reasonable steps to investigate and correct any reported inaccuracies in contact information for domain names registered through them. As part of our RRA (Registry-Registrar Agreement), we will include a policy that allows us to de-accredit any registrar who a) does not respond to our Whois accuracy requests, or b) fails to update Whois data or delete the name within 15 days of our report of invalid WHOIS data. In order to allow for inadvertent and unintentional mistakes by a registrar, this policy may include a "three strikes" rule under which a registrar may be de-accredited after three failures to comply.

12.3. PROXY⁄PRIVACY SERVICE POLICY TO CURB ABUSE

In our TLD, we will allow the use of proxy⁄privacy services. We believe that there are important, legitimate uses for such services. (For example, to protect free speech rights and avoid receiving spam.)

However, we will limit how proxy⁄privacy services are offered. The goal of this policy is to make proxy⁄privacy services unattractive to abusers, namely the spammers and e-criminals who use such services to hide their identities. We believe the policy below will enhance WHOIS accuracy, will help deter the malicious use of domain names in our TLD, and will aid in the investigation and mitigation of abuse complaints.

Registry policy will require the following, and all registrars and their registrants and resellers will be bound to it contractually:

a. Registrants must provide complete and accurate contact information to their registrar (or reseller, if applicable).. Domains that do not meet this policy may be suspended.
b. Registrars and resellers must provide the underlying registrant information to the registry operator, upon written request, during an abuse investigation. This

information will be held in confidence by the registry operator.
c. The registrar or reseller must publish the underlying registrant information in the Whois if it is determined by the registry operator or the registrar that the registrant has breached any terms of service, such as the TLD Anti-Abuse Policy.

The purpose of the above policy is to ensure that, in case of an abuse investigation, the sponsoring registrar has access to the registrant's true identity, and can provide that data to the registry. If it is clear the registrant has violated the TLD's Anti-Abuse Policy or other terms of service, the registrant's identity will be published publicly via the Whois, where it can be seen by the public and by law enforcement.

13.0. REGISTRY-REGISTRAR CODE OF CONDUCT AS RELATED TO ABUSE

Donuts does not currently intend to become a registrar for this TLD. Donuts and our back-end technical operator will comply fully with the Registry Code of Conduct specified in the New TLD Registry Agreement, Specification 9. For abuse issues, we will comply by establishing an adequate "firewall" between our registry operations and the operations of any affiliated registrar. As the Code requires, the registry will not "directly or indirectly show any preference or provide any special consideration to any Registrar with respect to operational access to registry systems and related registry services". Here is a non-exhaustive list of specific steps to be taken to enforce this:

- Abuse complaints and cases will be evaluated and executed upon using the same criteria and procedures, regardless of a domain's sponsoring registrar.
- Registry personnel will not discuss abuse cases with non-registry personnel or personnel from separate entities operating under the company. This policy is designed to both enhance security and prevent conflict of interest.
- If a compliance function is involved, the compliance staff will have responsibilities to the registry only, and not to a registrar we may be "affiliated" with at any point in the future. For example, if a compliance staff member is assigned to conduct audits of WHOIS data, that person will have no duty to any registrar business we may be operating at the time. The person will be free of conflicts of interest, and will be enabled to discharge his or her duties to the registry impartially and effectively.

14.0. CONTROLS TO ENSURE PROPER ACCESS TO DOMAIN FUNCTIONS

Our registry incorporates several measures to ensure proper access to domain functions, including authentication provisions in the RRA relative to notification and contact updates via use of AUTH-INFO codes.

IP address access control lists, SSL certificates, and proper authentication will be used to control registrar access to the registry system. Registrars will be given access only to perform operations on the objects they sponsor.

Every domain will have a unique AUTH-INFO code as per EPP RFCs. The AUTH-INFO code is a 6- to 16-character code assigned by the registrar at the time the name is created. Its purpose is to aid identification of the domain owner so proper authority can be established. (It is the "password" to the domain name.) Registrars must use the domain's password to initiate a Registrar-to-Registrar transfer. It is used to ensure that domain updates (update contact information, transfer, or deletion) are undertaken by the proper registrant, and that this registrant is adequately notified of domain update activity. Only the sponsoring Registrar of a domain has access to the domain's AUTH-INFO code stored in the registry, and this is accessible only via encrypted, password-protected channels.

Our Registry-Registrar contract will require that each registrar assign a unique

AUTH-INFO code to every domain it creates. Due to security risk, registrars should not assign the same AUTH-INFO code to multiple domains.

Information about other registry security measures such as encryption and security of Registrar channels are confidential to ensure the security of the registry system. Details can be found in our response to Question #30(b).

15.0. RESOURCING PLAN

Our back-end registry operator will perform the majority of Abuse Prevention and Mitigation services for this TLD, as required by our agreement with them. Donuts staff will supervise the activity of the provider. In some cases Donuts staff will play a direct role in the handling of abuse cases.

The compliance department of our registry operator has two full time staff members who are trained in DNS, the investigation of abuse complaints, and related specialties. The volume of abuse activity will be gauged and additional staff hired by our back-end registry operator as required to meet their SLA commitments. In addition to the two full-time members, they expect to retain the services of one or more outside contractors to provide additional security and anti-abuse expertise – including advice on the effectiveness of our policies and procedures.

Finally, Donuts’ Legal Department will have one attorney whose role includes the oversight of legal issues related to abuse, and interaction with courts and law enforcement.

29. Rights Protection Mechanisms

Q29 Standard CHAR: 25021

1.0. INTRODUCTION

To minimize abusive registrations and other activities that affect the legal rights of others, our approach includes well-developed policies for rights protection, both during our TLD’s rollout period and on an ongoing basis. As per gTLD Registry Agreement Specification 7, we will offer a Sunrise Period and a Trademark Claims service during the required time periods, we will use the Trademark Clearinghouse, and we will implement Uniform Rapid Suspension (URS) on an ongoing basis. In addition to these newly mandated ICANN protections, we will implement two other trademark protections that were developed specifically for the new TLD program. These additional protections are: (i) a Domain Protected Marks List (DPML) for the blocking of trademarked strings across multiple TLDs; and (ii) a Claims Plus product to alert registrars to registrations that potentially infringe existing marks.

Below we detail how we will fulfill these requirements and further meet or exceed ICANN’s requirements. We also describe how we will provide additional measures specific to rights protection above ICANN’s minimum, including abusive use policies, takedown procedures, and other covenants.

Our RPM approach leverages staff with extensive experience in a large number of gTLD and ccTLD rollouts, including the Sunrises for .CO, .MOBI, .ASIA, .EU, .BIZ, .US., .TRAVEL, TEL, .ME, and .XXX. This staff will utilize their first-hand, practical experience and will effectively manage all aspects of Sunrise, including domain application and domain dispute processes.

The legal regime for our gTLD will include all of the ICANN-mandated protections, as well as some independently developed RPMs proactively included in our Registry-Registrar Agreement. Our RPMs exceed the ICANN-required baseline. They are:

- Reserved names: to protect names specified by ICANN, including the necessary geographic names.
- A Sunrise Period: adhering to ICANN requirements, and featuring trademark validation via the Trademark Clearinghouse.
- A Trademark Claims Service: offered as per ICANN requirements, and active after the Sunrise period and for the required time during wider availability of the TLD.
- Universal Rapid Suspension (URS)
- Uniform Dispute Resolution Process (UDRP)
- Domain Protected Marks List (DPML)
- Claims Plus
- Abusive Use and Takedown Policies

2.0. NARRATIVE FOR Q29 FIGURE 1 OF 1

Attachment A, Figure 1, shows Rollout Phases and the RPMs that will be used in each. As per gTLD Registry Agreement Specification 7, we will offer a Sunrise Period and a Trademark Claims service during the required time periods. In addition, we will use the Trademark Clearinghouse to implement URS on an ongoing basis.

3.0. PRE-SUNRISE: RESERVED AND PREMIUM NAMES

Our Pre-sunrise phase will include a number of key practices and procedures. First, we will reserve the names noted in the gTLD Registry Agreement Specification 5. These domains will not be available in Sunrise or subsequent registration periods. As per Specification 5, Section 5, we will provide national governments the opportunity to request the release of their country and territory names for their use. Please also see our response to Question 22, “Protection of Geographic Names.”

We also will designate certain domains as “premium” domains. These will include domains based on generic words and one-character domains. These domains will not be available in Sunrise, and the registry may offer them via special means such as auctions and RFPs.

As an additional measure, if a trademark owner objects to a name on the premium name list, the trademark owner may petition to have the name removed from the list and made available during Sunrise. The trademark must meet the Sunrise eligibility rules (see below), and be an exact match for the domain in question. Determinations of whether such domains will be moved to Sunrise will be at the registry’s sole discretion.

4.0. SUNRISE

4.1. SUNRISE OVERVIEW

Sunrise registration services will be offered for a minimum of 30 days during the pre-launch phase. We will notify all relevant trademark holders in the Trademark Clearinghouse if any party is seeking a Sunrise registration that is an identical match to the name to be registered during Sunrise.

As per the Sunrise terms, affirmed via the Registry-Registrar Agreement and the

Registrar-Registrant Agreement, the domain applicant will assert that it is qualified to hold the domain applied for as per the Sunrise Policy and Rules.

We will use the Trademark Clearinghouse to validate trademarks in the Sunrise.

If there are multiple valid Sunrise applications for the same domain name string, that string will be subject to auction between only the validated applicants. After receipt of payment from the auction winning bidder, that party will become the registrant of the domain name. (note: in the event one of the identical, contending marks is in a trademark classification reflective of the TLD precedence to that mark may be given during Sunrise).

Sunrise applicants may not use proxy services during the application process.

4.2. SUNRISE: ELIGIBLE RIGHTS

Our Sunrise Eligibility Requirements (SERs) are:

1. Ownership of a qualifying mark.

a. We will honor the criteria in ICANN’s Trademark Clearinghouse document section 7.2, number (i): The registry will recognize and honor all word marks that are nationally or regionally [see Endnote 1] registered and for which proof of use — which can be a declaration and a single specimen of current use - was submitted to, and validated by, the Trademark Clearinghouse.

b. In addition, we may accept marks that are not found in the Trademark Clearinghouse, but meet other criteria, such as national trademark registrations or common law rights.

2. Representation by the applicant that all provided information is true and correct; and

3. Provision of data sufficient to document rights in the trademark. (See information about required Sunrise fields, below).

4.3. SUNRISE TRADEMARK VALIDATION

Our goal is to award Sunrise names only to applicants who are fully qualified to have them. An applicant will be deemed to be qualified if that applicant has a trademark that meets the Sunrise criteria, and is seeking a domain name that matches that trademark, as per the Sunrise rules.

Accordingly, we will validate applications via the Trademark Clearinghouse. We will compare applications to the Trademark Clearinghouse database, and those that match (as per the Sunrise rules) will be considered valid applications.

An application validated according to Sunrise rules will be marked as “validated,” and will proceed. (See “Contending Applications,” below.) If an application does not qualify, it will be rejected and will not proceed.

To defray the costs of trademark validation and the Trademark Claims Service, we will charge an application and⁄or validation fee for every application.

In January 2012, the ICANN board was briefed that “An ICANN cross-functional team is continuing work on implementation of the Trademark Clearinghouse according to a project plan providing for a launch of clearinghouse operations in October 2012. This will allow approximately three months for rights holders to begin recording trademark data in the Clearinghouse before any new gTLDs begin accepting registrations (estimated in January 2013).” (http:⁄⁄www.icann.org⁄en⁄minutes⁄board-briefing-materials-4-05jan12-en.pdf) The Clearinghouse Implementation Assistance Group (IAG), which Donuts is participating in, is working through a large number of process and technical issues as of this writing. We will follow the progress of this work, and plan our implementation details based on the final specifications.

Compliant with ICANN policy, our registry software is designed to properly check domains and compare them to marks in the Clearinghouse that contain punctuation, spaces, and special symbols.

4.5. CONTENDING APPLICATIONS, SUNRISE AUCTIONS

After conclusion of the Sunrise Period, the registry will finish the validation process. If there is only one valid application for a domain string, the domain will be awarded to that applicant. If there are two or more valid applications for a domain string, only those applicants will be invited to participate in a closed auction for the domain name. The domain will be awarded to the auction winner after payment is received.

After a Sunrise name is awarded to an applicant, it will then remain under a “Sunrise lock” status for a minimum of 60 days in order to allow parties to file Sunrise Challenges (see below). Locked domains cannot be updated, transferred, or deleted.

When a domain is awarded and granted to an applicant, that domain will be available for lookup in the public Whois. Any party may then see what domains have been awarded, and to which registrants. Parties will therefore have the necessary information to consider Sunrise Challenges.

Auctions will be conducted by very specific rules and ethics guidelines. All employees, partners, and contractors of the registry are prohibited from participating in Sunrise auctions.

4.6. SUNRISE DISPUTE RESOLUTION PROCESS (SUNRISE CHALLENGES)

We will retain the services of a well-known dispute resolution provider (such as WIPO) to help formulate the language of our Sunrise Dispute Resolution Process (SDRP, or “Sunrise Challenge”) and hear the challenges filed under it. All applicants and registrars will be contractually obligated to follow the decisions handed down by the dispute resolution provider.

Our SDRP will allow challenges based on the following grounds, as required by ICANN. These will be part of the Sunrise eligibility criteria that all registrants (applicants) will be bound to contractually:

(i) at the time the challenged domain name was registered, the registrant did not hold a trademark registration of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty;

(ii) the domain name is not identical to the mark on which the registrant based its Sunrise registration;

(iii) the trademark registration on which the registrant based its Sunrise registration is not of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; or

(iv) the trademark registration on which the domain name registrant based its Sunrise registration did not issue on or before the effective date of the Registry Agreement and was not applied for on or before ICANN announced the applications received.

Our SDRP will be based generally on some SDRPs that have been used successfully in past TLD launches. The Sunrise Challenge Policies and Rules used in the .ASIA and .MOBI TLDs (minus their unique eligibility criteria) are examples.

We expect that that there will be three possible outcomes to a Sunrise Challenge:

1. Original registrant proves his⁄her right to the domain. In this case the registrant keeps the domain and it is unlocked for his⁄her use.
2. Original registrant is not eligible or did not respond, and the challenger proved his⁄her right to the domain. In this case the domains is awarded to the complainant.
3. Neither the original registrant nor the complainant proves rights to the domain. In this case the domain is cancelled and becomes available at a later date via a mechanism to be determined by the registry operator.

After any Sunrise name is awarded to an applicant, it will remain under a “Sunrise Lock” status for at least 60 days so that parties can file Sunrise Challenges. During this Sunrise Lock period, the domain will not resolve and cannot be modified, transferred, or deleted by the sponsoring registrar. A domain name will be unlocked at the end of that lock period only if it is not subject to a Sunrise Challenge. Challenged domains will remain locked until the dispute resolution provider has issued a decision, which the registry will promptly execute.

5.0. TRADEMARK CLAIMS SERVICES

The Trademark Claims Service requirements are well-defined in the Applicant Guidebook, in Section 6 of the “Trademark Clearinghouse” attachment. We will comply with the details therein. We will provide Trademark Claims services for marks in the Trademark Clearinghouse post-Sunrise and then for at least the first 60 days that the registry is open for general registration (i.e. during the first 60 days in the registration period(s) after Sunrise). The Trademark Claims service will provide clear notice to a prospective registrant that another party has a trademark in the Clearinghouse that matches the applied-for domain name—this is a notice to the prospective registrant that it might be infringing upon another party’s rights.

The Trademark Clearinghouse database will be structured to report to registries when registrants are attempting to register a domain name that is considered an “Identical Match” with the mark in the Clearinghouse. We will build, test, and implement an interface to the Trademark Clearinghouse before opening our Sunrise period. As domain name applications come into the registry, those strings will be compared to the contents of the Clearinghouse.

If the domain name is registered in the Clearinghouse, the registry will promptly notify the applicant. We will use the notice form specified in ICANN’s Module 4, “Trademark Clearinghouse” document. The specific statement by the prospective registrant will warrant that: (i) the prospective registrant has received notification that the mark(s) is included in the Clearinghouse; (ii) the prospective registrant has received and understood the notice; and (iii) to the best of the prospective registrant’s knowledge, the registration and use of the requested domain name will not infringe on the rights that are the subject of the notice.

The Trademark Claims Notice will provide the prospective registrant access to the Trademark Clearinghouse Database information referenced in the Trademark Claims Notice. The notice will be provided in real time (or as soon as possible) without cost to the prospective registrant or to those notified.

“Identical Match” is defined in ICANN’s Module 4, “Trademark Clearinghouse” document, paragraph 6.1.5. We will examine the Clearinghouse specifications and protocol carefully when they are published. To comply with ICANN policy, the software for our registry will properly check domains and compare them to marks in the Clearinghouse that contain punctuation, spaces, and special symbols.

6.0. GENERAL REGISTRATION

This is the general registration period open to all registrants. No trademark or other qualification will be necessary in order to apply for a domain in this period.

Domain names awarded via the Sunrise process, and domain strings still being contended via the Sunrise process cannot be registered in this period. This will protect the interests of all Sunrise applicants.

7.0. UNIFORM RAPID SUSPENSION (URS)

We will implement decisions rendered under the URS on an ongoing basis. (URS will not apply to Sunrise names while they are in Sunrise Lock period; during that time those domains are subject to Sunrise policy and Sunrise Challenge instead.)

As per URS policy, the registry will receive notice of URS actions from ICANN-approved URS providers. As per ICANN’s URS requirements, we will lock the domain within 24 hours of receipt of the Notice of Complaint from the URS Provider. Locking means that the registry restricts all changes to the registration data, including transfer and deletion of domain names, though names will continue to resolve.

Our registry’s compliance team will oversee URS procedures. URS e-mails from URS providers will be directed immediately to the registry’s Support staff, which is on duty 24⁄7⁄365. Support staff will be responsible for executing the directives from the URS provider, and all support staff will receive training in the proper procedures.

Support staff will notify the URS Provider immediately upon locking the domain name, via e-mail.

Support staff for the registry will retain all copies of e-mails from the URS providers. Each case or order will be assigned a tracking or ticket number. This number will be used to track the status of each opened URS case through to resolution via a database.

Registry staff will then execute further operations upon notice from the URS providers. Each URS provider is required to specify the remedy and required actions of the registry, with notification to the registrant, the complainant, and the sponsoring registrar.

The guidelines provide that if the complainant prevails, the registry “shall suspend the domain name, which shall remain suspended for the balance of the registration period and would not resolve to the original web site. The nameservers shall be redirected to an informational web page provided by the URS Provider about the URS. The WHOIS for the domain name shall continue to display all of the information of the original Registrant except for the redirection of the nameservers. In addition, the WHOIS shall reflect that the domain name will not be able to be transferred, deleted or modified for the life of the registration.” We will execute the DNS re-pointing required by the URS guidelines, and the domain and its WHOIS data will remain unaltered until the domain expires, as per the ICANN requirements.

8.0. ONGOING RIGHTS PROTECTION MECHANISMS - UDRP

As per ICANN policy, all domains in the TLD will be subject to a Uniform Dispute Resolution Process (UDRP). (Sunrise domains will first be subject to the ICANN-mandated Sunrise SDRP until the Sunrise Challenge period is over, after which those domains will then be subject to UDRP.)

9.0 ADDITIONAL RIGHTS PROTECTION MECHANISMS NOT REQUIRED BY ICANN

All Donuts TLDs have two new trademark protection mechanisms developed specifically for the new TLD program. These mechanisms exceed the extensive protections mandated by ICANN. These new protections are:

9.1 Claims Plus: This service will become available at the conclusion of the Trademark Claims service, and will remain available for at least the first five years of registry operations. Trademark owners who are fully registered in the Trademark Clearinghouse may obtain Claims Plus for their marks. We expect the service will be at low or no cost to trademark owners (contingent on Trademark Clearinghouse costs to registries). Claims Plus operates much like Trademark Claims with the exception that notices of potential trademark infringement are sent by the registry to any registrar whose customer performs a check-command or Whois query for a string subject to Claims Plus. Registrars may then take further implementation steps to advise their customers, or use this data to better improve the customer experience. In addition, the Whois at the registry website will output a full Trademark Claims notice for any query of an unregistered name that is subject to Claims Plus. (Note: The ongoing availability of Claims Plus will be contingent on continued access to a Trademark Clearinghouse. The technical viability of some Claims Plus features will be affected by eventual Trademark Clearinghouse rules on database caching).

9.2 Domain Protected Marks List: The DPML is a rights protection mechanism to assist trademark holders in protecting their intellectual property against undesired registrations of strings containing their marks. The DPML prevents (blocks) registration of second level domains that contain a trademarked term (note: the standard for DPML is “contains”— the protected string must contain the trademarked term). DPML requests will be validated against the Trademark Clearinghouse and the process will be similar to registering a domain name so the process will not be onerous to trademark holders. An SLD subject to DPML will be protected at the second level across all Donuts TLDs (i.e. all TLDs for which this SLD is available for registration). Donuts may cooperate with other registries to extend DPML to TLDs that are not operated by Donuts. The cost of DPML to trademark owners is expected to be significantly less than the cost of actually registering a name.

10.0 ABUSIVE USE POLICIES AND TAKEDOWN PROCEDURES

In our response to Question #28, we describe our anti-abuse program, which is designed to address malware, phishing, spam, and other forms of abuse that may harm Internet users. This program is designed to actively discover, verify, and mitigate problems without infringing upon the rights of legitimate registrants. This program is designed for use in the open registration period. These procedures include the reporting of compromised websites⁄domains to registrars for cleanup by the registrants and their hosting providers. It also describes takedown procedures, and the timeframes and circumstances that apply for suspending domain names used improperly. Please see the response to Question #28 for full details.

We will institute a contractual obligation that proxy protection be stripped away if a domain is proven to be used for malicious purposes. For details, please see “Proxy⁄Privacy Service Policy to Curb Abuse” in the response to Question 28.

11.0. REGISTRY-REGISTRAR CODE OF CONDUCT AS RELATED TO RIGHTS PROTECTION

We will comply fully with the Registry Code of Conduct specified in the New TLD Registry Agreement, Specification 9. In rights protection matters, we will comply by establishing an adequate "firewall" between the operations of any registrar we establish and the operations of the registry. As the Code requires, we will not "directly or indirectly show any preference or provide any special consideration to any registrar with respect to operational access to registry systems and related registry services". Here is a non-exhaustive list of specific steps we will take to accomplish this:

- We will evaluate and execute upon all rights protection tasks impartially, using the same criteria and procedures, regardless of a domain's sponsoring registrar.
- Any registrar we establish or have established at the time of registry launch will not receive preferential access to any premium names, any auctions, etc. Registry personnel and any registrar personnel that we may employ in the future will be prohibited from participating as bidders in any auctions for Landrush names.
- Any registrar staff we may employ in the future will have access to data and records relating only to the applications and registrations made by any registrar we establish, and will not have special access to data related to the applications and registrations made by other registrars.
- If a compliance function is involved, the compliance staffer will be responsible to the registry only, and not to a registrar we own or are "affiliated" with. For example, if a compliance staff member is assigned to conduct audits of WHOIS data, that staffer will not have duties with the registrar business. The staffer will be free of conflicts of interest, and will be enabled to discharge his or her duties to the registry effectively and impartially, regardless of the consequences to the registrar.

12.0. RESOURCING PLAN

Overall management of RPMs is the responsibility of Donuts' VP of Business Operations. Our back-end registry operator will perform the majority of operational work associated with RPMs, as required by our agreement with them. Donuts VP of Business Operations will supervise the activity of this vendor.

Resources applied to RPMs include:

1. Legal team
a. We will have at least one legal counsel who will be dedicated to the registry with previous experience in domain disputes and Sunrise periods and will oversee the compliance and support teams with regard to the legal issues related to Sunrise and RPM's
b. We have outside counsel with domain and rights protection experience that is available to us as necessary
2. Dispute Resolution Provider (DRP): The DRP will help formulate Sunrise Rules and Policy, Sunrise Dispute Resolution Policy. The DRP will also examine challenges, but the challenger will be required to pay DRP fees directly to the DRP.
3. Compliance Department and Tech Support: There will be three dedicated personnel assigned to these areas. This staff will oversee URS requests and abuse reports on an ongoing basis.
4. Programming and technical operations. There are four dedicated personnel assigned to these functions.
5. Project Manager: There will be one person to coordinate the technical needs of this group with the registry IT department.

13.0. ENDNOTES

1 "Regional" is understood to be a trans-national trademark registry, such as the

European Union registry or the Benelux Office for Intellectual Property.

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

Q30A Standard CHAR: 19646

1.0. INTRODUCTION

Our Information Security (IS) Program and associated IS Policy, Standards and Procedures apply to all Company entities, employees, contractors, temps, systems, data, and processes. The Security Program is managed and maintained by the IS Team, supported by Executive Management and the Board of Directors.

Data and systems vary in sensitivity and criticality and do not unilaterally require the same control requirements. Our security policy classifies data and systems types and their applicable control requirements. All registry systems have the same data classification and are all managed to common security control framework. The data classification applied to all registry systems is our highest classification for confidentiality, availability and integrity, and the supporting control framework is consistent with the technical and operational requirements of a registry, and any supporting gTLD string, regardless of its nature or size. We have the experienced staff, robust system architecture and managed security controls to operate a registry and TLD of any size while providing reasonable assurance over the security, availability, and confidentiality of the systems supporting critical registry functions (i.e., registration services, registry databases, zone administration, and provision of domain name resolution services).

This document describes the governance of our IS Program and the control frameworks our security program aligns to (section 1.0), Security Policy requirements (section 2.0); security assessments conducted (see section 3.0), our process for executive oversight and visibility of risks to ensure continuous improvement (section 4.0), and security commitments to registrants (section 5). Details regarding how these control requirements are implemented, security roles and responsibilities and resources supporting these efforts are included in Security Policy B response.

2.0. INFORMATION SECURITY PROGRAM

The IS Program for our registry is governed by an IS Policy aligned to the general clauses of ISO 27001 requirements for an Information Security Management System (ISMS) and follows the control objectives where appropriate, given the data type and resulting security requirements. (ISO 27001 certification for the registry is not planned, however, our DNS⁄DNSSEC solution is 27001 certified). The IS Program follows a Plan-Do-Check-Act (PDCA) model of continuous improvement to ensure that the security program grows in maturity and that we provide reasonable assurance to our shareholders and Board of Directors that our systems and data are secure.

The High Security Top Level Domain (HSTLD) control framework incorporates ISO 27002, the code of practice for implementing an ISO 27001 ISMS. Therefore, our security program is already closely aligned HSTLD control framework. Furthermore, we agree to abide by the HSTLD Principle 1 and criteria 1.1 - 1.3. (See specifics in Security Policy B response):

Registry systems will be in-scope for Sarbanes-Oxley (SOX) compliance and will follow the SOX control framework governing access control, account management, change management, software development life cycle (SDLC), and job monitoring of all systems. Registry systems will be tested frequently by the IS team for compliance and audited by our internal audit firm, Protiviti, and external audit firm, Price Waterhouse Coopers (PWC), for compliance.

2.1. SECURITY PROGRAM GOVERNANCE

Our Information Security Program is governed by IS Policy, supported by standards, and guided by procedures to ensure uniformed compliance to the program. Standards and associated procedures in support of the policy are shown in Attachment A, Figure 1. Security Program documents are updated annually or upon any system or environment change, new legal or regulatory requirements, and/or findings from risk assessments. Any updates to security program are reviewed and approved by the Executive Vice President (EVP) of Information Technology (IT), EVP of Legal & General Counsel, and the EVP of People Operations before dissemination to all employees.

All employees are required to sign the IS Policy upon hire, upon any major changes, and/or annually. By signing the IS Policy, employees agree to abide by the supporting Standards and Procedures applicable to their job roles. To enable signing of the IS Policy, employees must pass a test to ensure competent understanding of the IS Policy and its key requirements.

3.0. INFORMATION SECURITY POLICY

3.1. INFORMATION ASSET CLASSIFICATION

The following data classification is applied to registry systems: High Business Impact (HBI): Business Confidential in accordance with the integrity, availability and confidentiality requirements of registry operations. All registry systems will follow Security Policy requirements for HBI systems regardless of the nature of the TLD string, financial materiality or size. HBI data if not properly secured, poses a high degree of risk to the Company and includes data pertaining to the Company’s adherence to legal, regulatory and compliance requirements, mergers and acquisitions (M&A), and confidential data inclusive of, but is not limited to: Personally Identifiable Information (PII) (credit card data, Social Security Numbers (SSN) and account numbers); materially important financial information (before public disclosure), and information which the Board of Directors/Executive team deems to be a trade secret, which, if compromised, would cause grave harm to the execution of our business model.

HBI safeguards are designed, implemented and measured in alignment with confidentiality, integrity, availability and privacy requirements characterized by legal, regulatory and compliance obligations, or through directives issued by the Board of Directors (BOD) and Executive team. Where guidance is provided, such as the Payment Card Industry (PCI) Data Security Standard (DSS) Internal Audit Risk Control Matrices (RCMs), local, state and federal laws, and other applicable regulations, we put forth the appropriate level of effort and resources to meet those obligations. Where there is a lack of guidance or recommended safeguards, Risk Treatment Plans (RTP’s) are designed in alignment with our standard risk management practices.

Other data classifications for Medium Business Impact (MBI): Business Sensitive and Low Business Impact (LBI): Public do not apply to registry systems.

3.2. INFORMATION ASSET MANAGEMENT

All registry systems have a designated owner and/or custodian who ensures appropriate security classifications are implemented and maintained throughout the lifecycle of the asset and that a periodic review of that classification is conducted. The system owner is also responsible for approving access and the type of access granted. The IS team, in conjunction with Legal, is responsible for defining the legal, regulatory and compliance requirements for registry system and data.

3.3. INFORMATION ASSET HANDLING, STORAGE & DISPOSAL

Media and documents containing HBI data must adhere to their respective legal, regulatory and compliance requirements and follow the HBI Handling Standard and the retention requirements within the Document Retention Policy.

3.4. ACCESS CONTROL

User authentication is required to access our network and system resources. We follow a least-privileged role based access model. Users are only provided access to the systems, services or information they have specifically been authorized to use by the system owner based on their job role. Each user is uniquely identified by an ID associated only with that user. User IDs must be disabled promptly upon a user’s termination, or job role change.

Visitors must sign-in at the front desk of any company office upon arrival and escorted by an employee at all times. Visitors must wear a badge while on-site and return the badge when signing out at the front desk. Dates and times of all visitors as well as the name of the employee escorting them must be tracked for audit purposes.

Individuals permitted to access registry systems and HBI information must follow the HBI Identity & Access Management Standard. Details of our access controls are described in Part B of Question 30 response including; technical specifications of access management through Active Directory, our ticketing system, physical access controls to systems and environmental conditions at the datacenter.

3.5. COMMUNICATIONS & OPERATIONAL SECURITY

3.5.1. MALICIOUS CODE

Controls shall be implemented to protect against malicious code including but not limited to:
- Identification of vulnerabilities and applicable remediation activities, such as patching, operating system & software upgrades and⁄or remediation of web application code vulnerabilities.
- File-integrity monitoring shall be used, maintained and updated appropriately.
- An Intrusion Detection Solution (IDS) must be implemented on all HBI systems, maintained & updated continuously.
- Anti-virus (AV) software must be installed on HBI classified web & application systems and systems that provide access to HBI systems. AV software and virus definitions are updated on a regular basis and logs are retained for no less than one year.

3.5.2. THREAT ANALYSIS & VULNERABILITY MANAGEMENT

On a regular basis, IS personnel must review newly identified vulnerability advisories from trusted organizations such as the Center for Internet Security, Microsoft, SANS Institute, SecurityFocus, and the CERT at Carnegie-Mellon University. Exposure to such vulnerabilities must be evaluated in a timely manner and appropriate measures taken to communicate vulnerabilities to the system owners, and remediate as required by the Vulnerability Management Standard. Internal and external network vulnerability scans, application & network layer penetration testing must be performed by qualified internal resource or an external third party at least quarterly or upon any significant network change. Web application vulnerability scanning is to be performed on a continual basis for our primary web properties applicable to their release cycles.

3.5.3. CHANGE CONTROL

Changes to HBI systems including operating system upgrades, computing hardware, networks and applications must follow the Change Control Standard and procedures described in Security Policy question 30b.

3.5.4. BACKUP & RESTORATION

Data critical to our operations shall be backed up according to our Backup and Restoration Standard. Specifics regarding Backup and Restoration requirements for registry systems are included in questions 37 & 38.

3.6. NETWORK CONTROLS

- Appropriate controls must be established for ensuring the network is operated consistently and as planned over its entire lifecycle.
- Network systems must be synchronized with an agreed upon time source to ensure that all logs correctly reflect the same accurate time.
- Networked services will be managed in a manner that ensures connected users or services do not compromise the security of the other applications or services as required in the HBI Network Configuration Standard. Additional details are included in Question 32: Architecture response.

3.7. DISASTER RECOVERY & BUSINESS CONTINUITY

The SVP of IT has responsibility for the management of disaster recovery and business continuity. Redundancy and fault-tolerance shall be built into systems whenever possible to minimize outages caused by hardware failures. Risk assessments shall be completed to identify events that may cause an interruption and the probability that an event may occur. Details regarding our registry continuity plan are included in our Question 39 response.

3.8 SOFTWARE DEVELOPMENT LIFECYCLE

Advance planning and preparation is required to ensure new or modified systems have adequate security, capacity and resources to meet present and future requirements. Criteria for new information systems or upgrades must be established and acceptance testing carried out to ensure that the system performs as expected. Registry systems must follow the HBI Software Development Lifecycle (SDLC) Standard.

3.9. SECURITY MONITORING

Audit logs that record user activities, system errors or faults, exceptions and security events shall be produced and retained according to legal, regulatory, and compliance requirements. Log files must be protected from unauthorized access or manipulation. IS is responsible for monitoring activity and access to HBI systems through regular log reviews.

3.10. INVESTIGATION & INCIDENT MANAGEMENT RESPONSE

Potential security incidents must be immediately reported to the IS Team, EVP of IT, the Legal Department and⁄or the Incident Response. The Incident Response Team (IRT) is required to investigate: any real or suspected event that could impact the security of our network or computer systems; impose significant legal liabilities or financial loss, loss of proprietary data⁄trade secret, and⁄or harm to our goodwill. The Director of IS is responsible for the organization and maintenance of the IRT that provides accelerated problem notification, damage control, investigation and incident response services in the event of security incidents. Investigation and response processes follow the requirements of the Investigation and Incident Management Standard and supporting Incident Response Procedure (see Question 30b for details).

3.11. LEGAL & REGULATORY COMPLIANCE

All relevant legal, regulatory and contractual requirements are defined, documented and maintained within the IS Policy. Critical records are protected from loss, destruction and falsification, in accordance with legal, contractual and business requirements as described in our Document Retention Policy. Compliance programs implemented that are applicable to Registry Services include:

- Sarbanes Oxley (SOX): All employees managing and accessing SOX systems and/or data are required to follow SOX compliance controls.
- Data Privacy and Disclosure of Personally Identifiable Information (PII): data protection and privacy shall be ensured as required by legal and regulatory requirements, which may include state breach and disclosure laws, US and EU Safe Harbor compliance directives.

Other compliance programs implemented but not applicable to Registry systems include the Payment Card Industry (PCI) Data Security Standard (DSS), Office of Foreign Assets Control (OFAC) requirements, Copyright Infringement & DMCA.

4.0. SECURITY ASSESSMENTS

Our IS team conducts frequent security assessments to analyze threats, vulnerabilities and risks associated with our systems and data. Additionally, we contract with several third parties to conduct independent security posture assessments as described below. Details of these assessments are provided in our Security Policy B response.

4.1. THIRD PARTY SECURITY ASSESSMENTS

We outsource the following third party security assessments (scope, vendor, frequency and remediation requirements of any issues found are detailed in our Security Policy B response); Web Application Security Vulnerability testing, quarterly PCI ASV scans, Sarbanes-Oxley (SOX) control design and operating effectiveness testing and Network and System Security Analysis.

4.2. INTERNAL SECURITY ASSESSMENTS

The IS team conducts routine and continual internal testing (scope, frequency, and remediation requirements of any issues found are detailed in our Security Policy B response) including; web application security vulnerability testing, external and internal vulnerability scanning, system and network infrastructure penetration testing, access control appropriateness reviews, wireless access point discovery, network security device configuration analysis and an annual comprehensive enterprise risk analysis.

5.0. EXECUTIVE OVERSIGHT & CONTINUOUS IMPROVEMENT

In addition to the responsibility for Information Security residing within the IS team and SVP of IT, risk treatment decisions are also the responsibility of the executive of the business unit responsible for the risk. Any risk with potential to impact the business financially or legally in a material way is overseen by the Incident Response Management team and/or the Audit Committee. See Figure 2 in Attachment A. The Incident Response Management Team or Audit Committee will provide assistance with management action plans and remediation.

5.1. GOVERNANCE RISK & COMPLIANCE

We have deployed RSA's Archer Enterprise Governance Risk and Compliance (eGRC) Tool to provide an independent benchmarking of risk, compliance and security metrics, assist with executive risk reporting and reduce risk treatment decision making time, enforcing continuous improvement. The eGRC provides automated reporting of registry systems compliance with the security program as a whole, SOX Compliance, and our Vulnerability Management Standard. The eGRC dashboard continuously monitors risks and threats (through automated feeds from our vulnerability testing tools and third party data feeds such as Microsoft, CERT, WhiteHat, etc.) that are actionable. See Attachment A for more details on the GRC solutions deployed.

6.0. SECURITY COMMITMENTS TO REGISTRANTS

We operate all registry systems in a highly secured environment with appropriate controls for protecting HBI data and ensuring all systems remain confidential, have integrity, and are highly available. Registrants can assume that:

1. We safeguard the confidentiality, integrity and availability of registrant data through access control and change management:
 - Access to data is restricted to personnel based on job role and requires 2 factors of authentication.
 - All system changes follow SOX-compliant controls and adequate testing is performed to ensure production pushes are stable and secure.
2. The network and systems are deployed in high availability with a redundant hot datacenter to ensure maximum availability.
3. Systems are continually assessed for threats and vulnerabilities and remediated as required by the Vulnerability Management Standard to ensure protection from external malicious acts.
 - We conduct continual testing for web code security vulnerabilities (cross-site scripting, SQL Injection, etc.) during the development cycle and in production.
4. All potential security incidents are investigated and remediated as required by our Incident Investigation & Response Standard, any resulting problems are managed to prevent any recurrence throughout the registry.

We believe the security measures detailed in this application are commensurate with the nature of the TLD string being applied for. In addition to the system/infrastructure security policies and measures described in our response to this Q30, we also provide additional safety and security measures for this string.

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

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

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

Annex 3.

New gTLD Application Submitted to ICANN by: Top Level Domain Holdings Limited

String: eco

Originally Posted: 13 June 2012

Application ID: 1-1039-91823

Applicant Information

1. Full legal name

Top Level Domain Holdings Limited

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact Information Redacted

4. Fax number

5. If applicable, website or URL

http://www.tldh.org

Primary Contact

6(a). Name

Mr. Antony Van Couvering

6(b). Title

Chief Executive Officer

6(c). Address

6(d). Phone Number

Contact Information Redacted

6(e). Fax Number

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Michael Salazar

7(b). Title

CFO

7(c). Address

7(d). Phone Number

Contact Information Redacted

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Corporation

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

British Virgin Islands

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.

London_Stock_Exchange;TLDH.LN

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

Antony Van Couvering	Chief Executive Officer
Caspar von Veltheim	Executive Director
Fred Krueger	Executive Chairman
Guy Elliott	Non Executive Director
Keith Teare	Non Executive Director
Michael Salazar	Chief Financial Officer

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

Frederick Krueger	Chief Strategy Officer

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.

eco

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

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

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

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

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

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

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

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

Attachments are not displayed on this form.

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

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

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

We ensured that there are no known operational or rendering problems concerning the applied-for gTLD string in two ways:

First, we researched whether any top-level string composed of the letters of the Latin alphabet has ever had any operational or rendering problems. We concluded from that research that there is no third-party experience or knowledge that would lead us to believe that there is any operational or rendering problems with the applied-for gTLD string.

Second, using Minds + Machines' Espresso system, we created a test-bed version of the applied-for gTLD string as a top-level domain. We then conducted a series of tests, including simulations of many of the day-to-day registry functions, and found no operational or rendering problems.

We concluded that there are no known operational or rendering problems with the applied-for gTLD string.

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.

Over the last twenty years it has become increasingly clear that unchecked population and industrial growth may have catastrophic--and possibly irreversible--near term consequences on Planet Earth. Global warming, in particular, is now established as a fact, not a theory, and with greater than 90% probability, it “very likely” to be a man-made phenomenon (source: Intergovernmental Panel On Climate Change).

Faced with this mounting evidence that we need to take action to control carbon dioxide emissions and pay much more attention to the environment we live in, a large number of independent groups have emerged in recent years in different parts of the globe to advocate “green” causes. No one group can claim “authority” to act as a representative of all things ecological; and in fact several groups diverge significantly on their strategies for dealing with this extremely difficult, and possibly unsolvable problem.

It is our goal that a significant percentage of revenues from sales of .ECO domains should benefit environmental leaders and causes.

The .ECO top-level domain will benefit concerned companies and individuals who wish to either rebrand under .ECO, or use the suffix to showcase what they are doing for the environment. As with .ORG, we feel that .ECO should not be run with an authoritative view on who is “eco” and who is not, but rather as a self-selecting badge for companies and customers who genuinely care about the environment.

It is our belief that .ECO can be run as a sustainable, profitable enterprise while serving the general needs of the various interests in the overall environmental world.

The market for green products and services has been steadily increasing over the past few decades. As defined by the EPA, products that are “environmentally preferable”, “have a lesser or reduced effect on human health and the environment when compared with competing products or services that serve the same purpose. The product or service comparison may consider raw materials acquisition, production, manufacturing, packaging, distribution, reuse, operation, maintenance, or disposal.” (Source: http:⁄⁄www.epa.gov⁄epp⁄pubs⁄guidance⁄finalguidanceappx.htm#AppendixA)

Eco-friendly products, services, and materials have entered the mainstream. As more and more green products are produced and their prices become comparable to conventional products, consumers will find it easier to use their wallets in service of their beliefs. This trend, as shown by the development and demand for hybrid cars, environmentally friendly cleaners and cosmetics, and even the partnerships behind the 2012 movie “The Lorax”, which touts an environmentally friendly message and has over 70 product partnerships. (Source: http:⁄⁄www.reuters.com⁄article⁄2012⁄02⁄08⁄idUS201171+08-Feb-2012+PRN20120208)

The .ECO top-level domain will offer businesses and people the opportunity to advertise their association with environmentally-friendly products, services, and materials through the purchase and use of a .ECO top-level domain. The .ECO domain is dedicated to accurate information about green, sustainable, and eco-friendly products, allowing customers to make informed decisions about the items they use, and helping to drive the positive image of green products and their benefits to the environment.

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

The .ECO domain will allow companies to attract like-minded customers to their green and eco-friendly offerings, as well as expand and diversify the current market, helping increase brand trust and product innovation. The .ECO domain will help create an even larger force for change in the race for sustainability.

PUBLIC BENEFIT
The .ECO gTLD will provide all those interested, world-wide, in disseminating or seeking information--whether non-commercial or commercial--issues, news, culture, lifestyle, entertainment, sports or any other topic with a convenient and recognizable domain name that associates them and⁄or their information with eco-consciousness.

We believe that the Internet-using world will benefit from the existence of a .ECO gTLD by:

- making domain names ending in .ECO available to all those who may want to use such .ECO domain names for their own business, personal, political or other legal purposes in the United States and world-wide.

- the promotion of eco-consciousness by having information of any and all types and for any and all legal purposes available and disseminated from websites and email addresses ending in .ECO for the registrants’ and users’ own purposes world-wide.

- the promotion of eco-consciousness by allowing businesses, not-for-profits and individuals to associate their products, services, information and selves with eco -consciousness for their own purposes.

- allowing people and organizations to promote their association with eco-consciousness on the Internet.

- providing an identifiable means for people, organizations and businesses to communicate with those who associate with or provide eco-friendly products.

EXPANDING THE TLD NAMESPACE
Over the past decade, the market for domain name registrations has grown at a tremendous pace. From 2000 to 2010 domain name registrations increased from 40 million to 200 million domain names registered globally. 2011 experienced a growth of approximately 9%, which was significantly higher than the previous year’s 6% growth, ending third quarter 2011 with approximately 220 million domain names registered globally. Approximately 60% of these are gTLDs, while the remaining 40% are comprised of ccTLDs. More specifically, gTLD growth was approximately 8% in 2011, while ccTLD growth exceeded 11%.

Existing TLDs, such as .COM and .NET, do not provide adequate solutions for many registrants. Domain names that relate to the registrants’ business, interests, or associations are often already registered, priced exorbitantly high, or available options are unsuitable. Additionally, other options, such as ccTLDs, do not provide adequate alternatives as a registrant may not have any geographic relation or meet the criteria associated with other gTLDs such as .MUSEUM or .AERO. Therefore, the only available opportunity to pursue a relevant and useful domain name registration may be through a brand new registration of a gTLD.

Taking into account the new opportunities available with new gTLDs, growth is expected to continue in all sections of the domain name industry. It will benefit registrants and users by allowing registrants to reach more targeted audiences and increase their web presence. Additionally, it will allow registrants to more closely identify with a particular market segment.

At present, there is no specific .ECO domain name, or useful top-level alternative domain name, that exists for the people, organizations or businesses that associate themselves with eco-consciousness or people, organizations or businesses that want to communicate with them. Those desirous of a domain name that indicates some level of association with eco-consciousness could seek a second level domain name such as “ECO.COM,” “ECO.US” or “ECO.NET,” but such domains (or similar names) are not readily available under the limited number of existing gTLDs, and--more importantly--only provide a secondary (at best) or weak (at worst) relationship between the domain name and eco-consciousness, which we believe is the primary goal of the registrant of such names.

From a competitive perspective, registrants that want a domain name that effectively and efficiently shows an association with eco-consciousness or registrants that want a domain name that allows them to identifiably communicate with people who associate or identify with it face a domain name marketplace that provides them with few, if any, options for their purposes. The .ECO top-level domain will resolve this problem by providing registrants with an efficient, effective, prominent, instantly understood way of showing their association with eco-consciousness, and provide those registrants who desire it a domain that that can effectively communicate information to such Internet users in an identifiable way. At the same time, .ECO provides competition with the existing TLDs and new gTLDs that will be approved by ICANN, benefiting the Internet community at large by increasing consumer choice.

We believe that the .ECO top-level domain will add significantly to competition and differentiation in the top-level domain space, both for registrants and Internet consumers. With respect to competition, registrants are presently extremely limited in their choice of domain names that allow them to efficiently and effectively associate themselves with eco-consciousness. The availability of useful, effective, straight-forward domain names on existing top-level domains, such as .COM, .NET and .ORG, are few and far between, or may be for sale at prices that are out of reach for most. .ECO will allow registrants to obtain useful, effective, straight-forward domain names rather than be forced to purchase, for example, their fifth, sixth or even later choice .COM or .NET name--which may well barely relate to the registrant’s purpose--or use of a domain name that may be confusingly similar with numerous other .COM or .NET domain names. In addition, some existing generic top-level domain names, though newer, such as .XXX, may be inappropriate for most registrants for content associational reasons, while country-code top-level domains, though numerous, are not useful or appropriate for many registrants for geographical associational reasons. Thus, .ECO will increase competition for registrants who want a domain name that clearly, effectively and efficiently associates them with eco-consciousness for their domain name purposes as well as for those registrants who want to reach Internet users who identify with it.

.ECO will also increase pricing competition in the top-level domain name space by assuring that .ECO domain names are priced at levels that are appropriate to the vast majority of potential registrants to whom .ECO is targeted.

Internet consumers benefit from this increase in competition, as less confusing and clearly associated .ECO domain names will make it easier for them to know that the owner of the second-level domain name is a member of or seeks to associate with eco-consciousness.

Likewise, .ECO will help significantly increase differentiation in the top-level domain space. Existing leading generic top-level domain names, such as .COM, .NET and .ORG no longer require and no longer represent any real differentiation in association, purpose or content. Newer top-level domains, such as .XXX, .AERO and .MUSEUM, do represent differentiation, but are either inappropriate or unavailable to most prospective registrants at whom .ECO is targeted. .ECO will further increase differentiation by allowing registrants to be associated, and consumers to know that the registrant seeks to associate with eco-consciousness.

In terms of user experience, .ECO will provide users with a top-level domain name that allows them to easily recognize that the registrant seeks to have its second-level domain name and content associated with eco-consciousness. We believe this will be of substantial benefit to the Internet user community in generally--and the eco-friendly market specifically--as it will allow them to more easily and more readily understand the purpose or motives of the registrant’s website or email, allowing for better, more efficient and more effective use of their time online.

On balance, and for the reasons set forth above, a .ECO domain will be in the public’s interest; it will serve as a catalyst to promoting eco-consciousness use; and it will benefit the “green” products market.

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

This applicant, like most organizations, takes its good reputation seriously. We are fully cognizant, for example, that artistic, political, economic and social issues, all of which can be associated with eco-consciousness, often provoke heated debate and are at times controversial. However, we recognize and support the free speech rights of both registrants and Internet users as fundamental rights and believe that such free speech rights are important to the success of the .ECO business plan. We believe that any plan to stifle free speech would be more harmful to .ECO’s reputation and business success than any attempt by us to govern speech. That being said, to protect .ECO’s reputation and the associational benefits it offers registrants and Internet consumers, we will actively promote and enforce our Acceptable Use and Abuse Prevention policies and procedures, which we believe will effectively combat improper or unlawful unprotected speech and online conduct. We believe that these mechanisms will be effective in assuring the reputation of the .ECO top-level domain, its registrants, Internet Users, as well as the public.

The .ECO top-level domain will be marketed to registrants who want to associate themselves, their products, services, thoughts, ideas or anything else in a positive way with eco-consciousness, as well as to those who want to communicate with them in an easily identifiable way. Therefore we believe that the great majority of registrants who apply for a .ECO domain name will do so because of its association with or because they want to reach those who do, and not for other reasons. In these ways, the .ECO top-level domain will bring a special association with eco-consciousness to the top-level domain name space.

We are dedicated to protection of third-party rights and prevention of abusive uses of the .ECO domain name. We intend to achieve this goal by crafting our Naming Policy, Acceptable Use Policy, and other policies to be readily understandable and easily accessible, and by making sure that our mechanisms for enforcing rights and preventing abuse (such as our Complaint Resolution Service) operate effectively, efficiently, and fairly. In addition, we will ensure that they work symbiotically with other ICANN-mandated rights protection mechanisms such as the UDRP.

We have crafted a draft framework for registration of .ECO domains that fully supports the goals and benefits set forth above. Our draft registration framework is based on advice from ICANN, WIPO, applicable laws, and a variety of other expert sources. Specifically, the .ECO draft framework includes these interrelated sets of agreements setting forth our policies and regulations, all of which registrants must agree to be bound by:

- The Registrant Agreement, which registrars contracted with .ECO must present to registrants. This is a collateral agreement to the Registrar Registry Agreement (detailed below), and will bind registrants to .ECO's Acceptable Use Policy (as detailed below), .ECO's Privacy & Whois Policy (detailed below), ICANN-mandated rights protection mechanisms (including the Universal Dispute Resolution Policy ("UDRP"), and the Complaint Resolution Service;

- The Acceptable Use Policy ("AUP"), which details the proper use of domain names that end in .ECO, which is incorporated by reference in the Registrant Agreement that registrants must agree to;

- The Privacy and Whois Policy, which describes how a registrant's personal data is to be used, which is also incorporated by reference in the Registrant Agreement;

- The Registrar-Registry Agreement, which is the contract between .ECO and its ICANN-accredited registrars, which sets forth, inter alia, the duties and obligations of the registrar with respect to .ECO registrants and the .ECO registry; and

- The Naming Policy, which sets out .ECO's policies governing prohibited, blocked or reserved domain names.

These agreements and policies are designed to ensure transparent and non-discriminatory policies for the registration of .ECO names; fair and competitive pricing; protection of personal data and privacy; adherence by registrars and registrants to the AUP; protection of trademarks, the names of natural and legal persons and other property rights; prevention of the registration of illegal terms; and the prevention violations of the law. Moreover, our policies promote competition among registrars, combat abuse of the DNS, address cybercrime, protect intellectual property rights, and align the .ECO top-level domain with applicable regulatory and legislative environments and Internet registry best practices.

These policies will effectively support the key mission, purposes and goals of the .ECO top-level domain, which is to allow registrants who want to associate themselves with, while at the same time protecting third-party rights and preventing abuse.

We specifically examined more restrictive registration policies, such as limiting registration to members of organizations with a specific tie to eco-consciousness. We rejected such limitations because they would interfere with .ECO's primary mission, purpose and goals--which is to encourage as many registrants as possible to associate themselves with the eco-consciousness for any legal purpose. Factors that we took into account when considering a more restrictive registration policy included:

- Our recognition that registrants of a .ECO domain name will self-select because they have an interest in eco-consciousness, naturally reducing the number of potential registrants; and, because restrictive policies such as, for example, requiring membership in a specific organization or organizations, would exclude many legitimate registrants from obtaining a .ECO domain name. For example, and by way of illustration, if membership an organization were required for registration, businesses and charitable organizations that would find a .ECO top-level domain name an effective marketing tool would be excluded from registering a .ECO domain name as they might not be eligible to be members in an organization that accepted only natural persons for membership.

With respect to protecting registrant privacy and confidential information, we will comply with all applicable ICANN rules, including Whois policies, and all applicable laws, rules and regulations of appropriate jurisdictions. Registrant privacy and use of confidential information are set forth in our Privacy & Whois

Policy. Information concerning updates and changes to the Privacy & Whois Policy will be promptly and prominently displayed on the .ECO web site.

.ECO’s back-end registry services provider will also be required to employ industry-standard procedures to prevent the unauthorized or illegal access of registrant privacy or confidential information.

With respect to users, .ECO’s Registration Agreement will require that all registrants comply with any and all applicable laws, rules or regulations concerning user privacy and confidential information for applicable jurisdictions; failure to do so may result in suspension or loss of their .ECO name and may, in addition, result in legal actions by appropriate authorities.

We plan to minimize social costs primarily through clearly written, widely disseminated, and easy-to-understand policies. Our Acceptable Use Policy clearly delineates unacceptable behavior and prohibited content by registrants using domain names in the .ECO zone.

Our rules concerning applications for the same domain name establish clearly delineated rules, and will be published well in advance. They provide adequate safeguards for the rights of all participants as well as expeditious and cost-effective challenge procedures in the event of disputes.

During the Sunrise period and Landrush periods, multiple applications for the same name will be resolved by auction. UDRP or URS will be used if there are disputes as to rights to a name.

After Sunrise and Landrush, domain names will be allotted on a first-come, first-serve basis. All domains are subject to UDRP and URS challenges.

At all times, .ECO’s Complaint Resolution Service will be available to registrants and the public in the case of alleged prohibited use or content.

.ECO does not envision special discounts for different classes of registrants, but may consider such offers in the future. We may offer introductory discounts for first-time registrants in .ECO. Bulk registration discounts are not being considered at this time.

.ECO plans to make contractual commitments to registrants regarding the magnitude of price increases. .ECO will contract with its registrars that any percentage increase in renewal and first registration fees will be applied uniformly across all registrations, and that notice of any price increases will be provided on the registrar’s website and by the registrar to registrants via email six months or more in advance.

Community-based Designation

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

No

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

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

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

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

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

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

Attachments are not displayed on this form.

Geographic Names

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

No

Protection of Geographic Names

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

We have accepted the advice of the Governmental Advisory Committee (GAC) that we should adopt appropriate procedures to block names with national or geographic significance at the second and other levels, and will do so in the manner described below:

The country and territory names contained in the following internationally recognized lists will be initially reserved at the second level, as follows:

The short form (in English) of all country and territory names contained on the ISO 3166-1 list, as updated from time to time, including the European Union; on the United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World; and on the list of United Nations member states in the six official United Nations languages prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names.

Procedurally, the geographical names contained in these lists, as described in Specification 5 of the New gTLD Agreement, will be added to the registry software system “prohibited word” function. This function, part of Espresso, our registry platform, allows strings to be blocked from registration. Upon an attempt via the EPP or web interface, the registration will not be allowed. Any attempt to register a domain containing those geographical names will be automatically denied, as they were similarly blocked in the .INFO TLD. If a Government or public authority decides to register a geographic name which has been blocked by the process describe above, the .INFO procedure for notice, authentication, and registration will be substantially adhered to, as follows:

1. The Government or public authority concerned informs the GAC Secretariat of their request to register the name, and the designated beneficiary.
2. The GAC Secretariat authenticates the request and transfers it to the ICANN staff and to the registry operator.
3. The registry operator verifies the availability of the name and issues an authorization number that is transmitted directly to the designated beneficiary in the country concerned.
4. The designated beneficiary (the Registrant) registers the name, paying the normal fee, with an ICANN-accredited registrar contracted with the registry operator using the authorization number as their authority.

The registry operator may at some point seek agreement with the applicable governments to release these reservations, subject to review by ICANN’s Governmental Advisory Committee and approval by ICANN.

For protection of geographic names at other levels, we have a complaint mechanism in place and any geographic entity may register a complaint if they feel their national rights have been violated.

We believe that the measures outlined above incorporate GAC’s advice and serve as a pledge to block, at no cost to governments, geographically significant names and allow a means of challenging any abuse of the use of a geographically significant name.

Registry Services

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

We have selected Minds + Machines as our backend registry provider. Minds + Machines currently operates the .FM TLD and has a proven registry system. The names and full descriptions of the registry services Minds + Machines will provide are summarized in this section.

Minds + Machines will provide the critical registry functions as well as the usual and customary functions provided by a backend registry operator:

1. The receipt of data from registrars concerning registrations of domain names and name servers (SRS) via EPP,
2. Dissemination of top-level domain (TLD) zone files (DNS);
3. Dissemination of contact or other information concerning domain name registrations (Whois service);
4. Domain Name Services Security Extensions (DNSSEC); and
5. Rights Protection Mechanisms and Abuse Prevention & Mitigation.
6. Data Escrow
7. Monthly reports to ICANN
8. Access to bulk zone files
9. IPv6 Support
10. Internationalized Domain Names

The registry will use the Espresso registry service platform ("Espresso") from Minds + Machines, an extensible provisioning protocol ("EPP") registry service already in use by the .FM ccTLD that meets the Internet Corporation for Assigned Names and Numbers (ICANN)'s new generic top-level domain (gTLD) compliance standards. Espresso receives data from registrars, writes the data to the registry database, and disseminates TLD zone files to DNS services.

The registry has a Whois function so that contact and domain registration information may be retrieved. Whois services will be rendered by a Port 43 Whois and via a web-based Whois at http:⁄⁄whois.nic.eco. Our current Whois provisioning provides for the same level of access and usability that a restful Whois implementation might and so we have no plans to implement a restful Whois in addition to our Port 43 Whois. The registry zone servers will hold the master zone files, and will be verifiable with DNSSEC. The registry system also automates required monthly reports to ICANN, and builds escrow data files according to ICANN requirements.

The registry services to be provided are customary services as listed at http:⁄⁄www.icann.org⁄en⁄registries⁄rsep⁄rsep.html.

Registry services are managed via an Extensible Provisioning Protocol (EPP) Application Programming Interface (API). The domain registrant submits an order for a domain to the registrar. The registrar then uses EPP to check the registry database to see if the domain is available. If the domain is available, the registry sends an EPP confirmation to the registrar, confirming availability. The registrar then displays the availability of the domain name to the customer. The registrant submits contact information and domain registration details such as nameservers, length of registration, and payment. The registrar then sends this information to the registry via EPP. The domain order is accepted and written to the registry database. A confirmation is sent to the registrar. Each transaction is recorded for accounting and billing purposes.

In addition, there is a web-interface API with varying levels of access privileges made available to customer service, database administrators, and Registrars.

The TLD zone files are updated regularly. The master servers pull the new zone files using Berkeley Internet Name Domain (BIND) and distribute the new domain information to querying secondary servers.

The registry will maintain a searchable Whois lookup service that meets the requirements in Specification 4, Registration Data Publication Services.

The registry system supports IDN domain names. IDN Language tables as posted at the IANA website can easily be added to the registry platform, thereby making those scripts available at the second level for domain registrations.

The DNSSEC function is RFC compliant. Registrars are provided with the ability to submit and manage DS records using EPP, or through the web interface.

The registry system has billing and reporting components. Database transactions such as read, write and deletes are logged and made available for reporting. These reports are used by the operator to monitor the health of the technical service, thereby informing business decisions, and for accounting and reporting to ICANN.

Data will be escrowed in compliance with Specification 2 of the New gTLD Registry Agreement through our contracted third party escrow provider, NCC Group.

Rights protection mechanisms and abuse prevention and mitigation will be implemented at the registry to protect intellectual property owners and the general public from abusive or illegal practices.

Each of these registry services are non-unique to .ECO. The registry services are standard and no new services are proposed for .ECO. The proposed registry service will not have an effect on security of the DNS. No unauthorized access to or disclosure of information or resources on the Internet will occur as a result of the implementation of the registry system. No unauthorized disclosure, alteration, insertion or destruction of the registry data will result from the implementation of the registry. The registry will have no negative effect on the stability of the Internet. All registry services are compliant with applicable relevant standards that are authoritative and published by the Internet Engineering Task Force (IETF).

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

.ECO will operate on Minds + Machines' Espresso registry platform. Espresso's design is proven to be secure, reliable and robust. The registry infrastructure is specifically configured to handle the high transaction volumes found in the TLD registry business. Espresso's Shared Registry System (SRS) is an automated production environment dedicated to managing transactions to the registry database from multiple registrars.

The SRS system fully complies with Specification 10 of the registry agreement, including all Service Level Agreements (SLAs).

The EPP interface, Whois service and DNS service are all fully RFC compliant including all RFCs listed in Specification 6 and 10: DNS RFCs 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 4343 and 5966; EPP RFCs 5910, 5730, 5731, 5732, 5733, 5734, 3915 and 3735; DNSSEC RFCs 4033, 4034, 4035, 4509, 4641 and 5155; IDN RFCs 5890, 5891, 5892, 5893; IPv6: RFCs 4472 and 3912. The registry will use anycast DNS networks. Whois and DNS servers are continually updated. Past performance and reliability records, based on service to the .FM domain registry, of the registry’s technical functions enable us to confidently commit to ICANN’s SLAs.

In addition to the core registry services described in Question 23, the registry system provides a comprehensive billing and reporting solution, data escrow services and full Internationalized Domain Name (IDN) support for .ECO. Services will be backed by a 24⁄7 help desk and network operations center provided by Minds + Machines.

The registry system uses a distributed architecture (as described in Question 32) that achieves the goals of scalability, reliability and extensibility. The registry system offers redundancy to function even if an entire server were to suffer catastrophic failure (see Question 39). The registry uses load balancers to mitigate hardware failure and assist in scalability. The registry's load balancing design allows hardware upgrades without customer impact.

Registry facilities and services will be operated in a minimum of two widely separated geographic locations, providing redundancy and fault tolerance. The primary registry facility is a live facility, meaning that it will be the normal full-time registry. The secondary registry facility is both a functional and standby facility, meaning that it will be activated for primary registry services if operational problems ever arise at the primary facility. The secondary facility is continuously synchronized with the primary. In case of a failover, the secondary site will be enabled to provide registry services such as reporting, daily zone file distribution and operational testing environment (OTE). A third site is used for database backup.

More information about facilities can be found in the answer to Question 34.

The registry system includes firewalls, routers, switches and virtual private network configurations. These are further detailed in the Security section of the application (Questions 30 and 31).

The registry operates multiple database servers to provide redundancy. The primary registry facility houses two database servers: one the main database and the other the secondary. The standby registry facility will house one database server which will be constantly synchronized with the primary registry. The database servers will be replicated but are not load balanced to ensure that there is one authoritative master database.

The SRS configuration and server allocation does not reflect the excessive multitude of servers presented by legacy registries in previous TLD application rounds. Hardware, software, database platforms and architecting have evolved significantly; it is no longer necessary to use dozens of servers to perform one registry function. Because we have access to state of the art systems, we have been able to architect the SRS so that our EPP servers are both business rule engines and protocol servers--less prone to errors and offering more efficient administration.

The Espresso platform is architected for ease of administration, which entails applications other than the registry transaction functions running on the same physical hardware. Currently, registering, updating, and deleting; any and all functions occur through the extensible provisioning protocol (EPP) servers. The software application contains all logic (business and policy) and applies them accordingly. Registrations, management of domains and management of accounts all occur through one application. Administrative changes and updating of business and policy rules are all EPP requests managed through the EPP servers. The registry configuration presented for .ECO is greatly over-provisioned for the best-case projected number of registrations. Combined, the Espresso platform is comprises conceptually different pieces: the individual functions will be split into separate servers if the registry reaches a threshold of 25% capacity.

-REPRESENTATIVE NETWORK DIAGRAM-
Please see the attached “Q 24 SRS Overview” for a graphical representation of the SRS.

-NUMBER OF SERVERS-
The number of physical or virtual servers planned for the .ECO registry SRS function (not including the DNS function, as fully detailed in the response to Question 35) are as follows:

At the primary location:
-2 Load balancers to listen and direct traffic to EPP servers: one primary, one standby;
-2 Database servers: one primary, one standby;
-2 Application servers to listen for EPP commands from registrars, query the database, and write to the database: one primary, one high availability spare;
-2 Hidden Master server instances for disseminating zone file information: one primary, one standby;
-1 System monitoring server for monitoring the health of servers, performing deep inspection and warning of denial of service and other malicious activities, plus external third party monitoring services;
-2 Whois Server instances to answer on Port 43 for RDDS queries: one primary, one standby
-2 Firewalls: one primary, one high availability spare;
-2 Routers/Switches: one primary, one high availability spare;
-2 VPN instances: one primary, one high availability spare;

In addition, a server is made available as an Operational and Testing Environment (OTE).

Technical resources required to run the SRS are adequate, on hand, committed and/or readily available.

-DESCRIPTION OF INTERCONNECTIVITY BETWEEN SERVERS-
Each registry instance is configured on a local area network. Servers are connected via redundant multi-homed 1 Gbps Ethernet. Connectivity between the primary and secondary registry facility (for replication) is over an encrypted VPN tunnel.

-FREQUENCY OF SYNCHRONIZATION BETWEEN SERVERS-
Local servers are synchronized constantly using encrypted asynchronous replication to update the database at the secondary facility.

-SYNCHRONIZATION SCHEME (E.G., HOT STANDBY, COLD STANDBY)-
The synchronization scheme is hot standby. The backup server is kept on and ready to failover should the primary database server fail. The secondary facility is also in hot standby. It runs idle, ready to failover should the primary facility be completely disabled. The monitoring system checks the health of the primary

facility: if emergency thresholds are met, the system fails-over to the secondary facility.

-SYSTEM ENVIRONMENTS AVAILABLE-
Registrars are provided with an OTE to test connectivity and EPP schema, an automated production environment (both via EPP and web-based graphical user interface (GUI)) and a demonstration system for training.

-DOMAIN NAME PROVISIONING SERVICE TYPE-
The registry system is EPP with software code development specifically targeted to meet ICANN’s new gTLD requirements. A GUI for administrative use and for registrars that have yet to integrate via EPP is available and provides all functions available via the EPP interface.

-REGISTRAR TOOLKITS AVAILABLE-
Registrar tool kits (EPP schema made available to Registrars to shorten development time and ensure accurate communications) will be made available for download from the Registry Administration site, as is standard across most TLDs. Special EPP extensions are also made available for registrar implementation.

-WHOIS SERVICE-
The Whois service is RFC 3912 compliant. The registry administrator may determine what information is displayed through the Whois server depending on additional policies established for the TLD.

-WHOIS CHECK SERVICE-
The Whois check service is RFC 3912 compliant. It accepts and returns ASCII queries. In anticipation of rapid adoption of IDNs, we also have a unicode-enabled Whois service allowing for querying and display of non-Roman characters. The Whois service also meets ICANN’s new gTLD “thick registry” requirements (where the registry collects registrant data and must provide Whois, rather than only the registrar providing Whois) and IP ranges can be black- or white-listed for specified lookup limits.

-REGISTRY PORTAL WEB APPLICATION-
The web portal is intuitive, easy to use and every registry function is accessible. For example, the Whois service is easily configured via the GUI.

-REGISTRY DATABASE-
The Registry database is fully scalable and over-provisioned to meet the requirements of our highest projected registration volumes. The registry database has 60 times the transactional capability required by registries of 1.25 million domains. When greater transaction capabilities are required, the system will be reconfigured to split out separate functions onto multiple protocol servers.

-DNS SERVICE-
We have contracted with Packet Clearing House (PCH) for DNS services. PCH complies with the RFCs as listed in Specification 6 and 10. The DNS uses BIND and is configured to respond to queries over TCP, UDP and all IANA-recognized DNS resource record types. Access to DNS servers over IPv6 is possible through enabled dual-stack IPv4⁄IPv6 connectivity. PCH utilizes anycast technology, which enables zero downtime as traffic can be redirected to alternate locations if local servers are overloaded or unavailable. PCH has provided Minds + Machines, our outsourced Registry Service Provider, with SLAs guaranteeing 100% uptime, with a twenty-year history proving 100% reliability.

-REGISTRY SUPPORT-
Critical support is available 24⁄7 with on-call technicians responding immediately upon notification. Support staff may be reached via telephone, email, or SMS.

-DISASTER RECOVERY SERVICES (BUSINESS CONTINUITY)-
Registry continuity in compliance with Specification 6 is assured through high availability and highly redundant network operations and is detailed in Question 39. In case of a physical disaster, anycast DNS and hot swapping to off-site registry mirror ensures no interruption to services. Regular off-site backups and escrow deposits ensure integrity of data. Our registry continuity plan follows ICANN's specifications and is tested regularly (as described in the answer to Question 39). In case of business failure, we also have in place mutual registry transition agreements with an alternate registry operator to ensure an uninterrupted, smooth transition of registry operations (as described in the answer to Question 40).

-SERVICE LEVEL AGREEMENT-
We will meet or exceed the SLAs required by ICANN and outlined in Specification 10 (Registry Performance Specifications) as evidenced by our current operational record of the .FM registry. Anycast DNS, high availability, redundancy and an off-site mirror ensure that SLAs will be met.

-WILDCARD PROHIBITION-
The registry will return a "Name Error" response for any domain names which are either not registered, do not have valid NS records or the status does not allow them to be published in the DNS, as prescribed in RFCs 1034 and 4592. Wildcarding will not be implemented in the registry.

-ICANN REPORTING-
The registry system outputs and submits all required reports to ICANN, including monthly the Per-Registrar Transaction Report and Registry Functions Activity Report as defined in Specification 3.

-IDNA2008 COMPLIANT-
The registry software is IDNA2008 compliant. It accepts xn--registrations into the database. The registry allows input of non-ASCII characters into "local language" registrant fields.

-IPV6 ENABLED-
The registry supports and resolves IPv6 records in the host fields.

-DNSSEC-
DNSSEC will be implemented and TLD zones will be signed in compliance with RFCs 4033, 4034, 4035, 4509 and 5155 and their successors. Key signature storage and processing methodologies have been developed and implemented at registry level.

-SETUP OF ESCROW SERVICES-
The registry operator will provide compressed, encrypted and signed secure data file transfers (SFTP) to the outsourced escrow agent on a daily and weekly basis and will validate every file within 24 hours. All requirements detailed in Specification 2 will be met.

-SETUP OF MANAGED DNS SERVICES-
Zone files will be disseminated through DNS via BIND. DNS system performance tests will show network availability, server and load capacity, query latency, reachability and transaction capability. DNSSEC support, including the full life cycle of KSK and ZSK keys will be proven. Since the DNS system is already operational and used by more than 19 different TLDs, setting up managed DNS services is a routine task for PCH staff.

-OBTAINING IANA DELEGATION-
All requirements for delegation will be satisfied, including adherence to relevant ICP-1 instructions.

-ON-GOING MANAGED DOMAIN NAME REGISTRY SERVICES-
Day-to-day operations of the TLD once it is set up involve several aspects of DNS: technical, administrative, support, financial and policy. From a technical perspective, all hardware and software on the system will be maintained and updated regularly. Monitoring of system stability and security occurs constantly. Escrow deposits will be made on a daily basis and ICANN reports will be submitted when required. Registrar relations will be managed, including OTE, EPP and Whois support. Specialized accounting and traffic reports will be produced and shared with relevant parties required for business operation and systems maintenance. Required configuration updates or changes will be made. Consensus or temporary policy changes enacted by ICANN will be incorporated into the system.

Question 31, is a summary of responses to Questions 32-44. All staff necessary for critical registry services and vital business operations only a registry service provider can provide are listed below and described in the attachment "Q 24 Staff." In the response to each specific question that follows, allocation of resources for each function is noted and described.

-RESOURCING PLANS-
We are outsourcing registry service provision to Minds + Machines. This response lists the personnel in their registry operation. For complete descriptions of each position, please refer to attachment "Q 24 Staff."
CEO
CFO
CMO
CTO
VP Policy
VP Client Services
VP Corporate Development
Director Legal Affairs
Compliance Administrator
Controller
Registrar Liaison
Registrar Cust Svc Admin 1
Registrar Cust Svc Admin 2
Registrar Cust Svc Tech 1
Registrar Cust Svc Tech 2
Network Ops Manager
Network Engineer 1
Network Engineer 2
Network Engineer 3
Espresso Application Developer
Espresso Application Developer 2
Espresso Application Developer 3
Database Developer
Database Developer 2
Information Security Officer
Database Administrator
Database Administrator 2
Marketing Manager
Public Relations Associate
IT Support Specialist
Executive Assistant
Office Manager
Network Architecht
Ombudsperson

-DNS: PCH-
PCH's technical advisory board sets strategic direction, provides expertise to make specific projects possible and drives them forward. Each member has built

major Internet exchanges or backbone networks and together they provide a basis of operational experience that spans more than twenty years of Internet development around the world.

PCH Staff
All PCH staff members are listed in Question 35.

-NCC (Escrow)-
NCC's resourcing information is described in detail in our answer to Question 38.

-Secondary NOC-
The Secondary NOC (hot standby) site is managed by Tucows. NOC staff that manage the Tucows facility in Brampton, CA also monitor and manage Minds + Machines' secondary failover NOC. Our use of the term "Network Operations Center (NOC)" indicates the co-location facility where the hardware is stored; i.e. the datacenter.

For complete information about Tucows' staff and staffing procedures, please see attachment "Q 24 Staff."

25. Extensible Provisioning Protocol (EPP)

The registry will make use of Espresso, a proprietary fork of the CoCCA SRS, which for many years has utilized an EPP API for the Registrar interface. The Registry System's early adoption and implementation of EPP ensures that all EPP-enabled registrars will be able to easily "speak" to the EPP enabled registry. This standardization minimizes development efforts and ensures regularity for registry transactions. The Espresso EPP implementation adheres strictly to ICANN and IETF standards, and was written according to and is fully compliant with the EPP standards as defined in the following RFCs listed below in RFCs Governing EPP Standards:

5730: Extensible Provisioning Protocol (EPP)
5731: Extensible Provisioning Protocol (EPP) Domain Name Mapping
5732: Extensible Provisioning Protocol (EPP) Host Mapping
5733: Extensible Provisioning Protocol (EPP) Contact Mapping
3735: Extensible Provisioning Protocol (EPP) Transport over TCP

The Espresso Registry EPP provides the four basic service elements as defined in RFC 5730: service discovery, commands, responses, and an extension framework that supports definition of managed objects and the relationship of protocol requests and responses to those objects.

The EPP tool used for the registry interface is compliant with IETF RFC standards, is extensible, scalable, fault-tolerant, configurable, secure, and fully auditable.

Espresso's EPP templates and schemas match the relevant RFCs. The following is a snapshot of EPP schema used by registrars during a one-hour period. More than 30 top-level domains and over 250 registrars are already using CoCCA Tools, the EPP-based ccTLD system Espresso is based on. The registry system is already fully established, validated, and used daily in existing TLDs. When we launch .ECO, contracted registrars will be provided immediate access and will be able to offer the TLD to their established customer bases as soon as they connect to the registry system. OTE is needed at all times for new registrars to test connectivity, and for old registrars to test new functions.

The Espresso Registry EPP component is EPP 1.0 and has all standard extensions. All the EPP Schemas and Templates that are utilized in Espresso are defined in the EPP RFCs listed above.

The Espresso EPP schema follow the IETF standardized EPP format. Please refer to “REQUEST, RESPONSE” in attachment “Q 25 EPP Sample Schemas” for an example of the REQUEST, RESPONSE.

Espresso supports the standard EPP schema including: login, logout, check, info, poll, transfer, create, delete, renew, transfer, update.

Please refer to “Live EPP Schema and Requests” in attachment “Q 25 EPP Sample Schemas” examples showing live EPP schema and requests sent from registrars in the past. They are provided to fulfill the request for sample EPP schema demonstrating the ability to support EPP.

The secondary mode of interface offered to registrars is a secure web administration portal known as the graphic user interface (GUI). This web interface is accessible from any security-enabled browser connected to the Internet, allowing registrars to log into their accounts and manually manage domain portfolios on behalf of their customers. The web interface enables user-friendly registry system administration, TLD management, and registrar portfolio viewing. Registrars may register, renew, transfer, delete, and perform every domain management function. Offering a web interface allows administrative and finance, and customer service users to easily access the full functionality of the registry system. This extended functionality eases use, supports system clients, and expands market reach.

--EXTENSIONS--
In addition to the EPP operations detailed in RFCs 5730 - 5734, the Espresso Registry adds three extensions compliant with the extension framework described in RFC 5730. The additional functionality includes: a redemption grace period, an Intellectual Property verification mechanism, and the ability to provide contact proxies for display in Whois results. Please refer to “EPP Greeting Response Reports” in attachment “Q 25 EPP Sample Schemas” for the EPP greeting response reports the extensions.

Espresso’s EPP extensions are made possible by the extension framework established in the EPP protocol. The framework provides for extensions at all of the protocol, object, and command-response levels, but Espresso has made extensions at only the command-response level. All of Espresso’s extensions relate to existing query or transform protocol commands. The specifics of each extension and the commands they relate to are described in the relevant extension sections that follow.

Espresso’s extensions have been made to query and transform commands and responses as categorized in RFC 5730. The set of query commands is: check, info, poll, and transfer. The set of transform commands is: create, delete, renew, transfer, and update. The specific commands from these sets that apply to each extension will be explicitly stated.

--REDEMPTION GRACE PERIOD (RGP)--
The redemption grace period extension is an extension of the EPP Domain mapping, and is a direct implementation of RFC 3915. Its purpose is to allow a grace period during which a registrar can reverse an action performed against a domain object and receive a refund for the original action. For instance, a registrar can renew a domain, then decide the renewal was a mistake and, by requesting that the domain be “restored” to its previous state, receive a refund. The refund and overall ability to restore a domain is contingent on the registrar exercising the restore

request during the grace period. A domain's state can be restored following any of the transform actions that typically incur a fee or result in a status change: registration, renewal, automated renewal, transfer, and delete. The redemption grace period extension is consistent with the registration life cycle as described in Question 27.

The RGP extension extends the domain info command's response and the domain update command.

The domain info response extension simply tells the state that the domain is in with regard to the grace period by including the element rgpStatus. Please refer to "Extension Element from an Example Response for the info Command" in attachment "Q 25 EPP Sample Schemas" for the extension element from an example response for the info command run on a domain that was recently registered.

The domain update command extension instructs the registry to restore a domain by including a restore element. The restore element can contain an optional report element. Until a report has been filed via EPP or the Registry's web interface, the restore request will remain in a pending state and will not be completed.

An important requirement is that the update request must contain an empty domain:chg, domain:rem, or domain:add element within the standard domain:update element.

Please refer to "Domain Update Command (Report Not Included)" in attachment "Q 25 EPP Sample Schemas" for an example domain update command that requests a restore of the domain but does not include a report.

Please refer to "Domain Update Command (Report Included)" in attachment "Q 25 EPP Sample Schemas" for an example domain update command that requests a restore of the domain and includes the report.

Please refer to "Domain Name Extension Schema for Registry Grace Period Processing" in attachment "Q 25 EPP Sample Schemas" for the formal syntax for the extension.

--INTELLECTUAL PROPERTY (IP) VERIFICATION--
The Espresso Registry adds an extension to support IP verification via the Trademark Clearing House (TMCH) verification.

Using TMCH verification, a client can receive automated, realtime pre-approval for a domain. This is especially helpful during the sunrise and landrush periods as the domain is registered immediately upon TMCH validation rather than going through the application process. When TMCH validation fails, the domain is given statuses pendingCreate and serverHold, thereby preventing the domain from being published to the zone files. The domain validation is then retried through the Registry's admin interface. A notification is sent to the administrator that a domain is pending approval. If an audit of the request proves legitimate, the domain is then published to the zone.

When a registrar includes a TMCH code in the registration request, TMCH validation is performed first against the domain, then against the registrant. If the Registry chooses to not use TMCH verification, registrars will receive an explanatory error in response to the domain:create command.

The IP verification extension extends only the domain:create command. The registrar adds the TMCH element to the extension section.

Please refer to "Example of the domain:create Extension Element with TMCH Information" in attachment "Q 25 EPP Sample Schemas" for an example of the domain:create extension element with TMCH information.

Please refer to "Example of the domain:create Extension Element with Trademark Information" in attachment "Q 25 EPP Sample Schemas" for an example of the domain:create extension element with trademark information.

Please refer to "Formal Syntax for the domain:create Extension with TMCH Information" in attachment "Q 25 EPP Sample Schemas" for the formal syntax for the extension.

--WHOIS CONTACT PROXIES--
The proxy extension provides a framework for registrars to establish a full set of information to be provided in Whois responses while maintaining domain contacts' privacy and still supplying the registry with the required contact related information. The registrar is able to create a contact proxy with similar data elements to those supplied when creating a typical contact. Once created, a proxy can be assigned to any contact controlled by the registrar. For contacts that have been assigned a proxy, Whois responses display the information from the proxy rather than the information for the actual contact.

The contact:create command and contact:create response were extended to facilitate contact proxies via EPP. A registrar may add an extension element that contains the structure to either create a new proxy or assign an existing proxy to the contact. The response to the contact:create command will contain the reference value for the proxy.

All proxies are identified by a reference. The reference can be provided during creation or is otherwise assigned by the Registry. When a proxy already exists, a registrar provides the existingProxy element which contains a reference element. The proxy identified by this reference will be assigned to the contact that is created as a result of the contact:create command.

Creating and updating a proxy is done by providing the newProxy element rather than the existingProxy element. The newProxy element contains a proxyDetails element as a container for the information necessary to create a proxy. The proxyDetails optionally contains a proxy:reference element. If the proxy:reference element matches an existing proxy, the existing proxy will be updated with the proxy details provided, otherwise a new proxy is created. When the proxy:reference element is not included, a reference value is assigned by the Registry.

The EPP aspect of the contact proxies is limited in scope. Only the contact:create command and contact:create command response were extended for contact proxies. The functional gaps in the EPP extension are adequately covered by Espresso's GUI, described above. From the GUI a registrar can assign a proxy to an existing contact, unassign a proxy from a contact, create, update, and delete a proxy.

Please refer to "Example of the Extension Element Creating a New Contact Proxy" in attachment "Q 25 EPP Sample Schemas" for an example of the extension element when creating a new contact proxy.

Please refer to "Example of the Extension Element Assigning an Existing Contact Proxy to a Contact" in attachment "Q 25 EPP Sample Schemas" for an example of the extension element when assigning an existing contact proxy to a contact.

Please refer to "Example of the Extension Section in a Response to a contact:create Command that Assigned a Proxy to a Contact" in attachment "Q 25 EPP Sample Schemas" for an example of the extension section in a response to a contact:create command that assigned a proxy to a contact.

Please refer to "Formal Syntax for the Contact Proxy Extension" in attachment "Q

25 EPP Sample Schemas” for formal syntax for the contact proxy extension.

--EPP PERSONNEL RESOURCES--
The number and type of personnel from Minds + Machines, our registry service provider, allocated to the implementation and maintenance of the EPP interface will vary depending on the stage of registry operations. Since the core registry system is already built, operational, and interfaces daily with registrars, the initial number of personnel allocated to EPP development will be limited to the man-hours required to create and fulfill any outstanding requirements, such as connecting to the Trademark Clearinghouse. Most ICANN-accredited registrars have already passed the OTE and are actively interfacing with Espresso on a daily basis for a TLD that is currently in operation. The Espresso Application Developers will actively keep the EPP extensions and connections up to date with relevant RFCs. The number of developers will scale accordingly as new requirements or functions are introduced, and new registrars that require assistance contract with the registry and require assistance passing the OTE.

The developers will collaborate with the Database Developers and Database Administrators to keep the EPP schema and Espresso platform up to date and in compliance with the relevant RFCs (as detailed in the introduction to Question 25: EPP). The Registrar Technical Customer Service personnel will assist the Registrars during their implementation and operation of the Espresso EPP schema. The Information Security Officer will ensure that all security policies and procedures are followed during the development, implementation, and daily use of the Espresso EPP functionality.

The technical resources required to manage the EPP are adequate, on hand or committed, and/or readily available. We have contracted with Cybercoders of Los Angeles for staff resources. Their analysis of the industry indicates that resourcing for the technical functions of the registry will be fully possible in years 1, 2, or 3 of operations.

Our registry functions are outsourced to Minds + Machines. Their staff resource allocation follows. All costs associated with the technical functioning of the registry are covered by Minds + Machines as per our contract with them. Please see the attachment to “Q 24 Staff” for complete descriptions of each staff position.

Title	Startup	Yr1	Yr2	Yr3
CTO	5%	5%	5%	5%
Developer 1	30%	30%	30%	30%
Developer 2	--	--	30%	30%
Developer 3	--	--	--	30%
Database Dev 1	5%	5%	5%	5%
Database Dev 2	--	--	--	5%
Database Admin 1	--	5%	5%	5%
Database Admin 2	--	--	--	5%
Cust Serv Tech 1	3%	3%	3%	3%
Cust Serv Tech 2	--	--	3%	3%
ISO	1%	1%	1%	1%

26. Whois

26.1 --A HIGH-LEVEL WHOIS SYSTEM DESCRIPTION--
The registry will operate a Whois service on Port 43 according to Specification 4 and in accordance with RFC 3912. The registry will also provide a free public query-based directory service on the web at http://whois.nic.eco. The Whois

directory will display domain name, registrar, and nameserver data. The fields will be formatted to conform to the mappings specified in EPP RFCs 5730, 5731, 5732, 5733 and 5734.

The Whois directory will support standard and Boolean searches (including AND, OR and NOT logical operators). Search results will include domain names matching the search criteria. We will implement appropriate measures to avoid abuse of the feature and ensure that the feature is in compliance with any applicable privacy laws or policies.

We will offer searchability on the web-based Directory Service. We will offer partial match capabilities on the following fields: domain name, contacts and registrant’s name, and contact and registrant’s full postal address. We will offer exact match capabilities on the following fields: registrar ID, nameserver name, and nameserver’s IP address for in-zone hosts (glue records).

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

Mitigation against abuse is achieved via black⁄white listing of IP addresses of known parties. We also configure a maximum hit threshold per IP range. The threshold applies to hits within a certain time, both from a single IP and a network.

Our Whois service meets Specifications 4 and 10 of the new gTLD Registry Agreement:
- Whois service available via port 43 in accordance with RFC 3912, and a web-based Directory Service at whois.nic.eco providing free public query-based access.
- The format of responses follows a semi-free text format, followed by a blankline and a legal disclaimer specifying the rights of Registry Operator, and of the user querying the database.
- Each data object is be represented as a set of key⁄value pairs, with lines beginning with keys, followed by a colon and a space as delimiters, followed by the value.
- For fields where more than one value exists, multiple key⁄value pairs with the same key shall be allowed (for example to list multiple name servers). The first key⁄value pair after a blank line should be considered the start of a new record, and should be considered as identifying that record, and is used to group data, such as hostnames and IP addresses, or a domain name and registrant information, together.
- RDDS availability SLA
- RDDS update time SLA
- RDDS query RTT SLA

Whois output meets the requirements listed in Specification 4 (Registration Data Publication Services). Additionally, each field can be toggled on or off for display on a per-zone basis to ensure compliance with any applicable privacy laws or policies. In other words, the Whois can be configured to accommodate more stringent privacy policies than the full disclosure that is possible. We will comply with Specification 4 such that the data objects listed will be displayed for public Whois records as follows:

Domain Name Data Objects:
    Domain Name
    Domain ID
    Whois Server
    Referral URL
    Updated Date

```
      Creation Date
      Expiration Date
      Sponsoring Registrar
      Sponsoring Registrar IANA ID
      Status
      DNSSEC
   Registrant Data Objects:
      Registrant ID
      Registrant Name
      Registrant Organization
      Registrant Street1
      Registrant City
      Registrant State/Province
      Registrant Postal Code
      Registrant Country
      Registrant Phone
      Registrant Phone Ext
      Registrant Fax
      Registrant Fax Ext
      Registrant Email
   Admin Contact Data Objects:
      Admin ID
      Admin Name
      Admin Organization
      Admin Street1
      Admin City
      Admin State/Province
      Admin Postal Code
      Admin Country
      Admin Phone
      Admin Phone Ext
      Admin Fax
      Admin Fax Ext
      Admin Email
   Tech Contact Data Object:
      Tech ID
      Tech Name
      Tech Organization
      Tech Street
      Tech City
      Tech State/Province
      Tech Postal Code
      Tech Country
      Tech Phone
      Tech Phone Ext
      Tech Fax
      Tech Fax Ext
      Tech Email
   Registrar Data Objects:
      Registrar Name
      Address fields
      Phone Number
      Fax Number
      Whois Server
      Referral URL
      Admin Contact
      Phone Number
      Fax Number
      Email
      Technical Contact
```

Phone Number
Fax Number
Email
Last update of Whois database

Nameserver Data Objects:

Server Name
IP Addresses
Registrar
Whois Server
Referral URL
Last update of Whois database

In addition to the RFC-compliant functions, the system allows character sets that are not ASCII as additional Whois display fields (Local Language contact details).

The registry system will implement abuse-prevention measures, such as white-listing contracted registrars’ IP address ranges for search, black-listing known bad-actors or previous violators, and capping the number of Whois searches possible during a time frame.

The registry administration will comply with applicable laws and policies regarding privacy (see Question 28: Abuse Prevention and Mitigation). The registry, in conjunction with the Vice President for Policy of Minds + Machines, will balance the ICANN Whois data display requirements with local laws, and will ensure compliance by users through enforcement of registration policies.

Third party access to zone files will be provided according to the requirements detailed in Section 2 of Specification 4. The zone files will match the file format standard, and use of data by users will only be permitted for lawful purposes. Bulk access to the zone files will be provided to ICANN and Emergency Operators as specified.

Thin registration data (domain name, registrar, Whois server, referral URL, nameservers, status, update date, creation date and expiration date) access will be granted to ICANN periodically, and thick registration data will be made available in case of a registrar failure.

The registry Whois service complies with RFC 3912 by listening on TCP port 43 for requests from Whois clients. Anyone with Internet access can use the Whois portal to check the registration data for a domain name. The Whois server replies with text content, and terminates in ASCII. As soon as the output is finished the Whois server closes the connection to the client.

--RESOURCE ALLOCATION--

The registry system, Espresso, is already in operation and regularly supports Whois requests for current TLDs. The Minds + Machines software development team will update the registry system code to meet IETF Whois RFC specifications as necessary. Since the Whois function is already built and operational, the software development team allocates personnel resources as needed when changes are required.

26.2 Relevant network diagram: Please see the attached diagram, “Q 26 Whois,” which shows the interrelationships of the Whois with the internal and external registry components.

26.3 --IT AND INFRASTRUCTURE RESOURCES--

The technical resources required to run Whois are adequate, on hand, committed, and readily available. The registry will operate two instances of Whois at the primary registry location, one primary and one hot standby backup; and another two Whois servers at the secondary location.

In the event of failure of one hardware component at the primary registry location, the backup server will handle all transactions until the failed server becomes available again. For further details about failover of Whois, see Question 39: Registry Continuity and Question 41: Failover. Any fail-over of the application or Whois service will not affect registrar transactions as fail-over testing has proven only seconds of downtime.

26.4 --INTERCONNECTIVITY WITH OTHER REGISTRY SYSTEMS--
Connectivity between the Internet, the Primary Site, and the Secondary Remote Site is via multiple redundant connections, as further described in Question 32: Architecture. In addition, connections between servers on the internal Registry Network are via redundant multi-homed 1 Gbps Ethernet. Connectivity between the primary and secondary registry facility (for replication) is via redundant SSH connections. In addition, a third data backup in a remote location is connected for disaster recovery.

High capacity routers and switches are used to route traffic to registry services (see response to Question 32: Architecture). Load balancing is used to distribute load across resources.

Internet connectivity will be supplied via a 100Mbps solution with fully diverse connections to multiple Internet service providers. Further details can be found in Question 32: Architecture and Question 35: DNS. The Registry Internet connections at both the Primary and Secondary Sites will be provisioned to support burstable 1 Gbps capacity.

When an update, for example, to a domain registrant record is made to the registry database, Whois automatically reflects these changes because it is an element of the overall SRS. There is never inaccuracy of the published data because of this configuration.

26.5 --DATA CENTER CONNECTIVITY--
Our primary NOC is a co-location facility hosted by Interxion, in Dublin, US. Interxion provides a multi-home Internet circuit presented as dual fibre connections. The Internet access is meshed across a number of carriers, which not only provides resilience but also minimizing latency. Interxion is carrier-neutral and is host to 18 of Europe’s leading Internet Exchanges allow for access to considerable additional Internet bandwidth if required.

Our secondary NOC, managed by Tucows at Q9, in Brampton, CA ,is directly connected to major Internet backbones and regional ISPs available in the vicinity of the Q9 data center. In addition, Q9 has a 1Gb Fibre connection to 151 Front (co-location facility) and a 1Gb Fibre connection to Tucows’ main office at 96 Mowat Ave. The office at 96 Mowat Ave has a 1Gb Fibre connection to 151 Front (co-location facility) creating a 3 x 1Gb triangle between the Q9 data center, 151 Front and 96 Mowat. At the Q9 data center, Tucows has a 1Gb Internet connection to Allstream. At the 151 Front, Tucows has a 1Gb Internet connection with Cogent and a 1Gb Internet connection with Level3. Tucows peers with TORIX and Rogers at 151 Front and, if needed, can aggregate up to 3Gb of Internet traffic to the Q9 datacenter via the 2 x 1Gb links to 151 Front and 96 Mowat + 1 Gb from Allstream. Tucows currently owns all its IP blocks, has its own ASN and BGP configuration and retains full control of peering and IP space. Tucows is fully autonomous and do not rely on third parties to provide or manage network peering capabilities.

Tucows maintains a dedicated, high-speed, low-latency, path-diverse network between its facilities in each geographic region. These regional networks are used to provide reliable, cost-effective connectivity based in different Tucows data centers within the same region.

The secondary NOC provides customers with a redundant Internet connection, a 100 per cent availability SLA and the flexibility to scale to higher bandwidth requirements.

Q9 maintains a dedicated, high-speed, low-latency path-diverse network between its facilities in each geographic region. These regional networks are used to provide reliable, cost-effective connectivity for customers with multi-site solutions based in different Q9 data centers within the same region. Solutions range from traditional switched Ethernet to dedicated wavelengths.

26.6 --FREQUENCY OF SYNCHRONIZATION BETWEEN SERVERS--
Updates from the SRS to the Whois servers happens in real-time via an asynchronous publish⁄subscribe messaging architecture. These are updated in each slave within the required SLA of 95% ≤ 60 minutes. See Question 30: Security and Question 32: Architecture for further details.

26.7 --POTENTIAL FORMS OF ABUSE OF SEARCHABLE WHOIS, AND MITIGATION--
Because the IETF Whois protocol has no provisions for strong security, the Whois directory service is vulnerable to abuse of access control, integrity, and confidentiality. The registry system Espresso features several functions to mitigate data mining, server overload, and access abuse, as explained below.

The web interface for Whois can be configured through the Espresso Registry administrative area. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is used on the web form to mitigate data mining. Network and IP limits are configurable to prevent overloading the Whois server with malicious or extraneous requests. Whois look-ups will be set to 100 requests every 60 minutes for unknown IP ranges. Network limits will be set to 1000 request every 1440 minutes for unknown networks. When the limits are reached, the requests will be restricted and a message will be displayed notifying the user that the limit has been reached. The message also provides instructions to the user to contact the registry if they would like to have their IP or Network range white-listed. Whois request records will be archived, in order to provide law enforcement officials with any necessary information they require for enforcement.

A blacklist is used to block IP addresses or networks of known bad actors. Similarly, a white list may be used to allow trusted users greater Whois look-up access. Terms of use will be displayed on the Whois interface, notifying all users of the terms and conditions for access to the Whois database.

The registry system logs all Whois queries. A server status field displays the number of active requests for a specified time range. The request logs can be searched by the minute, hour, day, month, year, and since delegation. These logs can be output and downloaded as comma-separated value (CSV) files and subsequently used to generate any type of report required.

The Whois server is constantly monitored to ensure 100% uptime. The monitoring tool outputs reports showing the number of queries, and response rates over variable time periods. Whois service will be in full compliance with the final specification of ICANN’s Registration Data Publication Services Document.

26.8 --RESOURCE ALLOCATION--
The SRS registry system, Espresso, is already operational and regularly supports Whois requests for the current TLD operated by Minds + Machines, .FM. The software development team will update the registry system code to meet IETF WHOIS RFC specifications as necessary. The CTO allocates personnel resources as needed to maintain the Whois infrastructure, and to update the code and hardware when changes are required. The Network Operations Managers and technical staff maintain the hardware that supports the Whois function. The Database Developers and Administrators ensure that the Whois element of the application is able to access real-time data from the registry database. The Director of Legal Affairs and the

compliance administrator assures that the Whois function and data displayed complies with ICANN consensus policy, privacy policies, and applicable laws and regulations. The Registrar Customer Service technical support personnel assist registrars with Whois access, including white-listing known and trusted IP ranges.

Our registry functions are outsourced to Minds + Machines. Their staff resource allocation follows. All costs associated with the technical functioning of the registry are covered by Minds + Machines as per our contract with them. Please see the attachment to “Q 24 Staff” for complete descriptions of each staff position.

Title	Startup	Yr1	Yr2	Yr3
CTO	2%	2%	2%	2%
Director Legal Affairs	2%	2%	2%	2%
Compliance Administrator	--	5%	5%	5%
Registrar CS Tech 1	2%	2%	2%	2%
Registrar CS Tech 2	--	--	2%	2%
Network Operations Mgr	2%	2%	2%	2%
Network Engineer 1	2%	2%	2%	2%
Network Engineer 2	--	--	2%	2%
Network Engineer 3	--	--	--	2%
Espresso Application Dev	10%	10%	10%	10%
Espresso Application Dev 2	--	--	10%	10%
Espresso Application Dev 3	--	--	--	10%
Database Developer	5%	5%	5%	5%
Database Developer 2	--	--	--	5%
Information Security Officer	5%	5%	5%	5%
Database Administrator	--	5%	5%	5%
Database Administrator 2	--	--	--	5%

27. Registration Life Cycle

The proposed registration life cycle for this TLD is similar to the life cycle requirements for current gTLDs. The registry adheres to all IETF EPP RFCs relevant to the domain life cycle. The proposed life cycle for the TLD is consistent with the technical, operational, and financial plans proposed for this TLD.

The following paragraphs and timeline describe the proposed life cycle of the domain as well as the criteria and procedures used to change the state.

The Registry will support the following registration states:

- Active: The registry sets this status. The domain can be modified by the registrar. The domain can be renewed. The domain will be included in the zone if the domain has been delegated to at least two nameservers.

- Registry Hold: The registry sets this status. The domain cannot be modified or deleted by the registrar. The registry must remove the Registry Hold status for the registrar to modify the domain. The domain can be renewed. The domain will not be included in the zone.

- Registrar Hold: The sponsoring registrar sets this status. The domain cannot be modified or deleted. The registrar must remove Registrar Hold status to modify the domain. The domain can be renewed. The domain will not be included in the zone.

- Suspend: The domain is suspended and no longer resolves. The domain cannot be transferred. The domain is still part of the zone file but the nameservers have been temporarily modified to ns1.suspended.eco.

- Exclude: The domain name is excluded from the zone file. It is still entered in the registry database but will not resolve nor display as “available”.

- Redemption Period: The registry sets this status when a registrar requests that the domain name be deleted from the registry and the domain has been registered for more than 5 calendar days (if the delete request is received within 5 days of initial domain registration it will instead be deleted immediately). The domain will not be included in the zone. The domain cannot be modified or purged; it can only be restored. Any other registrar requests to modify or otherwise update the domain will be rejected. The domain will be held in this status for a maximum of 30 calendar days.

- Pending Restore: The registry sets this status after a registrar requests restoration of a domain that is in Redemption Period status. The domain will be included in the zone. Registrar requests to modify or otherwise update the domain will be rejected. The domain will be held in this status while the registry waits for the registrar to provide required restoration documentation. If the registrar fails to provide documentation to the registry within 7 calendar days to confirm the restoration request, the domain will revert to Redemption Period status. The domain status will be set to Active only if the registrar provides documentation to the registry within 7 calendar days to confirm the restoration request.

- Pending Delete: The registry sets this status after a domain has been set in Redemption Period status and the domain has not been restored by the registrar. The domain will not be included in the zone. Once in this status all registrar requests to modify or otherwise update the domain will be rejected. The domain will be purged from the registry database after being in this status for 5 calendar days.

- Suspend and pending delete: The domain has been suspended and is pending deletion.

- Exclude and pending delete: The domain has been excluded from the zone and is pending deletion.

- Inactive: The domain is not actively resolving in the .ECO zone. This status occurs when the nameservers associated with the domain are inaccurate or not working.

- Pending Transfer: A request has been made by the registrar to transfer the domain to another registrar. It remains in pending state until the transfer has been authenticated.

- Deleted: The domain has been deleted from the database, and will be made available again for registration.

- Server Lock: The nameservers are locked by the registrar to prevent any unauthorized changes.

- Registrar Lock (also known as “Client Lock”): The sponsoring registrar sets this status. The domain cannot be modified or deleted. The registrar must remove Registrar Lock status to modify the domain. The domain can be renewed. The domain will be included in the zone.

- Registry Lock: The registry sets this status. The domain cannot be modified or deleted by the registrar. The registry must remove the Registry Lock status for the registrar to modify the domain. The domain can be renewed. The domain will be included in the zone if the domain has been delegated to at least two nameservers.

--REGISTRATION LIFE CYCLE--
The following process describes the typical registration life cycle and all intervening steps of a steady-state domain registration that may apply through the full life cycle:

- A domain name is available to be registered.

- A registration request for a one to ten year term is received at the registry, the domain is created, the domain status is “Active,” and the domain is added to the zone file. The domain may be locked.

- If the domain is renewed, the status remains “Active.”

- If the domain record is updated, the status remains “Active.”

- If the domain is transferred, the status remains “Active.”

- If the domain is deleted, the status is updated at the database as “deleted,” and the domain is removed from the zone file.

- A five-day “Add-Grace” period exists where names deleted during that Add-Grace period become available for re-registration.

- Once the domain expires, The “Auto-Renew Grace” period begins. It lasts 30 days from the date of the domain expiry. The domain may be in the zone file during this time, but the state is changed to “suspended.” The domain can be renewed and transferred during this time.

After the Auto-Renew Grace period is over, the “Redemption Grace” period begins. This is also known as the “Pending Delete-Restore” period. The domain is no longer in the zone (the website and email no longer function), but the record is still in the registry database. The Redemption Grace is a 30-day period. During this period, the registrant can “redeem” their domain name, thereby renewing it and making it active again. The domain cannot be transferred during this time.

If the domain is not redeemed within the 30 day Redemption Grace period, the “Pending Delete” period of 5 days begins. The domain is no longer in the zone and the website and email no longer function.

Finally, the domain is released from the registry database and made available for registration. The registration life cycle begins anew.

--DOMAIN TRANSFER PROCESS--
The following process describes the typical Domain Transfer process between Registrars:

- A request for the transfer of the domain is received at the registry.

- If the domain is active and not locked, and the correct authentication code is submitted, the domain is instantly transferred to the new registrar.

- If no authentication code is submitted, the domain goes into “Pending Transfer” status. The losing registrar must confirm the transfer out to the gaining registrar.

- If an incorrect authentication code is submitted, the transfer is denied.

- Once the transfer is complete the domain reverts to “Active” status.

--DOMAIN EXPIRATION--
The following process describes the typical process when a domain expires:

- When the domain has expired the status changes to “on-hold,” and the domain no longer resolves.

- During Auto-Renew Grace Period the domain may be renewed for the regular price; the domain cannot be transferred until it is renewed.

- During the Redemption Grace Period, the status is Pending-Delete-Restorable. The domain is no longer in the zone file. A redemption fee may be paid to re-gain the domain during the Redemption Grace Period.

- After the 30-day Redemption Grace Period, the domain can no longer be automatically restored; status is Pending-Delete.

- After five days at Pending-Delete status, the domain is dropped from the registry database and made available for registration once again.

27.1 --SUNRISE LIFE CYCLE--
Implementation of the Trademark Clearinghouse (TMCH) process may alter the typical registration life cycle during Sunrise. Until the TMCH process is finalized, the registry will continue to support the historical Sunrise registration life cycle as follows:

- Application received at registry, domain is created, status is Inactive.

- Application approved by auditor, domain status is Pending.

- If application is unique, domain status is updated to Active and may be locked to prevent transfer, server update, renewal or deletion.

- If application is not unique, applicant wins collision auction, domain status is updated to Active and may be locked.

- If application is not unique and applicant loses collision auction, registration application is denied and record is archived.

--LANDRUSH LIFE CYCLE--
The following process describes the typical Registration Life Cycle during Landrush:

- Application received at registry, domain is created, status is Inactive.

- If application is unique, domain status is updated to Active and may be locked.

- If application is not unique, applicant wins collision auction, domain status is updated to Active and may be locked.

- If application is not unique, applicant loses collision auction, application is denied and record is archived.

--STEADY STATE DOMAIN REGISTRATION LIFE CYCLE--
The following process describes the typical Registration Life Cycle during Steady State Domain Registration: Full Life Cycle
Domain name is available.

- A registration for a one- to ten-year term is received at the registry, the domain is created, the domain status is “Active,” and the domain is added to the zone file. The domain may be locked.

- If domain is renewed, status remains “Active.”

- If domain record is updated, status remains “Active.”

- If domain is transferred, status remains “Active.”

- If domain is deleted, status is updated at database as “deleted,” and domain is removed from the zone file.

- A five day Add-Grace Period exists where names deleted during Add-Grace become available for re-registration.

- Once the domain expires, The Auto-Renew Grace Period begins. It lasts 30 days from the domain expired date. The domain may be in the zone file during this time but the state is changed to “suspended.” The domain can be renewed and transferred during this time.

- After the Auto-Renew Grace Period is over, the Redemption Grace Period begins. This is also known as the Pending Delete-Restore period. The domain is no longer in the zone (the website and email no longer function), but the record is still in the registry database. The Redemption Grace is for 30 days. During this period, the registrant can “redeem” their domain name, renewing it and making it active again. The domain cannot be transferred during this time.

- If the domain is not redeemed, within the 30 day Redemption Grace Period, the Pending Delete period of 5 days begins. The domain is no longer in the zone and the website and email no longer function.

- Finally, the domain is released from the registry database and made available for registration. The registration life cycle begins anew.

The life cycle of a domain in steady-state (in other words, after the Sunrise and Landrush periods) is illustrated in the attachment “Q 27 Life Cycle Diagram” which captures definitions, explanations of trigger points, and transitions from state to state.

--RESOURCE ALLOCATION--
The registry platform, Espresso, has been built to meet the standard ICANN gTLD life cycle formats. Almost every domain name life cycle function is automated; EPP commands from the registrar to the registry to modify status such as pending transfer, delete, etc. require no personnel resources. The Sunrise validation will be automated with the implementation of the required Trademark Clearinghouse. The Database Administrator manages some life cycle elements such as exclusion and the manual approval of domain names that are on hold. The Compliance Administrator ensures that the Espresso Registration Life Cycle is in compliance with ICANN consensus policies, and IETF RFC requirements. The Development team ensure the life cycle process and fields are supported by the application and in the database. The Vice President for Policy intervenes when a domain name may contravene our Acceptable Use Policy or other policy. The registrar technical support staff assist the registrars with any life cycle issues.

Our registry functions are outsourced to Minds + Machines. Their staff resource allocation follows. All costs associated with the technical functioning of the registry are covered by Minds + Machines as per our contract with them. Please see the attachment to “Q 24 Staff” for complete descriptions of each staff position.

Title	Startup	Yr1	Yr2	Yr3
Compliance Administrator	--	5%	5%	5%

Registrar CS Tech 1	2%	2%	2%	2%
Registrar CS Tech 2	--	--	2%	2%
Espresso Application Developer	5%	5%	5%	5%
Database Developer	5%	5%	5%	5%
Database Administrator	--	5%	5%	5%

28. Abuse Prevention and Mitigation

28.1 --ABUSE POINT OF CONTACT--
Strong abuse prevention is an important benefit to the Internet community. .FASHION and its registry services provider, Minds + Machines, agree that a registry must not only aim for the highest standards of technical and operational competence but must also act as a steward on behalf of the Internet community in promoting the public interest. One of those public interest functions for a responsible domain name registry includes working towards the eradication of abusive domain name registrations, including, but not limited to, those resulting from:

- illegal or fraudulent actions
- spam
- phishing
- pharming
- distribution of malware
- fast flux hosting
- botnets
- distribution of child pornography
- online sale or distribution of illegal pharmaceuticals

Minds + Machines provides the staff and technology to handle abuse prevention and mitigation. Roles and responsibilities refer to Minds + Machines staff. The Compliance Administrator (CA) serves as the primary Abuse Point of Contact (as required by ICANN). CA will be responsible for overall policy development and enforcement.

CA will administer the complaint resolution process, and communicate with registrars (with the assistance of the Registrar Liaison), with law enforcement, the World Intellectual Property Organization and industry organizations such as the Anti-Phishing Working Group and the Registration Abuse Policies Working Group. Minds + Machines’ Chief Technical Officer (CTO) will also serve as the secondary Abuse Point of Contact. The CA, CTO or other personnel will be reachable on a 24/7 basis to deal with any alleged abuses that require immediate attention, whether from law enforcement or otherwise.

On the technical side, the Chief Technology Officer (CTO) is responsible for implementing abuse prevention and mitigation software on the Espresso registry platform and the abuse information and reporting features of the website.

All of the Registry staff will be trained to (i) respond to communication concerning abuse via the published (the required abuse point-of-contact) and restricted (only available to law enforcement and the customers) contact details; (ii) perform sufficient verification to distinguish genuine claims from the malicious and from false positives; (iii) enter the details into the abuse tracking and monitoring system; (iv) identify and contact the registrar of record, inform them of the complaint, initiate a prompt investigation of the complaint and note any information received back from the registrar; and (v) report progress to the complainant at appropriate times.

Primary and secondary Abuse Points of Contact, as well as designated employees, will be supplied with pagers and smart phones, and create an "on call" roster to assure 24x7 availability of abuse prevention and mitigation resources.

The website will prominently display and provide easy access to policies, resources available for handling complaints regarding abuse, and how to contact the designated Abuse Point of Contact. The Abuse Point of Contact staff will provide timely responses to complaints.

An abuse and complaint tracking and monitoring system will be set up as part of the registry software and maintained by Minds + Machines on our behalf. No further resourcing or provisioning will be required to maintain this effective 24x7 system.

28.2 --ABUSE PREVENTATION AND MITIGATION PROGRAM--
The abuse prevention and mitigation program (the "Program") is based on best practice policy recommendations developed by the Council of Country Code Administrators (CoCCA), on lessons learned from previous new gTLD launches, on the operating experience of TLDs such as .COM, and on participation in policy working groups and debate at ICANN. All policies are consistent with and conform to ICANN consensus policies where applicable. Twenty‑five ccTLDs use the CoCCA policy framework to ensure protection of the registry, and to minimize abusive registrations and other activities that affect the legal rights of others. We have updated the best parts of these policies to the new gTLD environment to protect the specific needs of the registry and the registrants, and the rights and needs of third parties. Wherever applicable, we follow the recommendations of NIST SP 800-83 Guide to Malware Incident Prevention and Handling.

The Program is comprised of policies, procedures and resource allocation that aim to prevent and mitigate abusive practices at all levels of registry operations and domain name use.

The Program aims to: (i) prevent the registration of names that violate policies; (ii) provide efficient procedures for the reporting and removal of names that violate policies if they are registered; (iii) provide efficient procedures for the reporting and removal of domains which engage in abusive or unlawful practices; and (iv) secure and protect domain name ownership and Whois information.

The Program is designed to provide for the transparent and non-discriminatory registration of domain names; to protect Whois data and privacy; to ensure adherence by registrars and registrants to the Acceptable Use Policy (AUP); to protect trademarks and prevent registration of blocked and reserved names; to prevent the registration of illegal terms and inappropriate names; to prevent violations of the law; to combat abuse of the DNS; to address cybercrime; to protect intellectual property, and to align use of the registry with the applicable regulatory and legislative environments. We note that while as a registry operator we cannot remove prohibited or unlawful content from the Internet, we can and will seek to ensure that the network is not part of the abuse or publication chain.

The Program is balanced between the need to prevent abusive registrations and uses, the need to properly implement ICANN policies and follow applicable laws, and the need to respect the legal rights of registrants and others. The goal is to encourage legitimate use while discouraging abusive or illegal use. We recognize the importance for the overall health and reputation of the registry that we handle abusive registrations and use quickly, fairly and impartially.

The Program will be administered to (i) ensure that registrars adhere to registration policies; (ii) enforce the policies with registrars and registrants; and (iii) prevent any violations as effectively and efficiently as possible. The means for enforcing policies and procedures will be the comprehensive contract, which sets out penalties for non-compliance; and the registry software, through which some regulations and procedures will be enforced (for instance, blocking reserved names and displaying Trademark Clearinghouse notices and warnings).

The Program employs a model that includes registry-level suspensions for AUP and other policy violations; and also provides that the use of a domain is subject at all times to the AUP's provisions concerning cybercrime, prohibited content, intellectual property abuses and other issues of importance to the Internet, security, intellectual property, legal and law enforcement communities.

Below we describe various agreements and policies, each of which will be a part of the Program:

(1) REGISTRANT AGREEMENT - The Registrant Agreement, which must be presented to the registrant for agreement by the registrar as a condition of registration, binds the registrant to ICANN-mandated rights protection mechanisms, including the Uniform Dispute Resolution Policy ("UDRP"), AUP, Privacy Policy, Whois Policy, and the Complaint Resolution Service. At the time of registration, registrars will be contractually required, pursuant to the Registry-Registrar Agreement, to bind registrants to these agreements.
(2) REGISTRY-REGISTRAR AGREEMENT (RRA) - The primary mechanism for ensuring that registrars adhere to registration guidelines, meet the obligations set forth in the policies and pass them on to registrants will be through the RRA we will sign with registrars. The terms of the RRA adhere to ICANN policies and contain additional abuse safeguards. The RRA includes provisions that must also be included in the contract between registrars and registrants. Registrars may include additional provisions, but those provisions may not conflict with the language provided by us, and registrars must include the terms and conditions in their entirety, and legally bind registrants to them. It is by this mechanism that registration and use policies, regulations and procedures will be passed on to registrants. The RRA contains provisions to combat abusive registrations or use as required by ICANN policies, applicable laws, and the registry's Acceptable Use Policy.

(3) ACCEPTABLE USE POLICY (AUP) - The AUP is incorporated by reference into the Registrant Agreement. It defines the acceptable use of second-level domains, and is designed to ensure that the registry is used for appropriate and legal purposes. It specifically bans, among other practices, the use of a domain name for abusive or illegal activities, including (i) illegal, fraudulent, misleading, or deceptive actions or behavior; (ii) spamming (the use of electronic messaging systems to send unsolicited bulk messages, including email spam, instant messaging spam, mobile messaging spam, the spamming of Web sites and Internet forums, and use of email in a Distributed Denial of Service (DDoS) attack); (iii) phishing (the use of counterfeit Web pages that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data); (iv) pharming (the redirecting of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning); (v) willful distribution of malware (the dissemination of software designed to infiltrate or damage a computer system without the owner's consent--e.g. computer viruses, worms, keyloggers and Trojan horses); (vi) 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); (vii) 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 DDoS attacks); (viii) distribution of obscene material, including but not limited to child pornography, bestiality, excessive violence; (ix) illegal or unauthorized access to computer networks or data (illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another party's system, often referred to as "hacking," or any activity that may be used as a

precursor to an attempted system penetration, such as port scanning, stealth scanning, probing, surveillance or other information gathering activity); (x) deceptive or confusing uses of the domain or any content provided thereon with respect to any third party’s rights; (xi) disrupting the registry network or the provision of any content capable of disruption of computer or systems or data networks; (xii) providing circumvention technologies, technical information or other data that violates export control laws; (xiii) spoofing (forging email network headers or other identifying information); and (xiv) distribution of any other illegal or offensive material including hate speech, harassment, defamation, abusive or threatening content, or any other illegal material that violates the legal rights of others including but not limited to rights of privacy or intellectual property protections.

(4) PRIVACY AND WHOIS POLICY - The Privacy & Whois Policy is incorporated into the terms and conditions presented to potential registrants. It is designed to prevent abuse by: (i) requiring that registrants provide us with accurate information to be included in their “thick” Whois listing; (ii) by requiring that registrars proactively require registrants to verify and⁄or modify their Whois information to ensure its accuracy on an ongoing basis as per ICANN policy; and (iii) making the failure to provide or maintain complete and accurate Whois information a material breach of the Registrant Agreement, which will allow us to cancel any registration for which the Whois information is not accurate or complete.

(5) EXPIRED DOMAIN DELETION POLICY – As per ICANN policy, the Expired Domain Deletion Policy sets out how a domain name is registered and renewed, and includes policies and procedures for redemption and grace periods.

(6) NAMING POLICY - The Naming Policy sets out policies governing prohibited, blocked, and reserved names and eligibility criteria for registrants. It also provides registrants with information regarding trademark and third party rights in names, and offers guidance on choosing a domain name that comports with the policies, regulatory and legal policies, and the rights of third parties. This Policy will provide registrants with the list of blocked and reserved names; explain the rights of trademark holders and the role of the Trademark Clearing House in the registration process; and explain the policies concerning “typosquatting” - misspellings, “typos” or other names that give false or misleading impressions.

A plain language version of the policies will be made available to registrars and potential registrants. Registrants will be required to give their informed consent to be bound by the policies during the registration process, but we recognize that registrants may not fully understand what they are agreeing to when they register a domain name, because the contractual language can be difficult, particularly for a non-native reader of English. As an example, registrars will present the terms and conditions to the registrants and secure their agreement prior to registration. The terms and conditions are many pages long and contain words and concepts that may not be familiar to an average Internet user. Since registrants cannot adhere to policies if they cannot understand them, we will also require registrars to provide a prominent link to a “plain-language” overview of the policies posted on the website. This link will set forth the major terms and conditions in non-legal terms in order to make them understandable to the average registrant. While contracts will be the official and legally binding agreements, we believe the plain-language overview will be very useful for conveying to registrants the major points of their obligations with regard to their domain name itself and their use of that domain name.

The policies and the plain language overview will be prominently available on the website together with explanations and links to the Uniform Rapid Suspension (URS) Service, the UDRP, and the Complaint Resolution Service, with instructions and facilities for reporting alleged abuses to us directly.

28.3 --ANTI-ABUSE MEASURES PRIOR TO REGISTRATION--
The Program will include policies and procedures designed to prevent abusive registrations and use from the start by providing users with guidelines for choosing names, informing them of the proper and improper use of those names, and the consequences of abuse. The anti-abuse measures prior to registration include:

(1) Implementation of the Trademark Claims Service (TCS): In the case where a potential registration is an exact match to an applicable trademark in the Trademark Clearing House, the TCS automated notification service will inform registrants that the name they may be about to register may be a violation of the trademark rights of a third party, and that their registration may be subject to challenge and possible cancelation. We will not, however, reserve or block domain name registration of terms, or confusingly similar terms, which might infringe intellectual property or other rights. The Naming Policy will however advise registrants that prior to registering the name, it is the registrants' responsibility to determine whether or not any particular term might infringe the intellectual property or other legal rights of an entity or individual. The Policy will also encourage registrants to perform a trademark search with respect to the term comprising the domain name prior to registration, and inform the registrant that it is solely liable in the event that the name constitutes an infringement or other violation of a third party's rights, which may include criminal liability for willful, fraudulent conduct.

(2) Prohibition of a duplicate application for registration of a domain name with another registrar: The policies prohibit a registrant from submitting an application for a domain name if the registrant has previously submitted an application for registration of a domain name for the same term with another registrar where the registrant is relying on the same eligibility criteria for both domain name applications, and the name has previously been rejected by a registrar or by the registry.

(3) Preventing numerous attempts to register reserved or blocked names: The policies provide that registrants who repeatedly try to register reserved or blocked names, or names that infringe the rights of others, will be banned from registering domain names. Further, any domain names registered to them will be cancelled or transferred, as provided for in the Registrant Agreement and AUP. We specifically inform such users that we reserve the right to refer them to appropriate legal authorities.

(4) Blocking⁄flagging certain names: We will be able to enforce many of the registration policies at the point of registration through the Espresso platform. For example, the Espresso platform can block certain prohibited names from registration. In addition, domain names that are doubtful--for instance names that contain within them blocked or reserved names--or portions thereof--may be flagged for further review before they are delegated. We believe that a robust implementation of registration policies through the registry software is the best first line of defense against certain types of violations. The Espresso platform is easily programmed to disallow any registrations set forth on the list of blocked or reserved names.

28.4 --POST-REGISTRATION ANTI-ABUSE MEASURES--
Even with policy implementation, oversight, and automated anti-abuse features, abuse registration and use may occur. In addition, innocuous domain names may be used for abusive purposes, such as phishing or spamming. Therefore, post-registration policies and procedures are designed to effectively and efficiently prevent and mitigate abuses with respect to registered domain names themselves and also their use.

(1) Suspension⁄Cancellation: The policy framework allows us to suspend or cancel registrations that violate certain terms of the Registrant Agreement and related policies. We reserve the right to cancel or suspend any name that in our sole judgment is in violation of the terms of service. With cancelation, to the extent permitted by applicable law, we may publish notice of the cancelation, along with a rationale for the decision.

We believe that this step is important for several reasons: (i) It will help us keep the trust of Internet users, who will see that our actions are not arbitrary; (ii) it will act as a deterrent, as violators’ names will be published; and (iii) it will provide valuable additional information to users about which names are considered violations, by providing examples of names that have been canceled because they are offending terms.

In the case of clear-cut violations of the policies, we will take immediate action without refund of the registration fee.

(2) Putting domain names in a “pending” status: In certain cases where we determine that a registration may be in breach of the policies, we may put a registration in “pending” status, in which the registration itself is not affected, but in which the domain name will not resolve. Names in a “pending” state can be restored to operational status. In this case, we will inform the registrant of the initial determination and provide the registrant with a speedy mechanism, such as the Complaint Resolution Service, to assist us in resolving the issue, or to appeal the decision.

(3) Infringement of trademarks: With respect to registrations that infringe trademarks, ICANN has policies and procedures in place that provide a wide net of protections. These policies provide for very quick cancelation of obvious infringements via the Uniform Rapid Suspension (URS), and for less obvious violations, the UDRP. These policies are the result of many years’ experience and extensive negotiations with the trademark community. Additionally, these mechanisms are reasonably well understood by both trademark holders and registrants. We believe that abiding by ICANN’s established policies for dealing with alleged trademark infringing registrations provides the best level of protections for both trademark owners and applicants. We will make the URS and UDRP mandatory procedures for handling such disputes through contracts with the registrars.

A more detailed discussion of the rights protection mechanisms may be found in Question 29: Rights Protection Mechanisms.

(4) Complaint Resolution Service (CRS): While ICANN has a number of procedures in place to prevent abusive registrations, especially with regard to violations of intellectual property rights, we will in addition implement a CRS. The CRS is a formal process that provides a low-cost, efficient, neutral, and clear-cut mechanism for complaints from the public concerning alleged illegal content, abusive or disruptive use of a domain name (e.g. phishing or spam) or other inappropriate conduct to be fairly adjudicated. The policies provide that the CRS is available to anyone, including rights holders. The CRS is a multi-step process designed to ensure fairness and is analogous to an ombudsperson process. It provides an easy method for lodging complaints while protecting registrants from arbitrary, harassing, or repetitive meritless claims. The CRS is described in detail in Question 29.

(5) Trademark Claims Service (TCS): In addition to warning potential registrants prior to registration that their choice of domain name may infringe the rights of others, the TCS will inform trademark holders that a potential infringement of their mark has been registered. This will provide the trademark holder with the opportunity to challenge the registration, via the URS, UDRP, or court action. The

TCS will provide means to inform trademark holders who have successfully deposited their trademarks in the Trademark Clearing House that a domain name has been registered that exactly matches their trademark.

28.5 --PROMOTION OF WHOIS ACCURACY--
As set forth in the Registrant Agreement, Whois Privacy Policy and related agreements we will take significant steps to collect and maintain complete and accurate Whois information.

To ensure Whois accuracy, the Registration Agreement requires that a registrant provide us with (i) true, current, complete, accurate, and reliable registration information; and requires (ii) that the registrant will maintain, update, and keep their registrant information true, current, complete, accurate, and reliable by notifying their registrar of a change to any such information in a timely manner. The Registration Agreement makes clear that providing true, current, complete, and accurate contact information is an absolute condition of registration of a domain name. Registrants are required to acknowledge that a breach of these provisions will constitute a material breach of the Registration Agreement, and that if any registration information provided during registration or subsequent modification to that information is false, inaccurate, incomplete, or misleading, or conceals or omits pertinent information, we may in our sole discretion terminate, suspend or place on hold the domain name of any Registrant without notification and without refund to the Registrant.

Whois accuracy verification at the point of registration as well as over the life of a registration will be carried out by the ICANN-accredited registrars pursuant to the terms of ICANN policy as embodied in the RRA.

Registrants are required to provide the following information to an accredited registrar, who will then provide it to us: (i) Legally recognized first and last name of the contact person for the registrant (this contact person may be the registrant itself), and if the Registrant is an organization, association, corporation, Limited Liability Company, Proprietary Limited Company, or other legally recognized entity, we require that the contact person must be a person authorized under the applicable law in the applicable territory to legally bind the entity; (ii) valid postal address of the Registrant; (iii) working e-mail address of the Registrant, and (iv) working telephone number for the Registrant, including country code, area code, and proper extension, if applicable. Attempted registrations lacking any of these fields will be automatically rejected by the system.

The Registration Agreement provides that the registrant is responsible for keeping the registrant information up to date and responding in a timely fashion to communications from registrars regarding their registered domain names.

Validation of Whois information prior to registration has not met with success among top-level domains. Historically, in many country-code top-level domains, pre-validation has been abandoned due to depressed user adoption and criticism from end users and industry businesses, such as web hosting companies, ISPs, and domain name registrars. With few exceptions, major registries validate Whois information after the domain name is delegated, if at all. This reduces cost, which keeps prices down and allows for the near-instant registration of domain names by ordinary registrants.

We will not use pre-delegation validation of registrant data. The strong policies against abusive registrations, combined with the easy-to-use CRS and active enforcement response, will better balance the needs of consumers and law enforcement or other users of Whois information than pre-verification, and in addition will result in higher customer satisfaction.

We will discourage illegitimate or abusive registrations by pricing our domain names above the price of .COM or .BIZ, which we believe will discourage various forms of noxious behaviors, as cybercriminals typically register large numbers of domains for their schemes and will therefore face a larger cost of doing business if they attempt to use the registry for their schemes. We therefore propose to price domain names at a wholesale cost higher than existing gTLDs as a way to discourage malicious use of second-level domain names. With fewer illegitimate registrations, we expect that Whois accuracy will be higher.

28.6 --ADEQUATE CONTROLS TO ENSURE PROPER ACCESS TO DOMAIN FUNCTIONS--
The RRA provides that a registrar must ensure that access to registrant accounts are adequately protected, at a minimum, by secure log-in process that requires username and password authentication, and comport with other security related ICANN registrar accreditation requirements. Registrars must ensure that its connection to the Shared Registry System (SRS) is secure and that all data exchanged between registrar’s system and the SRS is protected against unintended disclosure. Registrars are required to use multi-factor authentication and encryption methods for each EPP session with the SRS using both a server certificate identified by the Registry and the registrar password, which is disclosed only on a need to know basis.

To protect unauthorized transfers of domain names, the registry generates a Unique Domain Authentication ID, or UDAI (also known as an “authorization code” or “auth code”), and provides the UDAI only to the registrant, in a secure manner. A UDAI is a randomly generated unique identifier used to authenticate requests to transfer domain names from one registrar to another. A UDAI is generated when a domain name is registered. Registrars will be obliged to promptly support domain transfers from qualified registrants upon request and may not withhold them to prevent a domain name from being transferred, nor may they require burdensome manual steps (such as requiring a signature) as a condition of transferring a domain name to a new registrar.

Registrars will further be required to identify a duly authorized officer (or similar senior manager) to handle cases where a company or organization wants to make changes but where the original registration was performed by an individual working for the company in his or her own name. For example, a company might hire a web developer to design a web site, and ask the developer to register a domain name, which they may do, but in his or her own name. The purpose of this policy is to prevent mistakes in the case of a transfer of ownership. The instructions on the change of registrant form must ensure (i) that the current authorized registrant is authorizing the changes; (ii) that the prospective registrant is identified and that all relevant contact information has been provided; (iii) that the prospective registrant acknowledges the changes and agrees to be bound by all of agreements and policies; (iv) that the process utilized by the registrar for the change of registrant process is clearly identified to registrants; and (v) that all documentation and correspondence relating to the transfer is retained. Registrars may request a statutory declaration where they have concerns about the authority to effect the change in registrant details if the registrars have concerns about the authority to effect a change in registration or any detail thereof and include an indemnity clause for any costs, losses, or liabilities incurred in the reasonable performance of their duties in processing the registrant's request, or in dealing with claims arising from the allocation or use of the name.

The Minds + Machines CA will be responsible for ensuring that the ICANN-accredited registrars are implementing security protocols to provide adequate controls regarding access to registrants’ registration information. The RRA will provide that we may audit the registrant account access policies and procedures of the ICANN-accredited registrars to ensure their compliance with the policies. These audits will be carried out by the CA on a random basis or in response to a report or a complaint that a registrar is not complying with the account access policies. Failure to correct deficiencies identified in any audit may be considered a material breach of the RRA.

28.7 --ORPHAN GLUE RECORDS--
The registry policies and Shared Registration System (SRS) rules do not allow for orphan glue records in the zone. All glue records are automatically removed from the zone when the parent domain is deleted by the Espresso SRS. This automated registry software process prevents what are known as “fast-flux” phishing attacks.

28.8 --RESOURCE ALLOCATION--
The Abuse Prevention and Mitigation functions will be carried out by members of the Minds + Machines Technical and Legal staff. The CTO oversees the technical team in their development and implementation of, abuse prevention mechanisms such as black lists, removal of orphan glue records, automated warning emails, and creation and ongoing management of domain status fields such as “suspended” when a domain registration is under review for policy violation. The VP of Policy, the Director of Legal Affairs and the Compliance Administrator perform the duties of Abuse Point of Contact, complaint review, collaboration with law enforcement, and other legal duties necessary to conform to ICANN consensus policies, registry Acceptable Use Policies, and local laws.

Our registry functions are outsourced to Minds + Machines. Their staff resource allocation follows. All costs associated with the technical functioning of the registry are covered by Minds + Machines as per our contract with them. Please see the attachment to “Q 24 Staff” for complete descriptions of each staff position.

```
Title
-----
CTO
VP Policy
Director Legal AffairS
Compliance Administrator
Registrar Cust Svc - Tech 1
Registrar Cust Svc - Tech 2
Espresso Application Developer
Espresso Application Developer 2
Espresso Application Developer 3
Database Developer
Database Developer 2
Information Security Officer
Database Administrator
Database Administrator 2
```

29. Rights Protection Mechanisms

--PROTECTION OF LEGAL RIGHTS: A CORE OBJECTIVE--
Ensuring the protection of the legal rights of others is a core objective. We believe that protecting third-party rights enhances the reputation of the registry and encourages registrants. We are therefore committed to the protection of legal rights and have developed a series of mechanisms, including but not limited to, those minimum requirements for rights protection mechanisms as detailed in Specification 7. These mechanisms are intended to prevent infringing or abusive registrations and to identify and address the abusive use of registered names on an ongoing basis and in a timely manner. As part of this commitment, we have developed and will maintain and implement a series of related policies and practices specifically designed to prevent infringing and abusive registrations

and uses of domains that affect the legal rights of others. We will take reasonable steps to investigate and respond to any reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD.

--OVERVIEW--
As well as implementing all ICANN rights protection mechanisms (RPMs), we will introduce other additional RPMs that go beyond the current ICANN protections.

In order to do so, we have developed a detailed policy framework based on best practices from the ccTLD .NZ, from the Council of Country Code Administrators (CoCCA), and from existing gTLDs. This tapestry of policies provides rules and procedures regarding registrant eligibility; sets out which type of names can be registered and which cannot; defines abusive registration and usage and provides for penalties for non-compliance; describes and implements ICANN-mandated RPMs; and binds registrars and registrants to the major policies.

The major policies are the Naming Policy, which defines which names can be registered, and by whom; the Acceptable Use Policy, which describes permitted and non-permitted uses of registered names; the Whois and Privacy Policy, which helps registrants understand what we can and cannot do with their personal data; and the Complaint Resolution Services (CRS).

Registrants are bound to these four policies as a condition of registration through their contracts with their registrars, who are in turn compelled by us to get registrant consent to the policies as a condition of registration.

The Naming Policy first of all defines blocked and reserved names, which include geographical names at the second level, thereby adhering to ICANN rules and protecting the rights of governments. Secondly, it prohibits the registration of infringing names and specifically binds registrants to ICANN RPMs. It contains provisions beyond ICANN RPMs, such as prohibiting multiple attempts at blocked names, either through the same or by using different registrars. The Naming Policy further provides that we may sanction registrants who do not abide by its provisions by revoking names (with or without refund) and in appropriate cases informing law enforcement.

The Acceptable Use Policy (AUP) addresses abusive use of second-level domain names, prohibiting spam, phishing pharming, malware, illegal content and other abusive uses of second-level domain, including abusive registrations, particularly registrations that infringe the rights of third parties. Many best practices concerning infringing registrations that were developed in among ccTLD world have in the gTLD world been superseded by Consensus Policies developed at ICANN. Where ICANN has procedures and policies, we follow them. Therefore, the AUP requires that registrants abide by the terms of the Uniform Domain Name Dispute Resolution Policy (UDRP), the Uniform Rapid Suspension service (URS), and the Trademark Claims Services (TCS). Another ICANN-mandated rights protection mechanisms (RPM), the Sunrise Period, will be implemented as described later in this response.

Above and beyond the ICANN-mandated RPMs, the AUP contains provisions that exceed ICANN policy minimums to provide a higher standard of protection for the legal rights of others. The AUP allows us to suspend or cancel names, or multiple names by the same registrant, if an egregious use or pattern of abusive or infringing use is engaged in by a registrant. In addition, the Complaint Resolution Service (CRS) provides means for Internet users to alert us to abusive or infringing registrations.

Additional prevention or mitigation of abusive or infringing registrations include rapid takedown procedures; cancelation or suspension of multiple domain names registered to the same flagrant abuser; higher prices to discourage mass registrants of abusive names; and protection of second-level geographic names.

We first describe the implementation of ICANN-mandated mechanisms, then follow that with a description of the additional policies we plan to implement to prevent registration abuse and rights infringement.

--SUNRISE--
The Sunrise Period is mandated by ICANN, as per Section 6.2 of the Trade Mark Clearinghouse module of the registry agreement. It is a process by which owners of legal rights have the opportunity to register domain names before the process opens to the public or others. Specifically, rights holders may use the Sunrise Service to assert a priority right to register a second-level domain which matches their eligible word mark, as defined in paragraph 7.2 of the Trade Mark Clearinghouse module of the registry agreement. An identical match (as defined in paragraph 6.1.5 of the Trade Mark Clearinghouse module of the registry agreement) is required between the eligible word registered in the Trademark Clearing House (“TCH”) and the domain applied for as a condition of participation in the Sunrise Period. All Sunrise applications will be validated by a third-party verification agent through the ICANN-mandated TCH to check the eligibility of the legal right claimed.

We will offer the Sunrise period for a minimum of 30 days during the pre-launch phase, and according to the terms of the Sunrise Policy. Applications received within that period are treated as filed at the same time. Where there is a contest between valid claimants, allocation will be determined by auction.

The Sunrise policy will provide for a Sunrise Dispute Resolution policy, which will allow a challenge under the four grounds required in paragraph 6.2.4 of the Trade Mark Clearinghouse module of the registry agreement. Other grounds may be added as experience reveals their advantages.

Policy oversight of the Sunrise Service will be provided by the Minds + Machines Vice-President of Policy. Operational oversight of the Sunrise Period will be provided by Minds + Machines’ CEO, Antony Van Couvering. Antony is a veteran of several Sunrise periods as the head of a registrar (NameEngine) specializing in providing services to large brands and other holders of trademarks. We will provide all necessary infrastructure and sufficient resources to support the Sunrise Period.

--TRADEMARK CLAIMS SERVICE--
We will provide a TCS during an initial launch period for eligible marks as defined in para 7.1 of the Trade Mark Clearinghouse module of the registry agreement. This launch period will last at least the first 60 days of general registration, and will be operated according to the terms of Trademark Claims Policy.

The TCS allows a trademark owner to register a claim asserting trademark rights by putting potential registrants on notice of its possible legal claim of the domain name being considered for registration. We will provide notice in the approved format to all prospective registrants of domains that match trademarks in the TCH that their registration may infringe a trademark right. The mandatory form requires a prospective registrant to specifically warrant that: (i) the prospective registrant has received notification that the mark(s) is included in the TCH; (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.

Additionally, the Trademark Claims Notice will provide the prospective registrant with access to the Trademark Clearinghouse Database information referenced in the

Trademark Claims Notice to enhance understanding of the trademark rights being claimed by the trademark holder. These links (or other sources) will be provided in real time without cost to the prospective registrant. The Trademark Claims Notice will be provided in the language used for the rest of the interaction with the registrar or registry, and will be provided in the most appropriate UN-sponsored language as specified by the prospective registrant or registrar⁄registry.

Oversight of TCS will also rest with the Vice President of Policy (VPP). We will provide the necessary infrastructure and sufficient resources to support the VPP in this role, including adequate computers, connectivity, telephones including cell phones and administrative support.

Responsibility for implementing the customer-facing (registrar) aspects of the Trademark Sunrise Service and TCS will rest with the Registrar Liaison as part of their on-going responsibilities. Responsibility for the technical implementation of the Trademark Sunrise and TCS will rest with the Registry under the contract to provide registry services. Minds + Machines' CTO, network engineer, and systems engineer will maintain the functionality of the automated Trademark Clearinghouse system. No additional resourcing is required to support these functions, as they are part of the base level requirements for the Registrar Liaison and the CTO. We will pay fees to the TCH for Sunrise and TCS services. At the present time no fees details are available, but we assume that the higher fees we propose to charge Sunrise applicants during the 60-day TCS period will be sufficient to cover the fees likely to be charged by the TCH.

--PHISHING AND PHARMING--
Phishing and pharming are a kind of rights infringement in which the malefactor pretends to be a trusted source by using another's trademark, brand look-and-feel, or other protected property in order to lure Internet users to perform some action that benefits the perpetrator. These practices are prohibited by the AUP and will result in cancelation of any second-level domain name involved, and possibly in cancelation of additional names registered to the abuser.

--POST DELEGATION DISPUTE RESOLUTION POLICY--
In the Registry Agreement with ICANN, we will agree to participate in all post-delegation procedures and to be bound by the resulting determinations. Because we are fully committed to combatting abusive use and abusive registration of second-level registrations, we do not expect to have occasion to be involved in any proceedings stemming from ICANN's Post Delegation Dispute Resolution Policy (PDDRP), which deals with registries who knowingly engage in trademark infringement or abet those who do. We will comply with all Consensus Policies adopted by ICANN, including the PDDRP.

--ADDITIONAL ANTI-ABUSE POLICES--
We will be implementing RPMs and anti-abuse measures that go beyond the UDRP, URS, Sunrise, TCS and other ICANN-mandated mechanisms and procedures. These additional measures are detailed below.

--COMPLAINT RESOLUTION SERVICE--
The Complaint Resolution Service (CRS) is an alternative to litigation for resolution of complaints between the registrant of a domain name and a complainant who alleges a registrant or a domain name is in violation of the AUP. The CRS provides a transparent, efficient, and cost effective way for the public, law enforcement agencies, regulatory bodies, and intellectual property owners to address concerns regarding abuse on the system.

The CRS provides a reliable and simple way for the public to inform us if they think there is a problem. Submissions of suspected infringement or abuse are monitored by Registrar Customer Service personnel and escalated according to severity. Upon escalation, we may take immediate action to protect registry system or the public interest or refer the matter to law enforcement if we suspect criminal activity. In the case of a non-critical complaint, the CRS also provides an amicable complaint resolution and adjudication service conducted by an Ombudsperson hired by Minds + Machines. The CRS is a service intended to supplement parties' existing legal rights to resolve a dispute in a court of law. Any proceeding brought under the CRS will be suspended upon any pleading to a court, decision-making body, or tribunal, and only re-started if directed to do so by one of those bodies.

The Ombudsperson is a neutral third-party specialist with respect to conflict resolution who will provide informal arms-length mediation and adjudication of any complaints of alleged registrant abuses and violations of the AUP. The Ombudsperson shall have the power to direct that a domain name should be cancelled, suspended, transferred, modified or otherwise amended.

If the Ombudsperson takes a decision that a domain name registration should be cancelled, suspended, transferred, modified, or otherwise amended, the Ombudsperson will implement that decision by requesting the Registry to make the necessary changes to the Register. The CRS provides for a right of appeal by registrants if they believe the AUP has been enforced in error.
We will comply with the decisions of the Ombudsperson and the Appeal Panel under the direction of the VPP.

--PROVISIONS OF THE ACCEPTABLE USE POLICY--
The AUP defines a set of unacceptable behaviors by domain name registrants in relation to the use of their domain names. It is incorporated by reference into the Registrant Agreement. It defines the acceptable use of second-level domains, and is designed to ensure that the registry is used for appropriate and legal purposes.

The AUP specifically bans, among other practices, the use of a domain name for abusive or illegal activities, including:

(i) illegal, fraudulent, misleading, or deceptive actions or behavior;
(ii) spamming (the use of electronic messaging systems to send unsolicited bulk messages, including email spam, instant messaging spam, mobile messaging spam, the spamming of Web sites and Internet forums, and use of email in a Distributed Denial of Service (DDoS) attack);
(iii) phishing (the use of counterfeit Web pages that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data);
(iv) pharming (the redirecting of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning);
(v) willful distribution of malware (the dissemination of software designed to infiltrate or damage a computer system without the owner's consent--e.g. computer viruses, worms, keyloggers and Trojan horses);
(vi) 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);
(vii) 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 DDoS attacks);
(viii) distribution of obscene material, including but not limited to child pornography, bestiality, excessive violence;
(ix) illegal or unauthorized access to computer networks or data (illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another party's system, often referred to as "hacking," or any activity that may be used as a precursor to an attempted system penetration, such as port scanning, stealth scanning, probing,

surveillance or other information gathering activity);
(x) deceptive or confusing uses of the domain or any content provided thereon with respect to any third party's rights;
(xi) disrupting the registry network or the provision of any content capable of disruption of computer or systems or data networks;
(xii) providing circumvention technologies, technical information or other data that violates export control laws;
(xiii) spoofing (forging email network headers or other identifying information); and
(xiv) distribution of any other illegal or offensive material including hate speech, harassment, defamation, abusive or threatening content, or any other illegal material that violates the legal rights of others including but not limited to rights of privacy or intellectual property protections.

--MALWARE--
The AUP prohibits the use of the second-level domains to spread or install malware. Malware is software that is installed without the knowledge of the end user, or without the full understanding by the user of the software's effects, which are often deleterious or dangerous. It should be noted that malware cannot be spread by the registration of a domain name. Where applicable, we will adhere to and implement the recommendations of NIST SP 800-83, "Guide to Malware Incident Prevention and Handling." We have documented polices, processes, and procedures to mitigate operating system and application vulnerabilities that malware might exploit, as explained in further detail in our answers to Question 30: Security and Question 32: Architecture. We will implement a malware awareness program that includes guidance to users on malware incident prevention, detection and how to report suspect infections.

As recommended in NIST Special Publication 800-61, "Computer Security Incident Handling Guide," we have instituted a robust incident response process to address malware, which has four main phases: preparation, detection and analysis, containment⁄eradication⁄recovery, and post-incident activity. In order to be prepared, we will implement malware-specific incident handling policies and procedures. As part of our detection objective, we will review malware incident data from primary sources and monitor malware advisories and alerts to identify likely impending malware incidents. We understand that we can play a critical role in the containment and eradication process of malware, and we will develop strategies and implement procedures, reflecting the appropriate level of risk, to contain and mitigate malware threats. The policies will clearly define who has the authority to make major containment decisions and under what circumstances various actions are appropriate. We reserve the right in contracts, and will not hesitate to use that right, to shut down or block services, such as email, that are used as vectors by malware producers. We also reserve the right and are prepared to place additional temporary restrictions on network connectivity to contain a malware incident, such as suspending Internet access or physically disconnecting systems from network, even while we recognize the impact such restrictions might have on organizational functions. Our strategy for the recovery phase from malware incidents is to restore the functionality and data of infected systems and to lift temporary containment measures. Our strategy for handling malware incidents in the final phase includes conducting a robust assessment of lessons learned after major malware incidents to prevent similar incidents from occurring in the future.

Additionally, we will work with the Anti-Phishing Working Group and other industry leaders, including ICANN working groups on phishing and pharming, to ensure that our practices allow parties to act quickly when a registrant is in violation of the policies. Finally, we reserve the right to immediately terminate any activity deemed, in our sole judgment, to be abusive, in violation of the AUP or related policies, or against the public interest.

--RAPID TAKE-DOWN PROCEDURES--

The AUP and related policies provide for a rapid take-down of abusive domains that are in violation of the policies, including mass domain shutdowns to act against DDoS, phishing abuse, and Botnet exploitation of domain names. Experience has shown that aggressive policy enforcement, combined with user-accessible complaint procedures to shut down obviously abusive names discourages malefactors, who have the option of registering in more loosely administered TLDs, such as .COM or .INFO.

--PROTECTION OF GEOGRAPHIC NAMES--
We will enact measures for the protection of country and territory names. The geographical names contained in the lists described in Specification 5 of the registry agreement will be added to the registry software system "prohibited word" function. Any attempt to register a domain containing those geographical names will be automatically denied, as they were similarly blocked in the .INFO TLD. See our answer to Question 22: Protection of Geographic Names for a more complete description of polices to protect geographic names.

--COMMUNITY FLAGGING--
We will use the common practice of community flagging of abusive uses of domains in order to rapidly detect a possible abuse so that a rapid response may be provided, including a rapid take-down of an abusive domain. Community members can easily flag a domain name as potentially abusive by filing notice through the Complaint Resolution Service. The CRS provides a "community flagging" mechanism that allows Internet users to report suspected violations and has proven to be an effective and speedy policy to prevent unwanted behavior. Internet web sites such as Craigslist, OK Cupid and many others use community flagging as their primary means of combating illegal and abusive behavior, and we will implement it in the registry.

--SUSPENDING MULTIPLE DOMAINS FOR FLAGRANT ABUSE--
The Registry reserves the right to suspend all domain names registered to or associated with any user for flagrant or repetitive abuse of any domain name as a means of preventing and curtailing abuse of the systems.

--TRANSFER FEES TO MITIGATE ABUSE--
To create a deterrent to abuse in the registry, we will charge registrants with a processing fee for transferring domains to another registrar or registrant. The transfer processing fee assessed will not be high, but will act as a deterrent by those who register multiple domain names for their schemes.

--QUALIFICATION OF REGISTRANTS--
We will have no general eligibility requirements for registration as pre-qualification of registrations is not applicable to our business model. Validation of Whois information prior to registration has been met with widespread user non-adoption among top-level domains historically. In country-code top-level domains such as .FR (France), .ES (Spain), .PT (Portugal), and .SE (Sweden), pre-validation has been abandoned due to depressed user adoption and criticism from end users and industry businesses, such as web hosting companies, ISPs, and domain name registrars. With few exceptions, major registries validate Whois information after the domain name is delegated, if at all. This reduces cost, which keeps prices down and allows for the near-instant registration of domain names by ordinary registrants.

We will not use pre-delegation validation of registrant data. Our strong policies against abusive registrations, combined with the easy-to-use CRS and active enforcement response, will better balance the needs of consumers and law enforcement or other users of Whois information than pre-verification, and in addition will result in higher customer satisfaction.

We will discourage illegitimate or abusive registrations by pricing our domain names above the price of .COM or .BIZ, which we believe will discourage various forms of noxious behaviors, as cybercriminals typically register large numbers of domains for their schemes and will therefore face a larger cost of doing business if they attempt to use the registry for their schemes. We therefore will price domain names at a wholesale cost higher than existing gTLDs as a way to discourage malicious use of second-level domain names. With fewer illegitimate registrations, we expect that Whois accuracy will be higher.

--IMPLEMENTATION OF POLICY--
The Vice-President of Policy will oversee the management and maintenance of all policies and coordinate their implementation with Minds + Machines' CTO and other technical staff and any third-party service provider partners. The VP of Policy will also be responsible for assuring that the policies are complied with by both registrars and registrants. We are committed to providing sufficient resources to ensure full functioning and effective implementation of these policies, as described below.

We will implement all decisions rendered under the URS and UDRP and courts of law in an ongoing and timely manner. We have designated the Vice-President of Policy as the URS Point of Contact (URSPOC) for proceedings brought under the URS against registrations in the Registry. The URSPOC will monitor the receipt of emails from URS providers informing that a URS complaint has passed Administrative Review, and will, on receipt of such an email, immediately arrange to lock the relevant domain name. Resolution services shall not be affected. The USPOC will also monitor emails from URS providers for determinations in URS cases, and will act on them according to their terms. In those cases where the complainant has succeeded in the URS complaint, the domain name status will be moved from "locked" to "suspended", and will not longer resolve. Where a complainant has been unsuccessful, the domain name will be unlocked, with full control being restored to the registrant. If an appeal is filed, the URSPOC will monitor emails for any change of status resulting from such appeals. The software will designate the status of names during URS proceedings and provide for monitoring to ensure deadlines are met. In order to be able to monitor emails or phone calls and respond quickly, the VPP will be aided by one or more of the Registrar Customer Service representatives.

In the event that the rate of complaints is too high for existing personnel to handle, we will work to automate what can be automated, and hire additional staff as necessary. If a high percentage of complaints are nuisance complaints, or harassing complaints, we may institute a small fee for the Complaint Resolution service in order to prevent capricious use of the service.

Responsibility for maintaining and implementing technical protection mechanisms via the Registry software and hardware rests with the CTO. The CTO will be aided by developers, architect, and technicians in the NOC.

--RIGHTS PROTECTION MECHANISMS--
The Vice-President of Policy will oversee the management and maintenance of all the policies and coordinate their implementation with Minds + Machines' CTO and other technical staff and any third-party service provider partners. The VP of Policy, in co-ordination with the Compliance Administrator, will also be responsible for assuring that the policies are complied with by both registrars and registrants. We are committed to providing sufficient resources to ensure full functioning and effective implementation of these policies, as described below.

In the event that the rate of complaints is too high for existing personnel to handle, we will work to automate what can be automated, and hire additional staff as necessary. If a high percentage of complaints are nuisance complaints, or harassing complaints, we may institute a small fee for the Complaint Resolution service in order to prevent capricious use of the service.

Responsibility for maintaining and implementing technical protection mechanisms via the Registry software and hardware rests with Minds + Machines' CTO, who has worked extensively with enforcing Rights Protections in registries through software applications. The CTO will direct the technical team as necessary. The technical team will implement the trademark clearinghouse and sunrise services at the application level, including connecting to the TMCH, and managing the API for sunrise auction tools.

Our registry functions are outsourced to Minds + Machines. Their staff resource allocation follows. All costs associated with the technical functioning of the registry are covered by Minds + Machines as per our contract with them. Please see the attachment to "Q 24 Staff" for complete descriptions of each staff position.
Title

CTO
VP Policy
Compliance Administrator
Registrar CS Tech 1
Registrar CS Tech 2
Espresso Application Dev
Espresso Application Dev 2
Espresso Application Dev 3
Database Developer
Database Developer 2

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

SUMMARY OF SECURITY POLICY
Registry services are outsourced to Minds + Machines & their subcontracted partners, PCH (DNS, DNSSEC), NCC (data escrow) & Tucows (Secondary Failover Site). The registry is built to meet the security & stability requirements as defined in the ICANN new gTLD Applicant Guidebook. It is a secure, stable, scalable registry with high availability, dependability, & the flexibility needed to meet new gTLD requirements.

Appropriate security features will be documented & embedded within the registry services. Data confidentiality, integrity, & availability is the goal of the security policy. This response provides an explanation of how the security controls & mechanisms that will be put in place are relevant & how independent auditors will validate those controls. In the following discussion, all features mentioned in the present tense currently exist; those in the future tense will be implemented prior to operations.

Registry operations will be run in accordance with the ISO27001 framework. ISO27001 specifies a high level of requirements & best practices for managing internal company & external customer information. It incorporates periodic risk assessments appropriate to all threat scenarios. The policy covers the infrastructure, data centers, & services including SRS⁄EPP, Whois, & DNS.

Once the registry is operational, ISO27001 certification will be pursued. We are committed to providing the highest level of data security. A formal program to maintain the certification will be established, providing the registry with a current & sustainable security policy that is able to handle emerging security threats.

A layered security model will be employed. This approach increases the cost & difficulty of penetration for an attacker. Layering creates multiple points of resistance to intruders, ensures high availability, & decreases the likelihood that attackers will pursue attacks against our organization.

The computing environment is comprised of networks, operating systems, applications, & databases. Customer data is the basic underlying component of the business that we strive to protect; therefore, we focus on providing multiple layers of resistance to unauthorized access to that data.

There will be four basic security functions that will work in a complimentary manner to secure each layer of our computing environment: examination, detection, prevention, & encryption.

Examination identifies vulnerabilities in all computing layers before they become compromised. Automated examination appliances will be employed at the network layer, operating in-line with the network, discovering all assets in the network & then identifying vulnerabilities in each asset.

Using the monitoring tools described in Q 42, each layer of the operating system is monitored, providing detailed information about each host by discovering user accounts, fingerprinting software, & OSes. Vulnerabilities will be scanned for & thus identified by using a pre-defined, regularly-updated rules set. Examination at the OS level provides more in-depth information about a host than network-level examinations, & will be deployed with the use of agents on each host.

In addition to network & OS layer examination, applications & databases are also examined, focusing on vulnerabilities of a software application or database environment.

These products, fully described in Q 32, are written for our software packages & database. Examination products focused on software packages & databases provide the most granular level of security in a layered security model.

Detection products search for pre-existing problems in a computing environment. In -line detection and intrusion prevention products will be employed at the firewall layer, allowing attack signatures to be used to detect intrusions prior to entering our network.

Information will also be kept secure by using prevention products described in the response to Q 32 & Q 42. These tools filter entry into a specific network, & include virtual private networks (VPNs), access control for router & switches, & advanced state-full firewalls using policies to evaluate network traffic.

Firewalls at the network & host layer will use network addresses, port numbers, host names, & services to evaluate whether traffic is allowed into a specific network. Network-based firewalls are the first line in guarding against intrusion. Since this is a multi-site architecture, firewalls have been implemented at the edge to increase intra-site security while protecting against intrusion from the internal network & the external Internet.

Encryption products for data security both in transmission & storage will be employed. Encryption tools modify readable text into a non-readable state prior to decryption. VPN tools, further described in Q 32 (see: Firewall Specifications) focus on creating a secured transmission medium that prevents interception & deciphering of data. Other encryption products focus on securing stored data, both in databases & applications.

Encryption tools allow for secured remote management of critical system resources;

allowing establishment of a connection through a secured tunnel to firewalls, servers, & other critical systems.

Regular security audits by an accredited independent third party are commissioned to formally test & evaluate vulnerabilities & controls within the operations environment. Biannual internal security reviews are performed. The reviews emulate the evaluation performed in a security audit, but also provide detailed reviews of processes, procedures, & systems performance metrics. The documentation that results from internal reviews & external audits are securely archived, & these records can be made available for third parties with management approval.

ACCESS CONTROL
Systems supporting the registry are protected by the state-of-the-art tools described in Q 32 & Q 42, & are maintained in a secure manner. Network access is managed & logged. Access to systems, networks, peripheral devices, power, or other data center services is restricted. At data centers, keycard protocols & round-the-clock interior & exterior surveillance are used to monitor access. Only authorized personnel are granted access to data centers. No one else may enter the production area without prior clearance & an appropriate escort. Every data center employee undergoes background security checks before being hired. Physical access is provided only to personnel who are pre-authorized to perform maintenance. Devices requiring service or maintenance will have parts available to swap in as replacements.

All employees will be screened prior to hire & must agree to the System Access & Usage Policy as part of their contract. Security Awareness training will be provided. A security policy acknowledgement form must be completed & signed by new employees to acknowledge acceptance. Usage-policy statements outlining users' roles & responsibilities will be maintained. Acceptance of Information Security policies & procedures is required from contracted companies & individuals.

At the primary & secondary facilities, access privileges begin with HR. Once the HR team has a signed offer letter & start date, they begin the process to procure equipment, assign seating, create system accounts & grant access. The security team is required to approve all system access requests, whether a new hire or existing hire. Based on the job role, the security team has built access profiles so that all Operations & NOC staff tasked with creating accounts implement the appropriate levels of access.

External access is treated identically. If the profile calls for external access, the employee must be provided with a VPN client & encryption certificate from the Operations team that uniquely identifies the user & provides a second level of authentication. This ensures that external access authentication is two-factor & cannot be shared. External access follows the same profiling hierarchy & is simply an extension, i.e. if an internal employee does not have access to databases, they will continue to NOT have access to databases externally.

The only direct access to the network for Internet traffic is application traffic to & from pre-determined IP Addresses used in combination with recognized protocols on defined port numbers. Security at the network & protocol levels is controlled by the Internet routers & firewalls & is restricted by Access Control Lists.

Network access requires multiple layers of authentication. The system will identify who is connected & where they are, thereby assuring that users will have access to the network resources they need for their defined jobs while business systems & processes are protected from compromise.

For remote access to the system, specific points of entry for special access required by system or network administrators & the security team will be achieved by use of a VPN requiring a client profile & a private shared key, & a unique username⁄password validated against authentication databases.

System, Firewall, Network & other configurations will be updated at scheduled maintenance. The configuration changes are stored in a revision control system for review by security & network personnel, who must approve the changes prior to implementation.

PHYSICAL SECURITY
A variety of physical security systems are used to ensure that unauthorized personnel have no access to sensitive equipment or data.

All servers containing sensitive data are physically secured. Only a controlled list of people can obtain access. All internal networks are isolated from public access, & external Internet links are firewall-protected to prevent intrusion.

Physical precautions inside the server rooms include 24⁄7 video cameras to alert security personnel in case of intrusion. Alarms are fitted to all doors that access the data centers. Trained Data Center security staff are present at all times. Appropriate personnel will be contacted when necessary to help contain the situation as per the incident escalation procedure.

Access to the server room is controlled via two-factor authentication system. All access to the server room is logged & archived. Lost or stolen access card are immediately deactivated. Closed circuit TV is in place at all sites.

CAPACITY TO WITHSTAND ATTACKS
Operational security practices are employed to safeguard the registry infrastructure. Network & server resources are over-provisioned to ensure they can handle large attacks without performance degradation. IP transit link sizes are also over-provisioned, ensuring that capable routing & switching hardware is employed & that servers are sufficiently powerful to serve large query loads.

Hardware firewalls & Deep Packet Inspection (DPI) systems are used to ensure that only required UDP & TCP ports are exposed to the Internet. DPI systems check packet structure & DNS protocol validity on the wire to ensure that correctly-constructed DNS packets are answered by the name servers, reducing the burden on individual name servers by pre-filtering invalid traffic. Strict physical & administrative access policies are enforced.

RESOLUTION PROVISIONING AND DNS SERVICES
The anycast DNS network provided by PCH is designed to provide ample network resources to withstand extreme load situations such as DDoS attack. For overburdened Internet connections the placement of name servers in key exchange points allows DNS responses to reach the servers via an alternative provider. In the event a given site has both Internet connections overburdened, the geographical diversity & number of locations means that there will be another DNS server available.

The PCH anycast networks has more than 70 locations across the globe. The .ECO TLD will be available at all times, & registrants will be able to count on resolution services.

Integrity between the registry & name servers in the PCH anycast cloud is ensured via TSIG-signed IXFRs or AXFRs, ensuring the DNS provider is receiving the zones from a valid source.

The PCH DDoS mitigation approach involves knowing what attack profiles to watch for, having the technology capability & capacity to identify & deflect attacks while allowing legitimate traffic to reach its destination, & possessing the skills & experience to address issues appropriately. See Q 35 for a complete description of the DDoS mitigation approach.

INCIDENT ESCALATION
Support engineers follow established standard operating procedures consistent with the ISO27001 framework. These procedures will be continually reviewed & updated. Responsibilities & escalation amongst response teams will be clearly defined. Measures to test contingency plans for short-term, medium-term, & long-term network or service outages will be employed. These periodic tests will ensure the viability of the procedures, escalation model, & accountability.

THIRD PARTY AUDITS
Regular security audits performed by an accredited third party will be commissioned. Audits involve formally testing & evaluating vulnerabilities & controls within the operations environment. Internal security reviews will also be performed. These reviews involve the evaluation performed in a security audit in addition to detailed review of processes, procedures, & systems performance metrics. The resulting detailed documentation from each internal review & external audit will be securely archived. These records & documents can be made available, with management approval, for third parties when necessary.

Information Security Certification or Assessment
The .ECO registry will undergo annual information security assessments once it is operational. Minds + Machines undergoes annual assessments as well. Tucows, our secondary facility provider, undergoes yearly to bi-yearly IT audits. Tucows has gone through SOX audit & compliance & are PCI certified. Attached as Q 30a Security-Attestation to Compliance is the PCI certification questionnaire. While its purpose & intent are to protect the Cardholder environment, it is very exhaustive & has been extended across all systems when possible.

NETWORK SECURITY
Multi-factor authentication, user identification, passwords & IP range checking will be required for all restricted services including but not limited to access to the Registry database, servers, zone files, & DNS services.

Secure File Transfer Protocols will be used for all file transfers between the Registry & registrars (RFC2228, RFC2577, or similar equivalent).

System maintenance will be performed via SSH, VPN or similarly secured connections.

Each system will operate a very restricted set of basic services in the relevant sections for DNS, Contact Info, FTP, SCP & WWW services. Systems are firewall-protected in hardware, & IP filtering rule sets are in place to reject inappropriate packets.

DNS servers run a limited set of applications & system services. Frequent checks take place on all DNS servers to ensure that data integrity is maintained.

IP-restricted services have each IP address specified individually. Network addresses will not to be used, as this adds the risk that a host could masquerade as a spare IP address on an internal network.

Packet sniffers, designed to check all traffic passing through a network interface, will be in place to catch suspicious traffic. These actively scan for incorrect or illegal packets, & alert the security team. They also give further indications of the source of an attack, used for profiling & preventing that attack in the future.

Network security practices will be verified by a security audit process which involves scanning all TCP & UDP ports on servers operated by the registry.

Security tests will be periodically performed on the servers & the corresponding report is reviewed on a regular basis. Tests attempt to take advantage of specific security flaws using a variety of attack methods, & the results are reported & archived. Known attacks include:

* Buffer overflow exploit
* Missing format string exploit
* Packet fragmentation attack
* Data flooding (SMURF ping, etc.)
* DNS⁄IP spoofing
* FTP spoofing
* Dictionary passwords
* Replay attack
* DDoS
* SQL injection

Tests will be updated as new vulnerabilities, security flaws, or techniques are discovered. These updates are based on industry best practices.

BACKUP SECURITY
Backups are performed through a secure network. Encryption for the backup of all sensitive data is employed. Data is sent to secure locations where it is stored, maintained & recovered for later use. Please see the response to Q 37 for a complete review of the backup security & measures taken to ensure integrity & security of the registry data.

AUDITING & REPORTING
Security reviews are run regularly. In order to maintain ISO27001 certification, there will be an annual external third party security audit performed. Security audits & reviews test all systems for configuration issues and security holes, & compliance with both internal processes & ISO27001 standards. Results of audits form the basis of security reports, which detail any recommendations for system alterations & the timeline for remediation. All security breaches will be recorded, documented, & reported to management.

ROBUST PERIODIC SECURITY MONITORING
Comprehensive monitoring ensures stability & security of critical systems & services. Industry-standard monitoring & alerting practices will be used & will ensure remediation when an impacting event is detected.

See the response to Q 42 for a complete description on security monitoring.

BACKUP
Network access control lists, network & system activities, VPN access, EPP system access logs, & any other form of logging are backed up & stored securely locally & off-site at the secondary data center. Access to backup information is restricted by policy. Archives are encrypted & password-protected on a limited-access server & are retained for a minimum period of one year.

SECURITY CAPABILITIES
Minds + Machines’ security capabilities are consistent with the requirements of the data centers & with the overall business approach & planned size of the registry. The CTO & ISO will be responsible for enforcing the Registry Security Policy & ensuring that the registry technical system complies with ISO27001 standards.

COMMITMENTS MADE REGARDING SECURITY MEASURES
Security levels are appropriate for the nature of the use & level of trust

associated with the .ECO TLD. Registrants can expect a registry environment with the same or better security levels & functionality that current gTLDs provide. The Registry Policies define commitments made to registrants, specifically regarding privacy & protection of personal data.

ADEQUATE RESOURCING IN THE PLANNED COSTS
The planned costs detailed in the financial section show that our registry operations, including security, are provided by Minds + Machines in exchange for a fee. The secure NOC, Firewall & VPN hardware, & staffing for compliance, enforcement, & further security development are all considered in the cost discussion noted in the response to Q 47.

PERSONNEL ALLOCATED
The Information Security Officer (ISO) is responsible for identifying, developing, implementing & maintaining processes across the organization to reduce risks to information & information technology. The ISO also responds to incidents, establishes appropriate standards & controls, & directs the establishment & implementation of policies & procedures. The ISO is responsible for information-related compliance & ensures security policies are kept up-to-date & followed by staff.

Each member of the technical team is tasked with ensuring the registry remains secure. They also ensure the integrity of updates between registry systems & nameservers.

Annex 4.

New gTLD Application Submitted to ICANN by: Big Room Inc.

String: ECO

Originally Posted: 13 June 2012

Application ID: 1-912-59314

Applicant Information

1. Full legal name

Big Room Inc.

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact Information Redacted

4. Fax number

Contact Information Redacted

5. If applicable, website or URL

http://www.bigroom.ca

Primary Contact

6(a). Name

Mr. Jacob Joseph Malthouse

6(b). Title

President

6(c). Address

6(d). Phone Number

Contact Information Redacted

6(e). Fax Number

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Mr. Trevor Scott Bowden

7(b). Title

Secretary

7(c). Address

7(d). Phone Number

Contact Information Redacted

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Corporation

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

Canada Business Corporations Act. See http://laws-lois.justice.gc.ca/eng/acts/C-44/ (Canada Business Corporations Act, Department of Justice, Canada).

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

Anastasia Ruth O'Rourke	Director
David Levi	Chairman
Jacob Joseph Malthouse	Director
Nicholas Fitzpatrick	Director
Trevor Scott Bowden	Director

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

Jacob Joseph Malthouse	President
Trevor Scott Bowden	Secretary

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

Anastasia Ruth O'Rourke	Director
Jacob Joseph Malthouse	President
Trevor Scott Bowden	Secretary

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.

ECO

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.

Big Room anticipates the introduction of the .ECO top level domain (TLD) will be without operational or rendering problems. Based on a decade of experience launching and operating new TLDs, Afilias, the back-end provider of registry services for the .ECO Community TLD, is confident the launch and operation of this TLD presents no known challenges.

The rationale for this opinion includes:

* The string is not complex and is represented in standard ASCII characters and follows relevant technical, operational and policy standards;
 * The string length is within lengths currently supported in the root and by ubiquitous Internet programs such as web browsers and mail applications;
 * There are no new standards required for the introduction of this TLD;
 * No onerous requirements are being made on registrars, registrants or Internet users, and;
 * The existing secure, stable and reliable Afilias SRS, DNS, WHOIS and supporting systems and staff are amply provisioned and prepared to meet the needs of this TLD.

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

Mission/Purpose

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

The Global Environmental Community, the Community to be served by Big Room’s application and that would be implicitly targeted by any application for the .ECO top level domain (TLD), is an alliance of diverse, long-established, and internationally recognized environmental institutions with millions of members worldwide, a clear majority of which support this application.

Formal international evidence of the Community dates back to 1948, with the founding of the International Union for Conservation of Nature (IUCN). The Community has been organizing for over 60 years with respect to specific events, geographies, and issues through a variety of international alliances like 350.org, the Green Economy Coalition, TckTckTck, and since 1972, the United Nations Environment Programme.

The “eco” label has long been used to identify individuals, organizations, and activities committed to respectful, responsible, and sustainable use of the environment. As this label is widely understood as a representation of association with the Community’s goals and values, and to avoid consumer confusion, it is imperative that policy setting responsibility for the .ECO Community TLD be invested in a representative community member institution that provides stable and ongoing Community input and oversight.

In 2009, Big Room, itself a Certified B Corporation obliged to consider environmental, social and financial interests, launched an international multi-year stakeholder consultation process with the Community on the potential for .ECO to exist as a Community TLD. The process included 7 in-person consultations on 5 continents. Draft policies were published for 3 public comment periods of at least 30 days each.

Key to this process was an international council of community organizations, convened by the Meridian Institute at the request of Big Room, to review and consider the results of these global consultations and to reach consensus on the purpose, principles, and policies for .ECO. The council was governed by a Terms of Reference under which participants engaged. The Terms confirmed involvement on a voluntary basis and without compensation or obligation to support Big Room’s .ECO application.

Since establishment, this international multi-stakeholder community council, made up of leading environmental organizations including WWF International, Greenpeace International, Green Cross International and others, has worked to define the mission, purpose and policies for a .ECO Community TLD that reflects the Community’s interests. The council’s work included 2 in-person meetings (Brussels / Washington, DC) and more than 20 conference calls between members. In September 2010, the council unanimously adopted a charter for the .ECO Community TLD - the .ECO Policy Consensus. The purpose and principles outlined in the .ECO Policy Consensus define what .ECO will mean as an active expression of the goals, values and interests of the Community. The Consensus has been reviewed and affirmed by the Big Room board of directors.

Consistent with the Community’s history of organizing alliances around issues, in April 2012 the council formalized into the independent, not-for-profit, Dot ECO Global Community Organization (the Organization). The Organization’s mission is to act as the representative membership institution for the .ECO Community TLD, developing and protecting it and the .ECO Policy Consensus for the greater good.

As the .ECO Registry Operator, Big Room will implement the .ECO Policy Consensus under the terms of a contract with the Organization. .ECO will be operated for the benefit of the community in accordance with the commitments and actions below.

The purpose of .ECO is to:

1. Allow members of the Community to more easily identify themselves and other Community members online and to prevent misuse of .ECO domain names that could lead to confusion.

2. Utilize the power of the Internet to foster transparency, information sharing, communication and exchange of ideas to promote environmental goals, interests and values, amongst Community members and those who are exploring that opportunity.

3. Provide a platform for accurate and non-deceptive information and reliable resources to encourage environmental awareness and action on sustainability.

The underlying principles of .ECO are:

1. PRINCIPLE OF TRANSPARENCY AND ACCOUNTABILITY:

Specific commitments include:

a) Registrants will sign a Registrant Agreement that includes, at a minimum, commitments to: maintain an accurate .ECO-profile; to update or review that .ECO-profile at least annually; to link from their .ECO website to their .ECO-profile (if the two are separate); to provide accurate contact information to the Registry; and to submit to a review of their .ECO-profile if requested by the Registry.

b) The Registry has confirmed and maintains a contract with the Organization, and will implement all elements therein including the .ECO Policy Consensus registration policies. It will ensure those policies, procedures, and agreements are publicly available, and publish environmental performance metrics and indicators as part of its annual report.

c) The Organization has established and maintains a governance structure as defined by a set of bylaws, and confirmed and implemented a contract with the Registry. It will advise on disputes and complaints as requested by the Registry, and publicly report on policy development activities, including meetings and advice.

2. PRINCIPLE OF INCLUSIVENESS

While there is an existing, delineated, historically significant Global Environmental Community, part of the purpose for .ECO is to promote diversity and inclusivity in order to advance environmental goals, interests and values, particularly in developing countries.

Specific commitments include:

a) The Registry will assist and encourage registrants in registering .ECO domains and participating in the Community, particularly in developing countries and where linguistic, cultural or socio-economic barriers may exist. It will recognize and promote credible environmental standards and/or ways of calculating environmental impacts and performance.

b) The Organization is governed by bylaws that set term limits on participation in its governing and advisory bodies and actively identifies and encourages diverse participation and membership.

3. PRINCIPLE OF IMPROVEMENT

Showing improvement over time while recognizing that, due to degrees of variability across sectors and geography, registering a .ECO domain name does not equate to achieving environmental goals, but that continuous improvement towards environmental goals is a key value of the Community.

Specific commitments include:

a) Registrants will update or review their .ECO-profiles at least annually and show demonstrable progress towards environmental goals over time.

b) The Registry will institute an environmental policy for its own operations and require its suppliers and contractors to meet rigorous environmental standards.

c) The Organization will review the Registry’s environmental performance and implementation of .ECO registration policies, recognizing that as environmental goals evolve and progress over time, the policies governing .ECO may also need to evolve. The Organization will review all .ECO registration policies every two years and recommend revisions to the Registry.

In summary, the .ECO purpose and principles are the result of an extensive, independently-mediated public and community consultation process. The purpose and principles are enshrined in the .ECO Policy Consensus, a charter for the .ECO Community TLD that provides Community policy guidance on Naming, Registration, Accountability, and a grant-making foundation. Together, they ensure a .ECO Community TLD created and operated in the public interest and consistent with the Community’s values.

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

WHAT IS THE GOAL OF YOUR TLD IN TERMS OF AREAS OF SPECIALTY, SERVICE LEVELS, OR REPUTATION?

The .ECO Community top level domain (TLD) aims to establish the .ECO System, aggregating the .ECO-profiles of registrants, as a global trusted source of environmental information. Further, the Registry aims to be an internationally-respected TLD that follows best practices in both the Internet and Environmental communities.

In line with this global scope, developing country participation will be prioritized. Recognizing that linguistic diversity is an important part of the Global Environmental Community (the Community), the Registry plans to translate key registry information and systems into the six UN languages.

The .ECO System is also an accountability and compliance tool that will prevent fraudulent registrations and deliver accountability on member actions and commitments, particularly where a lack of transparency contributes to misleading claims about environmental goals or achievements.

II. WHAT DO YOU ANTICIPATE YOUR PROPOSED gTLD WILL ADD TO THE CURRENT SPACE, IN TERMS OF COMPETITION, DIFFERENTIATION, OR INNOVATION?

Big Room and the Dot ECO Global Community Organization (the Organization) believe that the .ECO System will provide a useful alternative to other TLDs. It will allow Community members to identify themselves and interact online, including with entities that are providing products and services aligned with Community values.

Currently, there is no unified way for members to identify themselves online. The .ECO System will be a unique and powerful tool, acting as a common global system for identifying members of the Community through the sharing of information about their actions and commitments. The ICANN DNS is the ideal structure to create an ECO identifier; the Internet community is global and organized in a way that reflects multi-stakeholder processes also prevalent in the environmental community.

Innovation

1. The .ECO System: Registrants will have to create a .ECO-profile on registering a .ECO domain. .ECO-profiles will consist of responses to questions about commitments to the environment and confirmation of community membership based on memberships, certifications, reporting, and other accreditations recognized by the Community.

Every Registrant’s .ECO-profile must be linked to their .ECO website. All .ECO-profiles will be publicly maintained by the Registry in an online database called the .ECO System. Together, .ECO-profiles and websites will create a unique resource of freely available, current, structured environmental data.

The following elements are also included in the .ECO System:

a) Verified .ECO-profiles: To speed .ECO domain activation and enhance existing community profiles, registrants with active public certification profiles at specified member organizations can utilize this profile as a proxy for their .ECO-profile.

b) .ECO-toolkits: Tools for calculating environmental performance, offered to registrants that want to improve their .ECO-profiles (eg, energy use or emissions calculators).

c) .ECO Trust-mark: Registrants can opt to make their .ECO website their .ECO-profile or to create a new website at their .ECO domain. If they choose the latter, they must include a .ECO logo (a trust-mark) on the website that links to their .ECO-profile, ensuring visitors to .ECO websites can discover the registrant’s .ECO-profile.

2. Platform Names: The Registry and the Organization will create a class of names reserved for community dialogue and information sharing. These ‘platform names’ may include industry sectors and keywords that will act as forums for community dialogue. (eg, finance.eco or forestry.eco).

3. Community Partnership: A collaborative process established in 2009 resulted in a new partnership between the .ECO Registry and the Community. This partnership comprises cross-board representation, the .ECO Policy Consensus, and the provision of explicit rights to an independent, not-for-profit community organization governed by community-agreed bylaws, connected to the .ECO Registry via a contract. This approach maximizes efficiency and independent multi-stakeholder community dialogue on .ECO policy.

4. Community Accountability: The Registry will layer community forums, online complaint and abuse reporting, dispute resolution, mediation, and arbitration to ensure eligibility, content, use and naming policies are enforced in a transparent and accountable way. The Registry will engage the Organization on matters requiring broader policy decisions. The Registry will conduct ‘spot-checks’ by reviewing .ECO-profiles to ensure compliance. These mechanisms are explained in an Accountability Policy. Also see Q20(e).

5. Independent Foundation: The Registry and Organization will create an independent foundation funded from sales and renewals of .ECO domains and dedicated to supporting environmental goals. Every user that registers a .ECO domain will know how much of their fee is going directly to the foundation, and users can suggest funding priorities.

III. WHAT GOALS DOES YOUR PROPOSED gTLD HAVE IN TERMS OF USER EXPERIENCE?

Community members will be able to rely on .ECO domains as a form of community identification for individuals, organizations and businesses as well as products and services they provide. In line with guidance from the .ECO Policy Consensus, the Registry’s goal will also be to inform and connect members of the Community and encourage actions that support the environment.

Registering a .ECO domain and creating a .ECO-profile will be inexpensive, user friendly, multi-lingual, and accessible to remote and/or slow internet connections and mobile platforms such as those in rural environments and/or developing countries. Community members will be able to access .ECO domains via existing registrar channels and through Community entities and networks.

Registrants and users will be able to flag exemplary or weak .ECO domains or .ECO-profiles, and suggest areas of improvement for the .ECO policies through the Organization. The Organization will provide a reliable and just accountability framework to resolve disputes in the interests of the Community.

Community members can provide information that highlights their environmental credentials, especially where this information is already public (eg, acknowledged member of an environmental alliance). Registrants can find new ways to engage and achieve Community goals.

Visitors to .ECO services will be able to understand and compare .ECO registrant qualifications and actions via their .ECO-profiles. Search engines will be able to identify the characteristics of a .ECO domain and crawl structured environmental disclosure information in the .ECO-profiles.

IV. PROVIDE A COMPLETE DESCRIPTION OF THE APPLICANT’S INTENDED REGISTRATION POLICIES IN SUPPORT OF THE GOALS LISTED ABOVE

The following registration policy is taken from the .ECO Policy Consensus. It represents Community guidance on the registration policies for the .ECO domain and directs .ECO Registry policies, contracts, and other documents to reflect the community interest. Please also see Q20(e). The Community will continue to review and refine the .ECO Policy

Consensus in accordance with the Dot ECO Global Community Organization’s contract with Big Room as the Community Registry Operator.

Registration Policy

Registration Process: When a registrant applies for a .ECO domain, they will fill out a questionnaire that is relevant to the type of use they identify for the website associated with their domain. The answers will form their .ECO-profile. Before DNS resolution is permitted for their domain, the registrant must demonstrate a commitment to the .ECO purpose, principles and policies by agreeing to the registrant agreement, which includes a commitment to the .ECO mission and purpose, affirmation of membership in the Community, and answering the mandatory .ECO-profile questions.

The Registry will prevent DNS resolution of .ECO names until such time as the registrant submits their .ECO-profile information to support their compliance with the .ECO community eligibility requirements. Provided that this step is completed, active DNS resolution will be enabled.

The Registry will employ standard registration lifecycle mechanisms, statuses, and states such as HOLD or LOCK functions, or other existing Extensible Provisioning Protocol (EPP) commands, in order to disallow a domain to be active when a registrant is not in compliance with the community eligibility requirements or under related community dispute resolution procedures.

Use Types: Different .ECO use types will have varying impacts and potential contributions to environmental goals. Therefore, registrants will be asked to respond to different questions based on declared type of use. The five types of .ECO use initially will be: not-for-profit, business, individual, government, and product.

Not-for-profit and business may be sub-divided into categories based on a blend of indicators, including number of employees, revenue and, in the future, by resource usage.

Results of the Registration Process: Answers to the .ECO-profile registration questions will be displayed via a required link from the registrant’s .ECO website and will also be searchable through the .ECO System. Archived versions of past .ECO-profiles will also be available through the .ECO System to show progress over time, in line with the Improvement Principle.

Registration Questions: The Organization will develop a process to establish and regularly review .ECO-profile questions. The questions, which must be verifiable, will cover community-recognized memberships, accreditations, registrations, certifications, and reports that demonstrate active commitment, practice and reporting. Additional questions may: be both qualitative and quantitative; include commitments to environmental and social issues that are considered to be linked to environmental goals; and, reference robust existing environmental standards, requirements, indicators, regulations, codes, and calculators.

Registrants holding certain certifications may automatically qualify to register for .ECO domain names without providing additional details through a .ECO-profile. The Organization will establish the qualifications for certified registrations in advance and agreements with certifiers will be put in place to enable rapid, accurate validation. Certified registrants will be identified and promoted as such within the .ECO System.

Community Naming Policies

The .ECO Policy Consensus includes a Names Policy that provides Community guidance on how to align .ECO domain names with Community interests. Key points from the names policy are summarized as follows:

Premium Names - Community-priority: The Organization will approve a list of community-priority names and will work with the Registry to develop a ‘best use plan’ competition. Allocated names will be donated to the winners for a defined term. All community-priority names will be reviewed every two years against their use plans.

Premium Names - Auction-able: The Registry will publish a list of names for auction. Funds generated from these names will be used to support the Registry and the independent .ECO Foundation.

Controversial Names: While some strings could be used in a manner inconsistent with the Community’s goals, values and/or interests or may be highly controversial, and/or potentially undermine trust in the .ECO Community TLD, controversial names will not be automatically blocked. Instead, the Organization will develop a method to flag strings based on existing public policy, Community recommendations, industry sector and green-washing watch-lists, and research/surveys. Registrants selecting identified names will be notified that registration will be subject to additional scrutiny.

Platform Names: The Registry will reserve names that could be useful in implementing the .ECO Purpose and .ECO System (eg, names of industry sectors, environmental issues or significant nouns).

Other Policies

Other reserved names will be those required in Specification 5 of the new gTLD Registry Agreement per our response to Questions 21 and 22. The Registry’s name, operations names, and variations thereof, names related to ICANN, Internet standards bodies, and United Nations Organizations, Funds and Programs, for delegation of those names to the relevant organizations upon their request.

The complete list of reserved, platform, auction-able, community-priority, and controversial names will be published publicly prior to Sunrise. The Registry will create policies that ensure clear and fair distribution of names. For example, all employees of the Registry and its contractors will be strictly prohibited from bidding for or allocating .ECO domains.

The Registry will continue to use the Trademark Clearinghouse during general availability for notifications of new registrations only where the string is a complete match with a filing in the Trademark Clearinghouse. The Registry will address this process asynchronously to the registration process and in consideration of the technical capabilities of the Trademark Clearinghouse.

Dispute Resolution Mechanisms: Registrants and rights holders will have access to fair and transparent processes to adjudicate claims to domains that also protect registrants against reverse domain hijacking. Names registered in the Sunrise Period will be subject to a Sunrise Dispute Policy. This policy and procedure will be in effect for a finite time period, to provide special protection of qualified trademark rights. See Question 29 (Rights Protection Mechanisms).

.ECO domains will be subject to the Uniform Dispute Resolution Policy (UDRP). See Question 29 (Rights Protection Mechanisms).

.ECO domains will also be subject to the Universal Rapid Suspension (URS) policy. See the URS specifications in Applicant Guidebook Module and Question 29 (Rights Protection Mechanisms) for full details. The Registry will provide systems to take in and administer cases as per ICANN’s Registrar Transfer Dispute Resolutions Policy, allowing registrars to protect registrants by filing disputes about inter-registrar transfers that they believe were unauthorized or improperly executed.

The Registry will support a Community Eligibility Dispute Resolution Process (CEDRP) aligned with the Accountability Policy described in the .ECO Policy Consensus. This dispute process can be initiated by either a member of the .ECO Community or a member of the general public to address an alleged violation of the .ECO member policies or operating requirements by a registrant or registrar.

V. WILL YOUR PROPOSED gTLD IMPOSE ANY MEASURES FOR PROTECTING THE PRIVACY OR CONFIDENTIAL

INFORMATION OF REGISTRANTS OR USERS? IF SO, PLEASE DESCRIBE ANY SUCH MEASURES.

The privacy and/or confidential information of registrants will be protected through several industry-standard measures. We will minimize the mining of WHOIS data by spammers and other parties who abuse access to the WHOIS. See Question 26 for details regarding searchable WHOIS and rate limiting.

The use of privacy services can protect the privacy and personal data of registrants from parties that mine zone files and WHOIS data. The Registry will allow these services where they comply with ICANN policies and requirements. We are also aware of and respect parties who may use privacy services to protect themselves from political or religious persecution. See Question 28 for details regarding privacy services, abuse management, as well as proposed policies to reduce e-crime by limiting the use of privacy services by malicious parties.

The Registry will notify each of our registrars regarding the purposes for which data about any identified or identifiable natural person (Personal Data) is collected and used, as well as the intended recipients of such Personal Data, as per the requirements of the new gTLD Registry Agreement (Article 2.17). Each registrar must also obtain the consent of each registrant in the TLD for such collection and use of Personal Data. We shall not use or authorize the use of Personal Data in a way that is incompatible with the notice provided to registrars.

Security policies and procedures will be used in order to protect the registry system and the data it contains from unauthorized access. As the Registry, Big Room will take significant steps to protect Personal Data from misuse, unauthorized disclosure, alteration, or destruction. For full details, see Question 30 (Security Policy) and Question 38 (Escrow).

Registrars must adhere to various information technology policies created to protect registrant data before obtaining accreditation for .ECO. Examples include password management protocols or standards for access to the registry system. See Question 30 (Security Policy).

In order to protect registrant’s data from unauthorized modification, domain transfers, and/or deletions, we will offer a registry lock service. See Question 23 (Registry Services).

The Registry will implement a privacy policy for inclusion in agreements with registrants, and/or users, and/or contractors. Key points include:

Personal Information will not be used for any other purpose without consent. The Registry will not transfer Personal Information to third parties, except for business partners who have agreed to comply with legally required privacy standards, and will use the information only for the purposes disclosed at the time of collection. The Registry may disclose Personal Information in some other limited circumstances, but will specifically describe them to registrants/users when we collect the information.

The Registry may disclose Personal Information to a third party without their consent if it has reason to believe that disclosing this information is necessary to identify, contact or bring legal action against someone who may be causing injury to or interference with (either intentionally or unintentionally) the Registry's rights or property, other registrants/users or anyone else that could be harmed. The Registry may also disclose Personal Information when we believe in good faith that such disclosure is required by and in accordance with the law.

The Registry will take technical, contractual, administrative, and physical security steps to protect Personal Information. We will implement procedures to ensure that Personal Information is only made available to designated staff to carry out the stated purposes communicated to registrants/users.

Registrants/users will have the right to access their Personal Information for verification. Upon receipt of a written request, the registry will provide them with a copy of their information.

VI. DESCRIBE WHETHER AND IN WHAT WAYS OUTREACH AND COMMUNICATIONS WILL HELP TO ACHIEVE YOUR PROJECTED BENEFITS

Communication and outreach will continue to play an important role in on-going engagement for .ECO registration, policy and accountability processes. Engagement on policy will ensure .ECO reflects the Community’s goals, which will drive registrations and active use of .ECO domains. Engagement on accountability will prevent misuse of .ECO.

Communication will emphasize that the .ECO Community TLD provides a meta-platform for trusted environmental data managed in the public interest by the Community, a way to identify Community members online, and the opportunity to make community-aligned choices based on reliable information. For Community members specifically, there will also be a focus on the opportunity to identify themselves via a .ECO domain, to share their actions in support of the environment, to participate in developing .ECO policies and suggest priorities for the .ECO foundation.

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

The .ECO Registry and Dot ECO Global Community Organization believe that the most critical negative consequence for consumers would be a .ECO TLD that does not reflect that the “eco” label is widely understood, both commonly and in regulatory guidance, to represent an association with the members of the environmental community as well as associated concepts and environmentally preferable products and services.

Consumer protection authorities around the world recognize the fact that the “eco” and “green” labels are powerful tools for consumer communication. Regulators agree that environment-related claims on products and services, including eco-, should only be used when qualifying information can be provided and/or the claim proven, including in the following policies: US Federal Trade Commission (FTC) Guides for the Use of Environmental Marketing Claims; UK Department for Environment Food and Rural Affairs (Defra) Green Claims Guidance and Advertising Standards Authority Codes; Environmental Claims: A Guide for Industry and Advertisers in Canada; Green marketing and the Australian Consumer Law; and, European Union Guidelines for Making and Assessing Environmental Claims.

The UN Guidelines for Consumer Protection are also designed to safeguard against false environmental claims. The UN pro consumer Guidelines are designed to protect consumers’ rights, especially those in developing countries, and to raise consumer awareness about the “environmental impact of products and services should be encouraged through such means as product profiles, environmental reports by industry, information centres for consumers, voluntary and transparent eco-labelling programmes and product information hotlines.”

Accordingly, the .ECO Community TLD will restrict .ECO domains to Community members and require registrants to complete and display a .ECO-profile. Without community restrictions and mandatory disclosures, a .ECO TLD could be construed as making environmental claims that would be impossible for consumers to verify.

In order to avoid consumer confusion, it is imperative that policy setting responsibility for the TLD be invested in a representative community member organization that can provide stable and ongoing environmental community input and oversight.

Furthermore, such policy oversight and guidance must be coupled with both pro-active and community-driven enforcement tools that will work to eliminate or minimize social costs arising from such confusion.

The .ECO Policy Consensus provides guidance on enforcement via an Accountability Policy, which will be implemented by the .ECO Registry, as part of any relevant contracts or relationships that the registry enacts. The .ECO Policy Consensus' Accountability Policy is as follows:

Accountability Policy:

The objective of this policy is to ensure that Registrants comply with the .ECO Purpose and Principles, and that the information provided in .ECO-profiles is of high quality, and is trustworthy and accurate.

.ECO-profiles: In order to use a .ECO domain name a Registrant must sign a registrant agreement that explains the actions they must take in support of the .ECO Purpose and Policies, including:

Updates: Registrants must review and/or update their .ECO-profiles at least annually. If they have not updated their .ECO-profile within a year's time, the Registry will remind them 30 and 10 days prior to the mandatory review date. Domains with .ECO-profiles that still have not been reviewed or updated after 12 months following this reminder will be subject to takedown proceedings.

Cross-referencing: Anywhere that .ECO (or Dot Eco) is mentioned and/or the .ECO logo is displayed on a Registrant's website or materials, that Registrant's corresponding .ECO-profile URL must also be displayed (as a footnote or hyperlink) so that the .ECO logo cannot be used without direct reference to the Registrant's .ECO-profile.

Registration Questions: Registrants must complete all mandatory .ECO-profile questions.

Independently Verified Information: Registrants can indicate whether or not the information in their .ECO-profile has been independently verified and if so, the verifier and the validity or expiry dates.

Reviews: The Registry will develop a set of review guidelines that will maximize .ECO System accuracy. A report on the review process and results will be submitted annually to the Organization by the Registry.

Complaints: Every .ECO-profile will have a "report abuse" link where a complaint can be submitted about that Registrant to the Registry. The Registry, or an approved dispute resolution provider contracted by the Registry, will evaluate complaints against the Registrant Agreement and decide whether and how to take action. The Organization will receive regular reports of all complaints received. In cases where there is not a clear resolution to the complaint in the view of the Registrant, Registry, or the Organization, the case may be referred to a dispute resolution process. The Registry, in keeping with the Principles of Improvement and Inclusiveness, will work with the affected Registrant through the dispute resolution process with the aim of reaching a mutually agreeable solution on behalf of the Community. In cases where complaints are not addressed to the satisfaction of the Registry and the Organization, the Registrant's domain name may be suspended or taken down. The Registry will document receipt of a response to all such complaints.

Complaints submitted by Registrants, who will have been verified as Community members, will be given higher priority than those from the general public. The Registry will also consider the number and nature of complaints received about a given Registrant when considering suspension or take-down measures.

Dispute Resolution Process: Complaints will first be addressed between the Registry, or a dispute resolution party contracted by the Registry, and the relevant Registrant. If a Registrant is dissatisfied with the decision, they may pay a fee to seek the recommendation of an independent mediator or arbiter approved by the Registry. If the Registry is dissatisfied with the recommendation of the independent mediator or arbiter, the Registry may choose to refer the dispute to the Organization for a final decision.

Comments on .ECO-Profiles: Every .ECO-profile will have a public comment forum. The registrant whose .ECO domain name is associated with an .ECO-profile will have the right to moderate comments on their profile. Registrants may also post comments about .ECO-profiles to relevant platform name pages.

The Registry will establish and regularly review a set of recommended moderation and commenting guidelines for registrants. The guidelines will include a way for Registrants to handle malicious comments.

Community Comment Forum: The Registry will implement a community forum where community members can interact with each other, the Registry, and the Organization, consistent with the community purpose of .ECO.

Take Down Process: Registrants that are found to be in breach of the .ECO Registrant Agreement, and therefore the purpose and policies of .ECO will be notified by email and given 60 days to come into compliance or opt for dispute resolution with the Registry. If this is not done, the .ECO domain name in question will be suspended for 60 days. If compliance is still not achieved, the domain will be taken down by the Registry.

Transparency: The Registry’s process for evaluating and resolving complaints and the results of disputes will be made public. The Registry will make public an annual report to the Organization summarizing its actions regarding this policy to ensure alignment with the purpose and principles of the .ECO Community TLD.

Please see response to Question 28 for additional abuse prevention and mitigation measures. These functions are resourced by Big Room and its partners or third-parties as appropriate.

I. HOW WILL MULTIPLE APPLICATIONS FOR A PARTICULAR DOMAIN NAME BE RESOLVED, FOR EXAMPLE, BY AUCTION OR ON A FIRST-COME/FIRST-SERVE BASIS?

The Registry will try to provide a fair opportunity for Community members to register for .ECO while also minimizing related costs to rights holders. We will hold three registration phases with specific allocation rules, as outlined below:

Phase 1 – Rights Holders & Community:

The first phase will run for a limited time period prior to the Land-rush and General Availability phases. In the past, Sunrise periods have been used in the launch of numerous TLDs including .INFO, .BIZ, .MOBI, .TEL, .ME, .XXX and others. These efforts have proven the need for a balanced approach that provides intellectual property (IP) holders an opportunity to register names they feel apply to their IP.

Big Room will hold a Sunrise period where holders of internationally recognized filed trademarks or possibly holders of existing (legacy) gTLD strings that are a perfect match to the .ECO string that they are applying for, will have the opportunity to apply for registration. A qualified third party must verify each trademark and/or legacy gTLD. In addition, the applicant must have a completed .ECO-profile and meet all criteria in order to be accepted as a Community member. No application will be accepted without these verifications.

Big Room plans to use the Trademark Clearinghouse to periodically check Sunrise applications against registered trademarks. If the trademark is verified and valid, we expect to be able to inform the IP holder that a Sunrise application for their string has been submitted. IP holders are only involved if an application is submitted that is an exact match to their registered trademark.

An auction process will determine the awarding party in the event that there is more than one valid Sunrise application for a given string.

Community-priority and Platform Names

1. Premium Names, including those that could have added community value, in two categories:

a) Community-priority: Prior to launch, the Organization will approve a list of community-priority names. The Registry will, with Organization input, develop rules for a best-use plan competition. Names allocated in the competition will be donated to the winners for a defined term. All community-priority names will be reviewed every two years by the Registry against their use-plans.

b) Auction-able: The Registry will also publish a list of names available for auction during sunrise. Funds generated from these names will be used to support the Registry.

2. Platform Names: The Registry will reserve a list of names that may be useful to the .ECO System, such as: industry sectors (eg, transportation); environmental issues (eg, biodiversity); nouns with environmental significance (eg, water); and, other names deemed technically useful to the Registry's implementation of .ECO as a community TLD (eg, council).

Phase 2 - Land Rush:

The second phase aims to reduce costs for registrants by minimizing speculation in the secondary market. It will run during a predetermined time period preceding the General Availability phase. During this period, applications will be accepted for any non-IP related strings. An auction will determine the awarding party should multiple applications be submitted for the same name. Registration restrictions to qualified .ECO members still apply.

Phase 3 - General Availability:

Phases 1 and 2 act to minimize the costs to potential registrants and provide a fair opportunity for registration. The third and final General Availability phase opens the .ECO Registry to live registrations on a first come, first served basis. Registration restrictions to qualified .ECO members still apply.

II. EXPLAIN ANY COST BENEFITS FOR REGISTRANTS YOU INTEND TO IMPLEMENT (EG, ADVANTAGEOUS PRICING, INTRODUCTORY DISCOUNTS, BULK REGISTRATION DISCOUNTS).

Specific discounts will be agreed upon with consultation and input from Community member alliances and entities. Members of these entities may receive discounts on .ECO domain names. For example, an agreement with an international environmental membership organization that allows its members to receive discounts on .ECO domains.

Registrants who register through .ECO Community members that have been through a verification process may also receive discounts. For example, certified B Corporation companies could obtain a discount on .ECO domain names.

Discounts may also be offered for business reasons to encourage growth in the number of active .ECO domain names; as a method of raising awareness or funding certain environmental campaigns and/or causes; and/or in periodic promotions to encourage innovative and creative use of .ECO domain names in support of the environment.

III. NOTE THAT THE REGISTRY AGREEMENT REQUIRES THAT REGISTRARS BE OFFERED THE OPTION TO OBTAIN INITIAL DOMAIN NAME REGISTRATIONS FOR PERIODS OF ONE TO TEN YEARS AT THE DISCRETION OF THE REGISTRAR, BUT NO GREATER THAN TEN YEARS. ADDITIONALLY, THE REGISTRY AGREEMENT REQUIRES ADVANCE WRITTEN NOTICE OF PRICE INCREASES. DO YOU INTEND TO MAKE CONTRACTUAL COMMITMENTS TO REGISTRANTS REGARDING THE MAGNITUDE OF PRICE ESCALATION? IF SO, PLEASE DESCRIBE YOUR PLANS.

The Community market will determine the viability of .ECO pricing. The Registry intends to maintain the freedom to set pricing first, based on costs and demand, in accordance with guidance from the Community, and in agreement with any ICANN and/or Registry Agreement criteria.

Big Room does not plan to make specific contractual price escalation commitments to our registrants. Any changes in pricing will be aligned with the mission⁄purpose of the .ECO Community TLD, will take the environmental community into account, and will be determined with input and consultation from the .ECO Organization.

Community-based Designation

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

Yes

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

The Global Environmental Community (the Community) – which the applicant Big Room Inc. commits to serve as the .ECO registry operator – is multi-stakeholder in nature, comprising individuals and entities (not-for-profit, business and government) that have come together for over 60 years through a variety of international alliances dedicated to the respectful, responsible and sustainable use of the environment.

In keeping with this tradition and in response to ICANN’s new gTLD program, the Community has established an alliance with the goal of creating and operating .ECO in the public interest and in keeping with the Community’s values.

The alliance formed in March 2009 by establishing a terms of reference for the .ECO Community Council. In September 2010 the stakeholders unanimously adopted a policy consensus for .ECO, including the purpose, principles and policies. In April 2012, council members formed the Dot ECO Global Community Organization (the Organization) to formally represent the Community in relation to .ECO. The Organization has signed an agreement with Big Room to apply to act as the registry operator of the .ECO Community TLD. The agreement was the result of 3 years of independently mediated discussion amongst the international council of Community members.

The Organization represents the majority of the Community including over 50 leading environmental groups from around the globe.

HOW THE COMMUNITY IS DELINEATED

Members of the Community are delineated from Internet users generally by community-recognized memberships, accreditations, registrations, and certifications that demonstrate active commitment, practice and reporting.

Community members include:

Relevant not-for-profit environmental organizations (ie, accredited by relevant United Nations (UN) bodies; International Union for Conservation of Nature (IUCN) member; proof of not-for-profit legal entity status with documented environmental mission).

Businesses (ie, members of environmental organizations; UN Global Compact participants; hold internationally-recognized environmental certifications; report to a global sustainability standard).

Government agencies with environmental missions (ie, UN bodies, national/sub-national government agencies with environmental responsibilities).

Individuals (ie, members of environmental organizations; academics; certified environmental professionals).

HOW THE COMMUNITY IS STRUCTURED AND ORGANIZED

The Community has historically structured and organized itself and its work through an international network of organizations, including millions of individual members with strongly aligned goals, values and interests. As well as collaborating via long-standing international multi-stakeholder fora and membership organizations, members traditionally organize through multi-organization alliances around specific events, geographies, and issues. The approach of forming alliances parallels the Internet community's method of designing solutions for issues of interest, most notably the Internet Governance Forum Dynamic Coalitions and Internet Engineering Task Force Birds-Of-a-Feather sessions. The alliance supporting this application embodies this organizing tradition.

Examples include:

International multi-stakeholder fora, eg, UN Environment Programme

Membership organizations, eg, WWF,Greenpeace and Friends of the Earth (FOE), the largest environmental membership organizations in the world, collectively representing 10 million individual members

Event-focused alliances, eg, TckTckTck, an alliance of 300 organizations formed to work for a fair, binding treaty at the 2010 Copenhagen climate summit

Geography-specific groups, eg, The Northern Alliance for Sustainability (ANPED), brings together not-for-profit organizations from the Northern hemisphere to create and protect sustainable communities

Issue-specific alliances, eg, 350.org, a grassroots organization working in over 188 countries to solve the climate crisis

WHEN THE COMMUNITY WAS ESTABLISHED

1948: First formal Community institution, the International Union for Conservation of Nature (IUCN), was established. Not-for-profit organizations, businesses and governments came together to address pressing environmental challenges.

1972: Global Environmental Community recognized by the world's governments on creation of the UN Environment Programme (UNEP), the UN's designated authority for addressing environmental issues at the global and regional level.

COMMUNITY ACTIVITES TO DATE

Some key global historical events:

International Organizations Established – IUCN (1948); World Wildlife Fund International (WWF) (1961); Friends of the Earth International (FOE), Greenpeace International (Greenpeace) (1971); UNEP (1972)

UN Global Summits – organizations, businesses and governments participate in global environmental events: UN Conference on the Human Environment (1972); Rio UN Conference on Environment and Development ("Earth Summit") (1992); Johannesburg World Summit on Sustainable Development (2002); Rio + 20 UN Conference on Sustainable Development (2012)

Organizations/UN collaborate on Global Conservation – "The World Conservation Strategy" by IUCN, UNEP, and WWF (1980); "World Charter for Nature" by IUCN adopted by UN (1982);

“Caring for the Earth” by IUCN, UNEP, and WWF (1991)

Binding International Legal Conventions – Convention on Wetlands (Ramsar) (1971); Convention on International Trade in Endangered Species (1973); Convention on Biological Diversity (1992); UN Framework Convention on Climate Change (1994); Kyoto Protocol (1997)

Integration of Environmental, Economic & Social Issues – Concept of Sustainable Development is established in “Our Common Future” (1987); World Business Council for Sustainable Development (WBCSD) (1995); Millennium Development Goals (2000); UN Global Compact (2004)

Consumer Protection – 1st ecolabel, The Blue Angel, created by the German government (1978); UN amends “UN Guidelines for Consumer Protection” to include environmental issues (1999); US Federal Trade Commission issues “Green Guides” to prevent false environmental claims (1992, 1996, 1998, 2010 review)

ESTIMATED SIZE OF THE COMMUNITY

The Community’s considerable size, longevity and enduring importance are evidenced by the nature and global range of its alliances of millions of individuals and entities, the variety of multi-stakeholder processes, the number of green businesses, and continuous global intergovernmental engagement.

Estimated Membership

40,000+ Not-for-Profit Organizations, eg, 34,376 US environmental organizations (2011 Internal Revenue Service Exempt Organizations Business Master File, National Center for Charitable Statistics); 6,157 in the UK (March 2012, 1/3 of 18,470 Environment / Conservation / Heritage registered charities, Charity Commission);

148,000+ Businesses, eg, 68,200 US businesses committed to environmental sustainability (Pew Charitable Trust, “The Clean Energy Economy”, 2009); 80,000 small and medium enterprises in the EU use certified environmental management systems (Danish Technological Institute, “SMEs and the Environment in the European Union”, 2010);

193+ Environment-focused Governmental Bodies – eg, 193 member states (UN website, March 2012);

18 million+ Individuals, eg, International: WWF, 5M; Greenpeace, 2.8M; FOE, 2M; Ocean Conservancy, 0.5M. National: National Wildlife Federation, 4M; Sierra Club, 1.4M; National Resources Defense Council, 1.2M; The Nature Conservancy, 1M (Members, 2010).

Estimated Geographic Extent

Membership Organization Offices: WWF (62 countries & presence in 100); Greenpeace (28 countries & presence in 40); FOE (77 national groups, 13 affiliates); IUCN Membership (101 international, 875 national organizations; 89 states; 124 government agencies);

UNEP Governing Council: 58 elected UN member seats; UNEP accredited organizations from 75 countries.

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

RELATIONS TO COMMUNITY ORGANIZATIONS

All the major international membership organizations (IUCN, WWF, Greenpeace, Friends of the Earth), the biggest global business and environment organizations (World Business Council for Sustainable Development (WBCSD), Green Economy Coalition), the largest international Community alliances (350.org, TckTckTck) and the key global environmental reporting standards (Global Reporting Initiative, Carbon Disclosure Project) support the creation of .ECO as a Community TLD. The United Nations Environment Programme (UNEP) has been an observer to the .ECO community process since 2010.

As the world’s largest and longest established organizations and alliances, these institutions represent over 190 countries, 1,000 entities, and more than 10 million individual members.

Organizations supporting the .ECO community-led approach:

Intergovernmental:
UN Environment Programme, UN Global Compact

International:
350.org, Amazon Watch, ANPED, BirdLife International, B Lab, Carbon Disclosure Project, Care2, Conservation International, DEKRA, Fauna & Flora International, Friends of the Earth International, Global Campaign for Climate Action (TckTckTck), Global Environmental Institute, Global Footprint Network, Global Reporting Initiative (GRI), Green Belt Movement International, Green Cross International, Green Economy Coalition, GreenTV, Greenpeace, Greenseal, International Centre for Trade and Sustainable Development, International Institute for Sustainable Development, IPAM Instituto de Pesquisa Ambiental da Amazônia, ISEAL, IUCN, Ocean Conservancy, People 4 Earth, Rainforest Action Network, Rare Conservation, UL Environment, UNEP/Wuppertal Institute Collaborating Centre, Verite, WBCSD, Wildlife Friendly Enterprise Network, WWF

National:
Akatu Institute, Canadian Parks and Wilderness Society, chinadialogue, David Suzuki Foundation, Development Alternatives, Dogwood Initiative, Ecojustice, Ecotrust Australia, Ecotrust Canada, Ecotrust US, Friends of Nature, Friends of the Earth Canada, Green America, Institute for Public and Environmental Affairs, Instituto Ethos, Pembina Institute, Project Dirt, Smart Approved Watermark, The Big Wild, YPB / LEAD Indonesia

The application explicitly addresses members active at the international level, while national-level members are implicitly addressed due to their more limited focus.

Support of .ECO continues to grow and will extend into the gTLD application review period. A current list of supporters can be found at www.doteco.org.

RELATIONS TO THE COMMUNITY AND ITS CONSTITUENT PARTS

Dot ECO Global Community Organization

Consistent with the Community’s history of organizing alliances around issues, leading members of the Community established the Dot ECO Global Community Organization (the Organization), an independent not-for-profit organization, as the representative membership institution for on-going .ECO policy development.

The Organization’s founding board comprises individuals from not-for-profit organizations involved in .ECO policy development since 2009 via the .ECO Community Council, and includes members from Brazil, France, India, Switzerland, the UK, and the US. The International Institute for Sustainable Development (IISD), founded in 1990 as a non-partisan charitable organization focused on sustainable development, acts as the secretariat for the Organization.

The 13 .ECO Community Council member organizations form the inaugural Community Council of the Organization to provide policy advice to the board: WWF International (Co-chair); Akatu Institute (Co-chair); B Lab; Conservation International; David Suzuki Foundation; Development Alternatives; Green Belt Movement International; Green Cross International; GreenTV; Greenpeace International; The ISEAL Alliance; UL Environment, and Verite. UNEP has been an observer to the Council since 2010 and in March 2012, the UN Department of Economic and Social Affairs Division for Sustainable Development indicated its interest to act as an observer.

The Organization has signed a contract for Big Room, a certified B Corporation, to apply for and act as the Registry operator for the .ECO Community TLD.

Information about the Organization background, establishment, governance and contract with Big Room is attached in 20f (20f-ECO-community-organization.pdf).

In line with the Community’s principles, Big Room’s founders, board members, investors, advisors, and observers have decades of combined environmental experience. The company is funded by a diverse group of mission-aligned leading environmental and social investors, including lead investor Working Enterprises, which has committed to donating its proceeds from .ECO to charity.

Big Room’s core business is in enhancing accountability in the green marketplace. Since 2008 it has operated Ecolabel Index (ecolabelindex.com), the authoritative global directory of environmental certifications. The site enables transparency and disclosure in the certification industry. A recognized authority on certification systems in green purchasing and supply chains, Big Room has provided advisory services to the General Services Administration of the US government, UNEP, the Sustainability Consortium, the Green Products Roundtable, and others.

Big Room was founded by Trevor Bowden, Jacob Malthouse and Dr. Anastasia O’Rourke. Trevor and Jacob previously worked at UNEP, where they launched the UN Principles for Responsible Investment. Trevor has also consulted to international banks on environmental risk. Jacob was previously Liaison to the Caribbean and Canada at ICANN. Anastasia is a leading environmental researcher, authoring over 20 reports, articles and whitepapers and has worked with INSEAD Business School, Yale University, The Carbon Trust, and the City of Sydney.

The co-founders also have environmental academic expertise: Trevor holds an MSc in Public Understanding of Environmental Change, University College London and a Diploma in Environmental Studies, McGill University; Jacob has a BA in Geography and Economics, University of Victoria; and, Anastasia holds a PhD, Yale School of Forestry and Environmental Studies and an MSc in Environmental Management and Policy, Lund University.

Big Room’s Advisory Board members include: Ashok Khosla, President, IUCN; James Gustave Speth, former Dean, Yale School of Forestry and Environmental Studies; William Nitze, former Assistant Administrator International Activities, US Environmental Protection Agency; and, Bill Knight, founding Commissioner, Financial Consumer Agency of Canada.

ACCOUNTABILITY MECHANISMS TO THE COMMUNITY

Accountability is a core principle of the .ECO Community TLD as evidenced by the multi-stakeholder process undertaken (see 20c) to develop community-driven principles and policies and to establish an independent governance structure for Community oversight of .ECO.

The Accountability Policy that forms part of the .ECO Policy Consensus includes guidelines to ensure registrants comply with the .ECO purpose and principles, and that information provided in .ECO-profiles is trustworthy and accurate. The Registry will conduct ‘spot-checks’ by reviewing a percentage of .ECO-profiles to ensure compliance.

Under the Organization’s contract with Big Room, the parties have established mutual non-voting observer board seats and defined the specific roles and responsibilities with regard to managing the .ECO Community TLD according to the .ECO Policy Consensus.

Community members can participate directly in the governance of .ECO through the Organization. Membership is free and open to all members of the Community. Entity members may apply to become voting members after two years of membership.

Big Room is committed to open, transparent multi-stakeholder engagement. It reports annually on its own environmental, social and economic impacts and requires suppliers to adopt eco-practices.

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

The .ECO Community TLD will create a global trusted source of environmental information, the .ECO System, to support the goals of the Global Environmental Community.

The December 2011 UNEP Eye on Earth Declaration vision whereby “decision-making for sustainable development is empowered by the availability and equitable accessibility of credible, relevant and timely information”, and that “effective mechanisms for the collection, management and dissemination of environmental information are needed.” The .ECO System also supports Principle 10 of the 1992 Rio Declaration on Environment and Development that states “Environmental issues are best handled with participation of all concerned citizens, at the relevant level.”

In the .ECO System, all registered .ECO domains will be linked to a separate web-based profile information system of .ECO-profiles that contain key environmental data in a user-friendly format. Together, .ECO domains and .ECO-profiles will form a new global aggregator of environmental information that includes controls and incentives to maintain the quality of information, while ensuring open access and freedom to innovate.

The purpose of the .ECO System per the .ECO Policy Consensus is to:

1. Allow members to more easily identify themselves and other Community members online and to prevent misuse of .ECO domain names that could lead to confusion;

2. Utilize the power of the Internet to foster transparency, information sharing, communication and exchange of ideas to promote environmental goals, interests and values, amongst community members and those who are exploring that opportunity; and,

3. Provide a platform for accurate and non-deceptive information and reliable resources to encourage environmental awareness and action.

INTENDED REGISTRANTS

Community members can become .ECO Registrants in the following categories: not-for-profit organizations, businesses, governments, individuals, and products. By completing their ECO-profile, Registrants can demonstrate their Community credentials (memberships, accreditations, certifications, and reporting). It will allow those wishing to join the Community to see the activities of current members, and facilitate interaction with eco-minded consumers.

INTENDED END-USERS

The intended end-user of the .ECO System is anyone interested in environmental data from the online trusted source created by millions of Community members. The .ECO System will provide accurate, reliable, and timely information about individuals, organizations, businesses and products to Community members, consumers, and others looking for environmental information. As a platform for innovation, members will foster transparency and consumer education by developing new ways to track, rank and display relevant information.

ACTIVITIES CARRIED OUT IN SERVICE OF THE .ECO PURPOSE

To establish the policies for .ECO, Meridian Institute (Meridian) mediated an international, transparent, and inclusive multi-stakeholder process, in compliance with the ISEAL Alliance Code of Good Practice for Setting Environmental and Social Standards, with members of the Global Environmental Community. Meridian is an independent, non-governmental, non-profit organization that is internationally recognized and trusted for designing and facilitating neutral consensus-building and problem-solving processes.

Global Multi-stakeholder Process

1. Creation of the .ECO Community Council (the Council)

At the request of Big Room, Meridian convened a council of community organizations, governed by a terms of reference (ToR) agreed by the members, to review and consider the results of a series of global consultations and to come to consensus on the purpose, principles, and policies for submission to ICANN on behalf of the Community. The ToR under which participants engaged confirmed that involvement was on a voluntary basis and without compensation or obligation to support Big Room’s application.

2. A Global Multi-Stakeholder Consultation with the Community

Big Room held 7 regional in-person consultations about the potential for .ECO to exist as a community TLD and to gather feedback on the purpose, principles and policies that should apply to the operation of a TLD purporting to be “pro environment.” Meetings were held in Canada, Australia, Sweden, Germany, Brazil, South Africa, the US from May to November 2009, on the margins of established international meetings/conferences where Community members were in attendance. The consultation process included public comment periods, town-hall meetings, open letters, bilateral communications, and global social and print media outreach.

3. An Extensive Public Campaign to Raise Awareness and Support

Working with the Council, Big Room posted at www.doteco.info drafts of all versions of the policies as they became available, and solicited Community input including 3 public comment periods from May 2009 to September 2010 of no less than 30 days each. In April 2010, the Council publicly announced its goal to develop a .ECO Policy Consensus by releasing an open letter to the Community by press release, posting to www.doteco.info, and delivery by Meridian to a number of community organizations.

Results of the Process

1. An agreement by the Council on the .ECO Policy Consensus, that defines the purpose, principles and policies for operation of the .ECO Community TLD.

2. The creation of an independent community-led organization, the Dot ECO Global Community Organization to act as the representative community member institution for .ECO and to provide on-going policy formulation, guidance, and advice to the Registry operator on behalf of the Community.

3. A contract between the Organization and Big Room defining their respective roles and procedures.

4. Support for the .ECO Community TLD application from over 50 environmental groups representing more than 10 million individual members and over 1,000 entities across 190 countries.

HOW THE PURPOSE AND PRINCIPLES ARE OF A LASTING NATURE

The over-arching purpose of the .ECO Community TLD is to support the goals, values and interests of the Global Environmental Community through increased transparency and awareness. The prevention of misuse of .ECO domain names that could lead to consumer confusion is a critical aspect of the .ECO mission. The Community’s goals are inherently of a lasting nature as it works, in the words of the Declaration of the 1972 UN Conference on the Human Environment “to defend and improve the human environment for present and future generations.” The importance of the consumer protection component of the Community’s work is recognized by many governments and organizations that have established standards for use of “green” or environmentally-friendly labelling.

Governance

The long-standing reliance on the multi-stakeholder model to pursue Community goals is reflected in the Dot ECO Global Community Organization. Its governance structure provides a community-led membership framework to manage .ECO for the long-term benefit of the Community including the opportunity to discuss and participate in the development and modification of .ECO policies and practices. The International Institute for Sustainable Development acts as secretariat for the Organization. On-going funding will be by the Registry. The Organization is linked to the Registry by a contract that defines the relationship between both parties and with ICANN.

Foundation

Per the .ECO Policy Consensus, a portion of sales from .ECO domain names will be donated to an independent foundation to support the Community’s goals, with a focus on building capacity in developing countries. The Organization and the Registry Operator will review the funding arrangement every 2 years, and publish annual financial reports to ensure transparency of funds allocated.

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

RELATIONSHIP TO THE ESTABLISHED NAME OF THE COMMUNITY AND TO THE IDENTIFICATION OF COMMUNTY MEMBERS

The term “eco” has long been used to identify members of the Global Environmental Community (the Community), as well as concepts, products and services associated with the Community’s goal of a respectful, responsible and sustainable use of the environment. The term appears in common usage and is clearly associated by consumers with environmentally responsible practices.

The Oxford English Dictionary (OED) offers the following examples:

Individuals and organizations (eg, eco-activist, eco-charities, eco-group)

Concepts (eg, eco-advocacy, eco-activism, eco-justice, eco-cultural, eco-historical, eco-literacy, eco-philosophy, eco-minded, eco-savvy, eco-awareness, eco-consciousness)

Products and services (eg, eco-product, eco-label, eco-house, eco-holiday, eco-resort, eco-bottle, eco-bulb, eco-forestry, eco-car)

(Oxford English Dictionary, 3rd edition, Mar. 2008; online version Sept. 2011)

Eco in Consumer Protection Public Policy

Consumer protection authorities around the world recognize the fact that the “eco” and “green” labels are powerful tools for consumer communication. Regulators agree that environment-related claims on products and services, including eco-, should only be used when qualifying information can be provided and/or the claim proven, including in the following policies: US Federal Trade Commission (FTC) Guides for the Use of Environmental Marketing Claims; UK Department for Environment Food and Rural Affairs (Defra) Green Claims Guidance & Advertising Standards Authority Codes; Environmental Claims: A Guide for Industry and Advertisers in Canada; Green Marketing & the Australian Consumer Law; and, European Union Guidelines for Making and Assessing Environmental Claims.

The UN Guidelines for Consumer Protection are also designed to safeguard against false environmental claims. The UN pro-consumer Guidelines are designed to protect consumers’ rights, especially those in developing countries, and to raise consumer awareness about the environmental impact of products and services “through such means as product profiles, environmental reports by industry, information centres for consumers, voluntary and transparent eco-labelling programmes and product information hotlines.”

Accordingly, the .ECO Community TLD will restrict .ECO domains to Community members and require registrants to complete and display a .ECO-profile. Without community restrictions and mandatory disclosures, a .ECO TLD could be construed as making environmental claims that would be impossible for consumers to verify.

Government-sponsored Research

Recent government-sponsored studies in the US and UK on consumer understanding clearly demonstrate that “eco,” “earth,” “environmentally-friendly” and to a lesser extent, “green” are commonly used and widely recognized by consumers to convey environmentally responsible practices.

Studies in the UK paid for by Defra show 70% of respondents were very familiar or fairly familiar with the term eco-friendly, being “explicitly linked to environmental issues, but only in as much as they show a product or claim broadly relates to the environment.” (DEFRA, “An Assessment of Green Claims in Marketing”, 2010; Consumer Understanding of Green Terms, 2011.)

Studies conducted as part of a 2010 review by the US Federal Trade Commission (FTC) Green Guides also noted a convergence of green, and eco- / earth- / environmentally-friendly as the most common general environmental terms. (FTC, “Green Marketing Internet Surf”, 2008). The studies also confirm the potential for misuse of such terms: “unqualified claims that an item is ‘environmentally friendly’ or ‘eco-friendly’ are likely to convey that it has specific and far-reaching environmental benefits.”

Independent Research

In February 2012, Vision Critical, on behalf of Big Room, conducted a survey to understand public perception around the term eco and of the .ECO TLD in general.

The majority of respondents (58%) indicated they would expect domain names ending in .ECO (eg, anyname.eco) to be members of an environmental organization, professional association or have made a specific commitment to the environment. Only 10% indicated they would not expect an environmental connection, while 32% said they did not know. Two-thirds (67%) of respondents also indicated that they would expect a website that had a domain name ending in .ECO to contain environmental/ecological related information. Half (51%) said they would be, and 25% said they might be confused by a .ECO TLD not associated with the Community.

The survey was a random online Omnibus survey of 1,016 US adults from diverse ages, incomes, ethnicities and regions, conducted 15-16 February 2012 among a sample of Americans who are also Springboard America panel members. The margin of error, which measures sampling variability, is +/-3.10%, 19 times out of 20. The sample was balanced by age, gender and region according to the most recent American Community Survey (2009).

Academic References

The OED defines the prefix eco- as a shortened form of ecology (noun) or ecological (adjective). When eco is used as stand-alone word, it is defined as shortened form of ecological (adjective), with the meaning environmentally friendly.

The OED lists over 30 words beginning with the prefix eco-, all of which relate to combined form adjectives with the sense “ecological and – –” or nouns with the sense “ecological –”. Throughout the over 70 years of documented use in the OED, eco has always been associated with ecology or ecological concepts, never as a shortened or combining form for words such as economy.

Support for a comparable use of “eco” in French is provided by Dr Pascaline Dury’s bilingual corpus-based study of the migration of vocabulary from scientific to non-scientific use. Of the 21 lexical units that appear in the study’s French news corpus, “all of them are semantically-related to the field of ecology and can be easily defined.” (Dury, P. “The rise of carbon neutral and compensation carbone”. Terminology 14(2): 236, 2008.)

POTENTIAL CONNOTATIONS BEYOND THE COMMUNITY

The OED identifies the potential for “greenwashing,” defined as “disinformation disseminated by an organisation, etc., so as to present an environmentally responsible public image; a public image of environmental responsibility promulgated by or for an organisation, etc., but perceived as being unfounded or intentionally misleading.” (BSR &Futerra, “Understanding and Preventing Greenwash: A Business Guide”, 2009.) Misuse of the “eco” label can negatively affect Community interests by making people skeptical of environmental initiatives and impeding consumers’ understanding of the impacts of their buying decisions.

While “eco” has no significant meaning other than as a short form for environment/ ecology, it infrequently occurs as an acronym. Known international acronyms and uses are:

European Communications Office (ECO): All European Conference of Postal and Telecommunications Administrators (CEPT) divisions are housed as part of the CEPT website (www.cept.org/eco). There is no confusion anticipated between this usage and the .ECO TLD.

Economic Cooperation Organisation (ECO): an intergovernmental regional group established by Iran, Pakistan and Turkey to promote economic cooperation in the region (www.ecosecretariat.org). As the focus is regional rather than global and on economic rather than environmental issues, there is no confusion anticipated between this usage and the .ECO TLD.

eco Association of the German Internet Industry: Confirmed in writing that it does not intend to apply for .ECO or object to Big Room’s .ECO application. See attached letter of non-objection in 20f (20d-eco-non-objection.pdf). There is no confusion anticipated between this usage and the .ECO TLD.

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

The policies developed by the .ECO Community Council form the .ECO policy consensus, a key result of the process discussed in 20c. Policies are also discussed in 18b. The Dot ECO Global Community Organization (the Organization) provides for continued community discussion and participation to develop and modify .ECO policies and practices.

The registry will prevent DNS resolution of .ECO names until the registrant submits information to support their compliance with the .ECO community eligibility requirements. Registrants will be required to satisfactorily complete their .ECO-profile, the central eligibility verification system. Provided that this step is completed, active DNS resolution will be enabled.

The registry will employ standard registration lifecycle mechanisms, statuses, and states such as HOLD or LOCK functions, or other existing Extensible Provisioning Protocol (EPP) commands, in order to disallow a domain to be active when a registrant is not in compliance with the community eligibility requirements or under related community dispute resolution procedures.

ELIGIBILITY

Eligibility is limited to individuals and entities (not-for-profit, business and government) that are members of the Global Environmental Community (the Community) that meet community-recognized standards:

1. Not-for-profit environmental organizations that affirm and can provide proof on request of:
A) Accreditation by relevant UN agencies (ie, UNEP, UN Economic and Social Council) or
B) Proof of legal establishment and environmental mission/purpose.

2. Business entities that affirm and can provide proof on request of:
A) Membership in environmental organizations and initiatives including:
i. Organizations as in 1 A)-B) or
ii. The United Nations Global Compact or
iii. Other memberships approved by the Organization

B) Accreditation by voluntary environmental certifications, standards and reporting systems of:
i. Organizations as in 1 A)-B) or
ii. UN member states, national and sub-national governmental bodies and entities or
iii. The International Organization for Standardization or
iv. Other certification, standards and reporting systems approved by the Organization

3. Governments, including environment-related departments and initiatives of UN member states, national and sub-national governmental bodies, and UN bodies

4. Individuals that affirm and can provide proof on request of membership, financial support for, or accreditation including:
A) Organizations as in 1 A)-B) or
B) Certified environmental professional qualifications approved by the Organization or
C) Academics/scientists affiliated with recognized universities

Registrants holding certain environmental certifications may qualify to register for .ECO domain names without providing additional details through a .ECO-Profile. The Organization will establish the required qualifications and agreements with certifiers to enable rapid, accurate validation. Certified registrants will be promoted as such within the .ECO System.

NAME SELECTION

Community-priority: Prior to launch, the Organization will approve a list of community-priority names and with the Registry, develop a best-use plan competition. Allocated names will be donated to the winners for a defined term. All community-priority names will be reviewed biennially by the Registry against their use plans (eg, Forest, Finance).

Platform Names: Registry will reserve a list of names that may be useful to the .ECO System like industry sectors, environmental issues, nouns with environmental significance and other names deemed useful to the Registry’s implementation of .ECO (eg, Council, Community) for allocation in a manner to be determined by the Organization.

Auction-able: Registry will publish a list of remaining names available for auction during sunrise. Funds generated from these names will be used to support the Registry and Organization.

CONTENT/USE

Registrants must comply with the .ECO Purpose and Principles and provide accurate information in their .ECO-profiles.

Applicants must complete a .ECO-profile that includes a series of mandatory and voluntary questions about commitments, memberships, certification, reporting and other activities undertaken in support of Community goals.

Responses will form a .ECO-profile webpage that will be added to a public online database called the .ECO System. Registrant .ECO-profiles will be linked to the registrant’s .ECO domain via a .ECO logo trust-mark.

The Organization will develop a process to establish, regularly review, and update the .ECO-profile Registrant questions.

The types of .ECO use will be not-for-profit, business, individual, government, and product.

Controversial Names: Organization will develop a method to flag controversial strings based on: existing public policy, community recommendations; industry sector and green-washing watch-lists; and research/surveys. Controversial names will not be automatically blocked but registrants selecting flagged names will be notified that registration will be subject to additional scrutiny.

.ECO-profiles: Registry, in consultation with Organization, will develop a set of review guidelines to maximize .ECO System accuracy and to ensure compliance with the .ECO eligibility requirements. Registry will report annually on review process and results to the Organization.

To use a .ECO domain name a registrant must sign a Registrant Agreement that explains the actions they will need to take in support of the .ECO purpose and policies.

Registrants must review and/or update their .ECO-profiles at least annually.
Non-compliant Registrants will be reminded by the Registry 30 and 10 days prior to the mandatory review date. Domain names with .ECO-profiles that remain non-compliant 12 months after the review date will be subject to takedown proceedings. This requirement further strengthens our rights protection and WHOIS accuracy mechanisms. See also Question 29.

Anywhere a registrant references .ECO (or Dot Eco) and/or the .ECO logo, the registrant’s corresponding Eco-profile URL must also be displayed (ie, as a footnote or hyperlink) as the .ECO logo must directly reference the registrant’s .ECO-profile.

Registrants must complete all mandatory .ECO-profile questions.

Registrants can indicate if the information in their .ECO-profile has been independently verified, and if so, include the verifier and validity/expiry dates.

ENFORCEMENT

Complaints: Every .ECO-profile will have a report abuse link where a complaint can be submitted about that registrant to the Registry. The Registry will evaluate complaints against the Registrant Agreement and decide whether and how to take action.

Where the registrant, Registry or Organization sees no clear resolution, the case may be referred to a dispute resolution process. The Registry, in keeping with the principles of improvement and inclusivity, will work with the registrant through the process to reach a mutually agreeable solution on behalf of the Community.

Where complaints are not addressed to the satisfaction of Registry and Organization, the registrant’s domain name may be suspended and/or taken down.

Complaints submitted by verified Community member registrants will be given priority over the general public. The Registry will review the number and nature of complaints about a registrant when considering suspension and take-down measures.

Dispute Resolution Process: Registry will support a Community Eligibility Dispute Resolution Process (CEDRP) aligned with the Accountability Policy described in the .ECO Policy Consensus. The CEDRP can be initiated by .ECO community member or the general public to address alleged violations of .ECO member policies or operating requirements by a registrant or registrar. Complaints will be first be addressed between the Registry, or a dispute resolution party contracted by the Registry, and the relevant Registrant. If not resolved to the satisfaction of the registrant, the registrant may pay a fee to seek the recommendation of an independent mediator or arbiter approved by the Registry. If not resolved to the satisfaction of the Registry, the Registry may choose to refer the dispute to the Organization for a final decision.

Comments on .ECO-profiles: .ECO-profiles are tools used to confirm Community membership and eligibility. Every .ECO-profile to have a public comment forum and the registrant whose .ECO domain name is associated with an .ECO-profile will have the right to moderate comments on their profile. Registrants may post comments about .ECO-profiles to relevant Platform Name pages. The Organization will establish and regularly review recommended moderation / commenting guidelines, including handling malicious comments.

Community Comment Forum: Registry will implement a .ECO community comment / debate forum for members to interact with each-other, the Registry and the Organization

Take-Down Process: For Registrants found to be in breach of the .ECO Registrant Agreement: receipt of a 60 day email notice to come into compliance and/or opt for dispute resolution, if no action, domain to be suspended for 60 days, if remains non-compliant, domain to be taken down by the Registry.

Transparency: Registry process for evaluating and resolving complaints and results of disputes will be made public. An Annual report of all complaints and actions taken will be made to the Organization.

Controversial Names: Registry mechanisms for community enforcement include: reporting controversial names, implementation of complaints, dispute resolution, takedown mechanisms per the Accountability Policy, and the right to take down names and sites that it or the Organization deem to be in breach of the .ECO Purpose and Registrant Agreement.

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.

Big Room Inc., the proposed .ECO registry operator, will protect names with national or geographic significance by reserving the country and territory names at the second level and at all other levels within the TLD, as per the requirements in the New TLD Registry Agreement (Specification 5, paragraph 5).

We will employ a series of rules to translate the geographical names required to be reserved by Specification 5, paragraph 5 to a form consistent with the ″host names″ format used in domain names.

Considering the Governmental Advisory Committee (GAC) advice “Principles regarding new gTLDs”, these domains will be blocked, at no cost to governments, public authorities, or Intergovernmental Organizations (IGOs), before the TLD is introduced (Sunrise), so that no parties may apply for them. We will publish a list of these names before Sunrise, so our registrars and their prospective applicants can be aware that these names are reserved.

We will define a procedure so that governments can request the above reserved domain(s) if they would like to take possession of them. This procedure will be based on existing methodology developed for the release of country names in the .INFO TLD, which is operated by Afilias, the registry services provider for the .ECO Community TLD. For example, we will require a written request from the country’s GAC representative, or a written request from the country’s relevant Ministry or Department. We will allow the designated beneficiary (the Registrant) to register the name, with an accredited .ECO Registrar, possibly using an authorization number transmitted directly to the designated beneficiary in the country concerned.

As defined by Specification 5, paragraph 5, such geographic domains may be released to the extent that Registry Operator reaches agreement with the applicable government(s). Registry operator will work with respective GAC representatives of the country’s relevant Ministry or Department to obtain their release of the names to the Registry Operator.

If internationalized domains names (IDNs) are introduced in the .ECO TLD in the future, we will also reserve the IDN versions of the country names in the relevant script(s) before IDNs become available to the public. If we find it advisable and practical, we will confer with relevant language authorities so that we can reserve the IDN domains properly along with their variants.

Regarding GAC advice regarding second-level domains not specified via Specification 5, paragraph 5, all domains awarded to registrants are subject to the Uniform Domain Name Dispute Resolution Policy (UDRP), and to any properly-situated court proceeding.

We will ensure appropriate procedures to allow governments, public authorities or IGOs to challenge abuses of names with national or geographic significance at the second level. In its registry-registrar agreement, and flowing down to registrar-registrant agreements, the registry operator will institute a provision to suspend domains names in the event of a dispute. We may exercise that right in the case of a dispute over a geographic name.

Registry Services

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

Throughout the technical portion (#23 - #44) of this application, answers are provided directly from Afilias, the back-end provider of registry services for the .ECO Community TLD. Big Room chose Afilias as its back-end provider for .ECO because Afilias has more experience successfully applying to ICANN and launching new TLDs than any other provider. Afilias is the ICANN-contracted registry operator of the .INFO and .MOBI TLDs, and Afilias is the back-end registry services provider for other ICANN TLDs including .ORG, .ASIA, .AERO, and .XXX.

Registry services for the .ECO Community TLD will be performed by Afilias in the same responsible manner used to support 16 top level domains today. Afilias supports more ICANN-contracted TLDs (6) than any other provider currently. Afilias' primary corporate mission is to deliver secure, stable and reliable registry services. The .ECO Community TLD will utilize an existing, proven team and platform for registry services with:

* A stable and secure, state-of-the-art, EPP-based SRS with ample storage capacity, data security provisions and scalability that is proven with registrars who account for over 95% of all gTLD domain name registration activity (over 375 registrars);
* A reliable, 100% available DNS service (zone file generation, publication and dissemination) tested to withstand severe DDoS attacks and dramatic growth in Internet use;
* A WHOIS service that is flexible and standards compliant, with search capabilities to address both registrar and end-user needs; includes consideration for evolving standards, such as RESTful, or draft-kucherawy-wierds;
* Experience introducing IDNs in the following languages: German (DE), Spanish (ES), Polish (PL), Swedish (SV), Danish (DA), Hungarian (HU), Icelandic (IS), Latvian (LV), Lithuanian (LT), Korean (KO), Simplified and Traditional Chinese (CN), Devanagari (HI-DEVA), Russian (RU), Belarusian (BE), Ukrainian (UK), Bosnian (BS), Serbian (SR), Macedonian (MK) and Bulgarian (BG) across the TLDs it serves;
* A registry platform that is both IPv6 and DNSSEC enabled;
* An experienced, respected team of professionals active in standards development of innovative services such as DNSSEC and IDN support;
* Methods to limit domain abuse, remove outdated and inaccurate data, and ensure the integrity of the SRS, and;
* Customer support and reporting capabilities to meet financial and administrative needs, e.g., 24x7 call center support, integration support, billing, and daily, weekly, and monthly reporting.

Afilias will support the .ECO Community TLD in accordance with the specific policies and procedures of Big Room (the “registry operator”), leveraging a proven registry infrastructure that is fully operational, staffed with professionals, massively provisioned, and immediately ready to launch and maintain the .ECO Community TLD.

The below response includes a description of the registry services to be provided for this TLD, additional services provided to support registry operations, and an overview of Afilias' approach to registry management.

REGISTRY SERVICES TO BE PROVIDED

To support the .ECO Community TLD, Big Room and Afilias will offer the following registry services, all in accordance with relevant technical standards and policies:
* Receipt of data from registrars concerning registration for domain names and nameservers, and provision to registrars of status information relating to the EPP-based domain services for registration, queries, updates, transfers, renewals, and other domain management functions. Please see our responses to questions #24, #25, and #27 for full details, which we request be incorporated here by reference.
* Operation of the registry DNS servers: The Afilias DNS system, run and managed by Afilias, is a massively provisioned DNS infrastructure that utilizes among the most sophisticated DNS architecture, hardware, software and redundant design created. Afilias' industry-leading system works in a seamless way to incorporate nameservers from any number of other secondary DNS service vendors. Please see our response to question #35 for full details, which we request be incorporated here by reference.
* Dissemination of TLD zone files: Afilias' distinctive architecture allows for real-time

updates and maximum stability for zone file generation, publication and dissemination. Please see our response to question #34 for full details, which we request be incorporated here by reference.
* Dissemination of contact or other information concerning domain registrations: A port 43 WHOIS service with basic and expanded search capabilities with requisite measures to prevent abuse. Please see our response to question #26 for full details, which we request be incorporated here by reference.
* Internationalized Domain Names (IDNs): Ability to support all protocol valid Unicode characters at every level of the TLD, including alphabetic, ideographic and right-to-left scripts, in conformance with the ICANN IDN Guidelines. Please see our response to question #44 for full details, which we request be incorporated here by reference.
* DNS Security Extensions (DNSSEC): A fully DNSSEC-enabled registry, with a stable and efficient means of signing and managing zones. This includes the ability to safeguard keys and manage keys completely. Please see our response to question #43 for full details, which we request be incorporated here by reference.

Each service will meet or exceed the contract service level agreement. All registry services for this TLD will be provided in a standards-compliant manner.

Security

Afilias addresses security in every significant aspect – physical, data and network as well as process. Afilias' approach to security permeates every aspect of the registry services provided. A dedicated security function exists within the company to continually identify existing and potential threats, and to put in place comprehensive mitigation plans for each identified threat. In addition, a rapid security response plan exists to respond comprehensively to unknown or unidentified threats. The specific threats and Afilias mitigation plans are defined in our response to question #30(b); please see that response for complete information. In short, Afilias is committed to ensuring the confidentiality, integrity, and availability of all information.

NEW REGISTRY SERVICES

No new registry services are planned for the launch of the .ECO Community TLD.

ADDITIONAL SERVICES TO SUPPORT REGISTRY OPERATION

Numerous supporting services and functions facilitate effective management of the TLD. These support services are also supported by Afilias, including:
* Customer support: 24x7 live phone and e-mail support for customers to address any access, update or other issues they may encounter. This includes assisting the customer identification of the problem as well as solving it. Customers include registrars and the registry operator, but not registrants except in unusual circumstances. Customers have access to a web-based portal for a rapid and transparent view of the status of pending issues.
* Financial services: billing and account reconciliation for all registry services according to pricing established in respective agreements.

Reporting is an important component of supporting registry operations. Afilias will provide reporting to the registry operator and registrars, and financial reporting.

Reporting provided to registry operator

Afilias provides an extensive suite of reports to the registry operator, including daily, weekly and monthly reports with data at the transaction level that enable the registry operator to track and reconcile at whatever level of detail preferred. Afilias provides the exact data required by ICANN in the required format to enable the registry operator to meet its technical reporting requirements to ICANN.

In addition, Afilias offers access to a data warehouse capability that will enable near real-time data to be available 24x7. This can be arranged by informing the Afilias Account Manager regarding who should have access. Afilias' data warehouse capability enables drill-down analytics all the way to the transaction level.

Reporting available to registrars

Afilias provides an extensive suite of reporting to registrars and has been doing so in an exemplary manner for more than ten years. Specifically, Afilias provides daily, weekly and monthly reports with detail at the transaction level to enable registrars to track and reconcile at whatever level of detail they prefer.

Reports are provided in standard formats, facilitating import for use by virtually any registrar analytical tool. Registrar reports are available for download via a secure administrative interface. A given registrar will only have access to its own reports. These include the following:
* Daily Reports: Transaction Report, Billable Transactions Report, and Transfer Reports;
* Weekly: Domain Status and Nameserver Report, Weekly Nameserver Report, Domains Hosted by Nameserver Weekly Report, and;
* Monthly: Billing Report and Monthly Expiring Domains Report.

Weekly registrar reports are maintained for each registrar for four weeks. Weekly reports older than four weeks will be archived for a period of six months, after which they will be deleted.

Financial reporting

Registrar account balances are updated real-time when payments and withdrawals are posted to the registrars' accounts. In addition, the registrar account balances are updated as and when they perform billable transactions at the registry level.

Afilias provides Deposit/Withdrawal Reports that are updated periodically to reflect payments received or credits and withdrawals posted to the registrar accounts.

The following reports are also available:

a) Daily Billable Transaction Report, containing details of all the billable transactions performed by all the registrars in the SRS,
b) daily e-mail reports containing the number of domains in the registry and a summary of the number and types of billable transactions performed by the registrars, and
c) registry operator versions of most registrar reports (for example, a daily Transfer Report that details all transfer activity between all of the registrars in the SRS).

AFILIAS APPROACH TO REGISTRY SUPPORT
Afilias, the back end registry services provider for this TLD, is dedicated to managing the technical operations and support of this TLD in a secure, stable and reliable manner. Afilias has worked closely with Big Room to review specific needs and objectives of this TLD. The resulting comprehensive plans are illustrated in technical responses #24-44, drafted by Afilias given Big Room's requirements. Afilias and Big Room also worked together to provide financial responses for this application which demonstrate cost and technology consistent with the size and objectives of the .ECO Community TLD.

Afilias is the registry services provider for this and several other TLD applications. Over the past 11 years of providing services for gTLD and ccTLDs, Afilias has accumulated experience about resourcing levels necessary to provide high quality services with conformance to strict service requirements. Afilias currently supports over 20 million domain names, spread across 16 TLDs, with over 400 accredited registrars.

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

With over a decade of registry experience, Afilias has the depth and breadth of experience that ensure existing and new needs are addressed, all while meeting or exceeding service level requirements and customer expectations. This is evident in Afilias’ participation in business, policy and technical organizations supporting registry and Internet technology within ICANN and related organizations. This allows Afilias to be at the forefront of security initiatives such as: DNSSEC, wherein Afilias worked with Public Interest Registry (PIR) to make the .ORG registry the first DNSSEC enabled gTLD and the largest TLD enabled at the time; in enhancing the Internet experience for users across the globe by leading development of IDNs; in pioneering the use of open-source technologies by its usage of PostgreSQL, and; being the first to offer near-real-time dissemination of DNS zone data.

The ability to observe tightening resources for critical functions and the capacity to add extra resources ahead of a threshold event are factors that Afilias is well versed in. Afilias’ human resources team, along with well-established relationships with external organizations, enables it to fill both long-term and short-term resource needs expediently.

Afilias’ growth from a few domains to serving 20 million domain names across 16 TLDs and 400 accredited registrars indicates that the relationship between the number of people required and the volume of domains supported is not linear. In other words, servicing 100 TLDs does not automatically require 6 times more staff than servicing 16 TLDs. Similarly, an increase in the number of domains under management does not require in a linear increase in resources. Afilias carefully tracks the relationship between resources deployed and domains to be serviced, and pro-actively reviews this metric in order to retain a safe margin of error. This enables Afilias to add, train and prepare new staff well in advance of the need, allowing consistent delivery of high quality services.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

NOTE: THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (LESS THAN / GREATER THAN CHARACTERS) (THE “ ” and “ ” CHARACTERS, or and), WHICH ICANN INFORMS US (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE ANSWER BELOW AS DISPLAYED IN TAS MAY NOT RENDER THE FULL RESPONSE AS INTENDED. THEREFORE, THE FULL ANSWER TO THIS QUESTION IS ALSO ATTACHED AS A PDF FILE (24-SRS-Performance.pdf), ACCORDING TO SPECIFIC GUIDANCE FROM ICANN UNDER CASE ID 11027.
====

Answers for this question (#24) are provided directly from Afilias, the back-end provider of registry services for the .ECO Community TLD.

Afilias operates a state-of-the-art EPP-based Shared Registration System (SRS) that is secure, stable and reliable. The SRS is a critical component of registry operations that must balance the business requirements for the registry and its customers, such as numerous domain acquisition and management functions. The SRS meets or exceeds all ICANN requirements given that Afilias:
* Operates a secure, stable and reliable SRS which updates in real-time and in full compliance with Specification 6 of the new gTLD Registry Agreement;
* Is committed to continuously enhancing our SRS to meet existing and future needs;
* Currently exceeds contractual requirements and will perform in compliance with

Specification 10 of the new gTLD Registry Agreement;
* Provides SRS functionality and staff, financial, and other resources to more than adequately meet the technical needs of the .ECO Community TLD, and;
* Manages the SRS with a team of experienced technical professionals who can seamlessly integrate this TLD into the Afilias registry platform and support the .ECO Community TLD in a secure, stable and reliable manner.

DESCRIPTION OF OPERATION OF THE SRS, INCLUDING DIAGRAMS

Afilias' SRS provides the same advanced functionality as that used in the .INFO and .ORG registries, as well as the fourteen other TLDs currently supported by Afilias. The Afilias registry system is standards-compliant and utilizes proven technology, ensuring global familiarity for registrars, and it is protected by our massively provisioned infrastructure that mitigates the risk of disaster.

EPP functionality is described fully in our response to question #25; please consider those answers incorporated here by reference. An abbreviated list of Afilias SRS functionality includes:
* Domain registration: Afilias provides registration of names in the TLD, in both ASCII and IDN forms, to accredited registrars via EPP and a web-based administration tool.
* Domain renewal: Afilias provides services that allow registrars the ability to renew domains under sponsorship at any time. Further, the registry performs the automated renewal of all domain names at the expiration of their term, and allows registrars to rescind automatic renewals within a specified number of days after the transaction for a full refund.
* Transfer: Afilias provides efficient and automated procedures to facilitate the transfer of sponsorship of a domain name between accredited registrars. Further, the registry enables bulk transfers of domains under the provisions of the Registry-Registrar Agreement.
* RGP and restoring deleted domain registrations: Afilias provides support for the Redemption Grace Period (RGP) as needed, enabling the restoration of deleted registrations.
* Other grace periods and conformance with ICANN guidelines: Afilias provides support for other grace periods that are evolving as standard practice inside the ICANN community. In addition, the Afilias registry system supports the evolving ICANN guidelines on IDNs.

Afilias also supports the basic check, delete, and modify commands.

As required for all new gTLDs, Afilias provides "thick" registry system functionality. In this model, all key contact details for each domain are stored in the registry. This allows better access to domain data and provides uniformity in storing the information.

Afilias' SRS complies today and will continue to comply with global best practices including relevant RFCs, ICANN requirements, and this TLD's respective domain policies. With over a decade of experience, Afilias has fully documented and tested policies and procedures, and our highly skilled team members are active participants of the major relevant technology and standards organizations, so ICANN can be assured that SRS performance and compliance are met. Full details regarding the SRS system and network architecture are provided in responses to questions #31 and #32; please consider those answers incorporated here by reference.

SRS servers and software

All applications and databases for this TLD will run in a virtual environment currently hosted by a cluster of servers equipped with the latest Intel Westmere multi-core processors. (It is possible that by the time this application is evaluated and systems deployed, Westmere processors may no longer be the "latest"; the Afilias policy is to use the most advanced, stable technology available at the time of deployment.) The data for the registry will be stored on storage arrays of solid state drives shared over a fast storage area network. The virtual environment allows the infrastructure to easily scale both vertically and horizontally to cater to changing demand. It also facilitates effective utilization of system resources, thus reducing energy consumption and carbon footprint.

The network firewalls, routers and switches support all applications and servers. Hardware traffic shapers are used to enforce an equitable access policy for connections coming from registrars. The registry system accommodates both IPv4 and IPv6 addresses. Hardware load balancers accelerate TLS/SSL handshaking and distribute load among a pool of application servers.

Each of the servers and network devices are equipped with redundant, hot-swappable components and multiple connections to ancillary systems. Additionally, 24x7 support agreements with a four-hour response time at all our data centers guarantee replacement of failed parts in the shortest time possible.

Examples of current system and network devices used are:
* Servers: Cisco UCS B230 blade servers
* SAN storage arrays: IBM Storwize V7000 with Solid State Drives
* SAN switches: Brocade 5100
* Firewalls: Cisco ASA 5585-X
* Load balancers: F5 Big-IP 6900
* Traffic shapers: Procera PacketLogic PL8720
* Routers: Juniper MX40 3D
* Network switches: Cisco Nexus 7010, Nexus 5548, Nexus 2232

These system components are upgraded and updated as required, and have usage and performance thresholds which trigger upgrade review points. In each data center, there is a minimum of two of each network component, a minimum of 25 servers, and a minimum of two storage arrays.

Technical components of the SRS include the following items, continually checked and upgraded as needed: SRS, WHOIS, web admin tool, DNS, DNS distributor, reporting, invoicing tools, and deferred revenue system (as needed).

All hardware is massively provisioned to ensure stability under all forecast volumes from launch through “normal” operations of average daily and peak capacities. Each and every system application, server, storage and network device is continuously monitored by the Afilias Network Operations Center for performance and availability. The data gathered is used by dynamic predictive analysis tools in real-time to raise alerts for unusual resource demands. Should any volumes exceed established thresholds, a capacity planning review is instituted which will address the need for additions well in advance of their actual need.

SRS DIAGRAM AND INTERCONNECTIVITY DESCRIPTION

As with all core registry services, the SRS is run from a global cluster of registry system data centers, located in geographic centers with high Internet bandwidth, power, redundancy and availability. All of the registry systems will be run in a n+1 setup, with a primary data center and a secondary data center. For detailed site information, please see our responses to questions #32 and #35. Registrars access the SRS in real-time using EPP.

A sample of the Afilias SRS technical and operational capabilities (displayed in Figure 24-a) include:
* Geographically diverse redundant registry systems;
* Load balancing implemented for all registry services (e.g. EPP, WHOIS, web admin) ensuring equal experience for all customers and easy horizontal scalability;
* Disaster Recovery Point objective for the registry is within one minute of the loss of the primary system;
* Detailed and tested contingency plan, in case of primary site failure, and;
* Daily reports, with secure access for confidentiality protection.

As evidenced in Figure 24-a, the SRS contains several components of the registry system. The interconnectivity ensures near-real-time distribution of the data throughout the registry infrastructure, timely backups, and up-to-date billing information.

The WHOIS servers are directly connected to the registry database and provide real-time responses to queries using the most up-to-date information present in the registry.

Committed DNS-related EPP objects in the database are made available to the DNS Distributor via a dedicated set of connections. The DNS Distributor extracts committed DNS-related EPP objects in real time and immediately inserts them into the zone for dissemination.

The Afilias system is architected such that read-only database connections are executed on database replicas and connections to the database master (where write-access is executed) are carefully protected to ensure high availability.

This interconnectivity is monitored, as is the entire registry system, according to the plans detailed in our response to question #42.

SYNCHRONIZATION SCHEME

Registry databases are synchronized both within the same data center and in the backup data center using a database application called Slony. For further details, please see the responses to questions #33 and #37. Slony replication of transactions from the publisher (master) database to its subscribers (replicas) works continuously to ensure the publisher and its subscribers remain synchronized. When the publisher database completes a transaction the Slony replication system ensures that each replica also processes the transaction. When there are no transactions to process, Slony “sleeps” until a transaction arrives or for one minute, whichever comes first. Slony “wakes up” each minute to confirm with the publisher that there has not been a transaction and thus ensures subscribers are synchronized and the replication time lag is minimized. The typical replication time lag between the publisher and subscribers depends on the topology of the replication cluster, specifically the location of the subscribers relative to the publisher. Subscribers located in the same data center as the publisher are typically updated within a couple of seconds, and subscribers located in a secondary data center are typically updated in less than ten seconds. This ensures real-time or near-real-time synchronization between all databases, and in the case where the secondary data center needs to be activated, it can be done with minimal disruption to registrars.

SRS SERVICE LEVEL AGREEMENT (SLA) PERFORMANCE COMPLIANCE

Afilias has a ten-year record of delivering on the demanding ICANN SLAs, and will continue to provide secure, stable and reliable service in compliance with SLA requirements as specified in the new gTLD Registry Agreement, Specification 10, as presented in Figure 24-b.

The Afilias SRS currently handles over 200 million EPP transactions per month for just .INFO and .ORG. Overall, the Afilias SRS manages over 700 million EPP transactions per month for all TLDs under management.

Given this robust functionality, and more than a decade of experience supporting a thick TLD registry with a strong performance history, Afilias, on behalf of Big Room, will meet or exceed the performance metrics in Specification 10 of the new gTLD Registry Agreement. The Afilias services and infrastructure are designed to scale both vertically and horizontally without any downtime to provide consistent performance as this TLD grows. The Afilias architecture is also massively provisioned to meet seasonal demands and marketing campaigns. Afilias’ experience also gives high confidence in the ability to scale and grow registry operations for this TLD in a secure, stable and reliable manner.

SRS RESOURCING PLANS

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of the .ECO TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Over 100 Afilias team members contribute to the management of the SRS code and network that will support this TLD. The SRS team is composed of Software Engineers, Quality Assurance Analysts, Application Administrators, System Administrators, Storage Administrators, Network Administrators, Database Administrators, and Security Analysts located at three geographically separate Afilias facilities. The systems and services set up and administered by these team members are monitored 24x7 by skilled analysts at two NOCs located in Toronto, Ontario (Canada) and Horsham, Pennsylvania (USA). In addition to these team members, Afilias also utilizes trained project management staff to maintain various calendars, work breakdown schedules, utilization and resource schedules and other tools to support the technical and management staff. It is this team who will both deploy this TLD on the Afilias infrastructure, and maintain it. Together, the Afilias team has managed 11 registry transitions and six new TLD launches, which illustrate its ability to securely and reliably deliver regularly scheduled updates as well as a secure, stable and reliable SRS service for the .ECO Community TLD.

25. Extensible Provisioning Protocol (EPP)

NOTE: THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (LESS THAN ⁄ GREATER THAN CHARACTERS) (THE “ ” and “ ” CHARACTERS, or and), WHICH ICANN INFORMS US (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE ANSWER BELOW AS DISPLAYED IN TAS MAY NOT RENDER THE FULL RESPONSE AS INTENDED. THEREFORE, THE FULL ANSWER TO THIS QUESTION IS ALSO ATTACHED AS A PDF FILE (25-EPP-response.pdf), ACCORDING TO SPECIFIC GUIDANCE FROM ICANN UNDER CASE ID 11027.
====

Answers for this question (#25) are provided by Afilias, the back-end provider of registry services for the .ECO Community TLD.

Afilias has been a pioneer and innovator in the use of EPP. .INFO was the first EPP-based gTLD registry and launched on EPP version 02⁄00. Afilias has a track record of supporting TLDs on standards-compliant versions of EPP. Afilias will operate the EPP registrar interface as well as a web-based interface for this TLD in accordance with RFCs and global best practices. In addition, Afilias will maintain a proper OT&E (Operational Testing and Evaluation) environment to facilitate registrar system development and testing.

Afilias’ EPP technical performance meets or exceeds all ICANN requirements as demonstrated by:
* A completely functional, state-of-the-art, EPP-based SRS that currently meets the needs of various gTLDs and will meet this new TLD’s needs;
* A track record of success in developing extensions to meet client and registrar business requirements such as multi-script support for IDNs;
* Supporting six ICANN gTLDs on EPP: .INFO, .ORG, .MOBI, .AERO, .ASIA and .XXX
* EPP software that is operating today and has been fully tested to be standards-compliant;
* Proven interoperability of existing EPP software with ICANN-accredited registrars, and;
* An SRS that currently processes over 200 million EPP transactions per month for both .INFO and .ORG. Overall, Afilias processes over 700 million EPP transactions per month for all 16 TLDs under management.

The EPP service is offered in accordance with the performance specifications defined in the new gTLD Registry Agreement, Specification 10.

EPP STANDARDS

The Afilias registry system complies with the following revised versions of the RFCs and operates multiple ICANN TLDs on these standards, including .INFO, .ORG, .MOBI, .ASIA and .XXX. The systems have been tested by our Quality Assurance (“QA”) team for RFC compliance, and have been used by registrars for an extended period of time:
* 3735 - Guidelines for Extending EPP
* 3915 - Domain Registry Grace Period Mapping
* 5730 - Extensible Provisioning Protocol (EPP)
* 5731 - Domain Name Mapping
* 5732 - Host Mapping
* 5733 - Contact Mapping
* 5734 - Transport Over TCP
* 5910 - Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)

This TLD will support all valid EPP commands. The following EPP commands are in operation today and will be made available for this TLD. See attachment #25a for the base set of EPP commands and copies of Afilias XSD schema files, which define all the rules of valid, RFC compliant EPP commands and responses that Afilias supports. Any customized EPP extensions, if necessary, will also conform to relevant RFCs.

Afilias staff members actively participated in the Internet Engineering Task Force (IETF) process that finalized the new standards for EPP. Afilias will continue to actively participate in the IETF and will stay abreast of any updates to the EPP standards.

EPP SOFTWARE INTERFACE AND FUNCTIONALITY

Afilias will provide all registrars with a free open-source EPP toolkit. Afilias provides this software for use with both Microsoft Windows and Unix/Linux operating systems. This software, which includes all relevant templates and schema defined in the RFCs, is available on sourceforge.net and will be available through the registry operator’s website.

Afilias’ SRS EPP software complies with all relevant RFCs and includes the following functionality:
* EPP Greeting: A response to a successful connection returns a greeting to the client. Information exchanged can include: name of server, server date and time in UTC, server features, e.g., protocol versions supported, languages for the text response supported, and one or more elements which identify the objects that the server is capable of managing;
* Session management controls: login to establish a connection with a server, and logout to end a session;
* EPP Objects: Domain, Host and Contact for respective mapping functions;
* EPP Object Query Commands: Info, Check, and Transfer (query) commands to retrieve object information, and;
* EPP Object Transform Commands: five commands to transform objects: create to create an instance of an object, delete to remove an instance of an object, renew to extend the validity period of an object, update to change information associated with an object, and transfer to manage changes in client sponsorship of a known object.

Currently, 100% of the top domain name registrars in the world have software that has already been tested and certified to be compatible with the Afilias SRS registry. In total, over 375 registrars, representing over 95% of all registration volume worldwide, operate software that has been certified compatible with the Afilias SRS registry. Afilias’ EPP Registrar Acceptance Criteria are available in attachment #25b, EPP OT&E Criteria.

Free EPP software support

Afilias analyzes and diagnoses registrar EPP activity log files as needed and is available to assist registrars who may require technical guidance regarding how to fix repetitive errors or exceptions caused by misconfigured client software.

Registrars are responsible for acquiring a TLS/SSL certificate from an approved certificate authority, as the registry-registrar communication channel requires mutual authentication; Afilias will acquire and maintain the server-side TLS/SSL certificate. The registrar is responsible for developing support for TLS/SSL in their client application. Afilias will provide free guidance for registrars unfamiliar with this requirement.

REGISTRAR DATA SYNCHRONIZATION

There are two methods available for registrars to synchronize their data with the registry:

* Automated synchronization: Registrars can, at any time, use the EPP info command to obtain definitive data from the registry for a known object, including domains, hosts (nameservers) and contacts.

* Personalized synchronization: A registrar may contact technical support and request a data file containing all domains (and associated host (nameserver) and contact information) registered by that registrar, within a specified time interval. The data will be formatted as a comma separated values (CSV) file and made available for download using a secure server.

EPP MODIFICATIONS

There are no unique EPP modifications planned for the .ECO Community TLD.

All ICANN TLDs must offer a Sunrise as part of a rights protection program. Afilias uses EPP extensions that allow registrars to submit trademark and other intellectual property rights (IPR) data to the registry. These extensions are:

* An ipr:name element that indicates the name of Registered Mark.

* An ipr:number element that indicates the registration number of the IPR.

* An ipr:ccLocality element that indicates the origin for which the IPR is established (a national or international trademark registry).

* An ipr:entitlement element that indicates whether the applicant holds the trademark as the original “OWNER”, “CO-OWNER” or “ASSIGNEE”.

* An ipr:appDate element that indicates the date the Registered Mark was applied for.

* An ipr:regDate element that indicates the date the Registered Mark was issued and registered.

* An ipr:class element that indicates the class of the registered mark.

* An ipr:type element that indicates the Sunrise phase the application applies for.

Note that some of these extensions might be subject to change based on ICANN-developed requirements for the Trademark Clearinghouse.

EPP RESOURCING PLANS

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

108 Afilias team members directly contribute to the management and development of the EPP based registry systems. As previously noted, Afilias is an active member of IETF and has a long documented history developing and enhancing EPP. These contributors include 11 developers and 14 QA engineers focused on maintaining and enhancing EPP server side software. These engineers work directly with business staff to timely address existing

needs and forecast registry/registrar needs to ensure the Afilias EPP software is effective today and into the future. A team of eight data analysts work with the EPP software system to ensure that the data flowing through EPP is securely and reliably stored in replicated database systems. In addition to the EPP developers, QA engineers, and data analysts, other EPP contributors at Afilias include: Technical Analysts, the Network Operations Center and Data Services team members.

26. Whois

Answers for this question (#26) are provided by Afilias, the back-end provider of registry services for the .ECO Community TLD.

Afilias operates the WHOIS (registration data directory service) infrastructure in accordance with RFCs and global best practices, as it does for the 16 TLDs it currently supports. Designed to be robust and scalable, Afilias' WHOIS service has exceeded all contractual requirements for over a decade. It has extended search capabilities, and methods of limiting abuse.

The WHOIS service operated by Afilias meets and exceeds ICANN's requirements. Specifically, Afilias will:
* Offer a WHOIS service made available on port 43 that is flexible and standards-compliant;
* Comply with all ICANN policies, and meeting or exceeding WHOIS performance requirements in Specification 10 of the new gTLD Registry Agreement;
* Enable a Searchable WHOIS with extensive search capabilities that offers ease of use while enforcing measures to mitigate access abuse, and;
* Employ a team with significant experience managing a compliant WHOIS service.

Such extensive knowledge and experience managing a WHOIS service enables Afilias to offer a comprehensive plan for the .ECO Community TLD that meets the needs of constituents of the domain name industry and Internet users. The service has been tested by our QA team for RFC compliance, and has been used by registrars and many other parties for an extended period of time. Afilias' WHOIS service currently serves almost 500 million WHOIS queries per month, with the capacity already built in to handle an order of magnitude increase in WHOIS queries, and the ability to smoothly scale should greater growth be needed.

Big Room, as the .ECO registry operator, commits to abiding by all local privacy laws and requirements with respect to the WHOIS service for the .ECO Community TLD.

WHOIS SYSTEM DESCRIPTION AND DIAGRAM

The Afilias WHOIS system, depicted in figure 26-a, is designed with robustness, availability, compliance, and performance in mind. Additionally, the system has provisions for detecting abusive usage (e.g., excessive numbers of queries from one source). The WHOIS system is generally intended as a publicly available single object lookup system. Afilias uses an advanced, persistent caching system to ensure extremely fast query response times.

Afilias will develop restricted WHOIS functions based on specific domain policy and regulatory requirements as needed for operating the business (as long as they are standards compliant). It will also be possible for contact and registrant information to be returned according to regulatory requirements. The WHOIS database supports multiple string and field searching through a reliable, free, secure web-based interface.

Data objects, interfaces, access and lookups

Registrars can provide an input form on their public websites through which a visitor is able to perform WHOIS queries. The registry operator can also provide a Web-based search on its site. The input form must accept the string to query, along with the necessary input elements to select the object type and interpretation controls. This input form sends its data to the Afilias port 43 WHOIS server. The results from the WHOIS query are returned by the server and displayed in the visitor’s Web browser. The sole purpose of the Web interface is to provide a user-friendly interface for WHOIS queries.

Afilias will provide WHOIS output as per Specification 4 of the new gTLD Registry Agreement. The output for domain records generally consists of the following elements:
* The name of the domain registered and the sponsoring registrar;
* The names of the primary and secondary nameserver(s) for the registered domain name;
* The creation date, registration status and expiration date of the registration;
* The name, postal address, e-mail address, and telephone and fax numbers of the domain name holder;
* The name, postal address, e-mail address, and telephone and fax numbers of the technical contact for the domain name holder;
* The name, postal address, e-mail address, and telephone and fax numbers of the administrative contact for the domain name holder, and;
* The name, postal address, e-mail address, and telephone and fax numbers of the billing contact for the domain name holder.
The following additional features are also present in Afilias’ WHOIS service:
* Support for IDNs, including the language tag and the Punycode representation of the IDN in addition to Unicode Hex and Unicode HTML formats;
* Enhanced support for privacy protection relative to the display of confidential information.

Afilias will also provide sophisticated WHOIS search functionality that includes the ability to conduct multiple string and field searches.

Query controls

For all WHOIS queries, a user is required to enter the character string representing the information for which they want to search. The object type and interpretation control parameters to limit the search may also be specified. If object type or interpretation control parameter is not specified, WHOIS will search for the character string in the Name field of the Domain object.

WHOIS queries are required to be either an ″exact search″ or a ″partial search,″ both of which are insensitive to the case of the input string.

An exact search specifies the full string to search for in the database field. An exact match between the input string and the field value is required.

A partial search specifies the start of the string to search for in the database field. Every record with a search field that starts with the input string is considered a match. By default, if multiple matches are found for a query, then a summary containing up to 50 matching results is presented. A second query is required to retrieve the specific details of one of the matching records.

If only a single match is found, then full details will be provided. Full detail consists of the data in the matching object as well as the data in any associated objects. For example: a query that results in a domain object includes the data from the associated host and contact objects.

WHOIS query controls fall into two categories: those that specify the type of field, and those that modify the interpretation of the input or determine the level of output to provide. Each is described below.

The following keywords restrict a search to a specific object type:
* Domain: Searches only domain objects. The input string is searched in the Name field.
* Host: Searches only nameserver objects. The input string is searched in the Name field and the IP Address field.
* Contact: Searches only contact objects. The input string is searched in the ID field.

* Registrar: Searches only registrar objects. The input string is searched in the Name field.
By default, if no object type control is specified, then the Name field of the Domain object is searched.

In addition, Afilias WHOIS systems can perform and respond to WHOIS searches by registrant name, postal address and contact names. Deployment of these features is provided as an option to the registry operator, based upon registry policy and business decision making.

Figure 26-b presents the keywords that modify the interpretation of the input or determine the level of output to provide.

By default, if no interpretation control keywords are used, the output will include full details if a single match is found and a summary if multiple matches are found.

Unique TLD requirements

There are no unique WHOIS requirements for the .ECO Community TLD.

Sunrise WHOIS processes

All ICANN TLDs must offer a Sunrise as part of a rights protection program. Afilias uses EPP extensions that allow registrars to submit trademark and other intellectual property rights (IPR) data to the registry. The following corresponding data will be displayed in WHOIS for relevant domains:
* Trademark Name: element that indicates the name of the Registered Mark.
* Trademark Number: element that indicates the registration number of the IPR.
* Trademark Locality: element that indicates the origin for which the IPR is established (a national or international trademark registry).
* Trademark Entitlement: element that indicates whether the applicant holds the trademark as the original “OWNER”, “CO-OWNER” or “ASSIGNEE”.
 * Trademark Application Date: element that indicates the date the Registered Mark was applied for.
* Trademark Registration Date: element that indicates the date the Registered Mark was issued and registered.
* Trademark Class: element that indicates the class of the Registered Mark.
* IPR Type: element that indicates the Sunrise phase the application applies for.

IT AND INFRASTRUCTURE RESOURCES

All the applications and databases for the .ECO Community TLD will run in a virtual environment hosted by a cluster of servers equipped with the latest Intel Westmere multi-core processors (or a more advanced, stable technology available at the time of deployment). The registry data will be stored on storage arrays of solid-state drives shared over a fast storage area network. The virtual environment allows the infrastructure to easily scale both vertically and horizontally to cater to changing demand. It also facilitates effective utilization of system resources thus reducing energy consumption and carbon footprint.

The applications and servers are supported by network firewalls, routers and switches. The WHOIS system accommodates both IPv4 and IPv6 addresses.

Each of the servers and network devices are equipped with redundant hot-swappable components and multiple connections to ancillary systems. Additionally, 24x7 support agreements with our hardware vendor with a 4-hour response time at all our data centers guarantees replacement of failed parts in the shortest time possible.

Models of system and network devices used are:
* Servers: Cisco UCS B230 blade servers
* SAN storage arrays: IBM Storwize V7000 with Solid State Drives
* Firewalls: Cisco ASA 5585-X

* Load balancers: F5 Big-IP 6900
* Traffic shapers: Procera PacketLogic PL8720
* Routers: Juniper MX40 3D
* Network switches: Cisco Nexus 7010, Nexus 5548, Nexus 2232

There will be at least four virtual machines (VMs) offering WHOIS service. Each VM will run at least two WHOIS server instances - one for registrars and one for the public. All instances of the WHOIS service is made available to registrars and the public are rate limited to mitigate abusive behavior.

FREQUENCY OF SYNCHRONIZATION BETWEEN SERVERS

Registration data records from the EPP publisher database will be replicated to the WHOIS system database on a near-real-time basis whenever an update occurs.

SPECIFICATIONS 4 AND 10 COMPLIANCE

The WHOIS service for this TLD will meet or exceed the performance requirements in the new gTLD Registry Agreement, Specification 10. Figure 26-c provides the exact measurements and commitments. Afilias has a 10 year track record of exceeding WHOIS performance and a skilled team to ensure this continues for all TLDs under management.

The WHOIS service for the .ECO Community TLD will meet or exceed the requirements in the new gTLD Registry Agreement, Specification 4.

RFC 3912 COMPLIANCE

Afilias will operate the WHOIS infrastructure in compliance with RFCs and global best practices, as it does with the 16 TLDs Afilias currently supports.

Afilias maintains a registry-level centralized WHOIS database that contains information for every registered domain and for all host and contact objects. The WHOIS service will be available on the Internet standard WHOIS port (port 43) in compliance with RFC 3912. The WHOIS service contains data submitted by registrars during the registration process. Changes made to the data by a registrant are submitted to Afilias by the registrar and are reflected in the WHOIS database and service in near-real-time, by the instance running at the primary data center, and in under ten seconds by the instance running at the secondary data center, thus providing all interested parties with up-to-date information for every domain. This service is compliant with the new gTLD Registry Agreement, Specification 4.

The WHOIS service maintained by Afilias will be authoritative and complete, as this will be a “thick” registry (detailed domain contact WHOIS is all held at the registry); users do not have to query different registrars for WHOIS information, as there is one central WHOIS system. Additionally, visibility of different types of data is configurable to meet the registry operator’s needs.

SEARCHABLE WHOIS

Afilias offers a searchable WHOIS on a web-based Directory Service. Partial match capabilities are offered on the following fields: domain name, registrar ID, and IP address. In addition, Afilias WHOIS systems can perform and respond to WHOIS searches by registrant name, postal address and contact names.

Providing the ability to search important and high-value fields such as registrant name, address and contact names increases the probability of abusive behavior. An abusive user could script a set of queries to the WHOIS service and access contact data in order to create or sell a list of names and addresses of registrants in this TLD. Making the WHOIS machine readable, while preventing harvesting and mining of WHOIS data, is a key requirement integrated into the Afilias WHOIS systems. For instance, Afilias limits search returns to 50 records at a time. If bulk queries were ever necessary (e.g., to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process), Afilias makes such query responses available to carefully screened and limited staff members at the registry operator (and customer support staff) via an internal data warehouse. The Afilias WHOIS system accommodates anonymous access as well as pre-identified and profile-defined uses, with full audit and log capabilities.

The WHOIS service has the ability to tag query responses with labels such as “Do not redistribute” or “Special access granted”. This may allow for tiered response and reply scenarios. Further, the WHOIS service is configurable in parameters and fields returned, which allow for flexibility in compliance with various jurisdictions, regulations or laws.

Afilias offers exact-match capabilities on the following fields: registrar ID, nameserver name, and nameserver’s IP address (only applies to IP addresses stored by the registry, i.e., glue records). Search capabilities are fully available, and results include domain names matching the search criteria (including IDN variants). Afilias manages abuse prevention through rate limiting and CAPTCHA (described below). Queries do not require specialized transformations of internationalized domain names or internationalized data fields

Please see “Query Controls” above for details about search options and capabilities.

DETERRING WHOIS ABUSE

Afilias has adopted two best practices to prevent abuse of the WHOIS service: rate limiting and CAPTCHA.

Abuse of WHOIS services on port 43 and via the Web is subject to an automated rate-limiting system. This ensures that uniformity of service to users is unaffected by a few parties whose activities abuse or otherwise might threaten to overload the WHOIS system.

Abuse of web-based public WHOIS services is subject to the use of CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) technology. The use of CAPTCHA ensures that uniformity of service to users is unaffected by a few parties whose activities abuse or otherwise might threaten to overload the WHOIS system. The registry operator will adopt a CAPTCHA on its Web-based WHOIS.

Data mining of any sort on the WHOIS system is strictly prohibited, and this prohibition is published in WHOIS output and in terms of service.

For rate limiting on IPv4, there are configurable limits per IP and subnet. For IPv6, the traditional limitations do not apply. Whenever a unique IPv6 IP address exceeds the limit of WHOIS queries per minute, the same rate-limit for the given 64 bits of network prefix that the offending IPv6 IP address falls into will be applied. At the same time, a timer will start and rate-limit validation logic will identify if there are any other IPv6 address within the original 80-bit(/48) prefix. If another offending IPv6 address does fall into the /48 prefix then rate-limit validation logic will penalize any other IPv6 addresses that fall into that given 80-bit (/48) network. As a security precaution, Afilias will not disclose these limits.

Pre-identified and profile-driven role access allows greater granularity and configurability in both access to the WHOIS service, and in volume/frequency of responses returned for queries.

Afilias staff are key participants in the ICANN Security & Stability Advisory Committee’s deliberations and outputs on WHOIS, including SAC003, SAC027, SAC033, SAC037, SAC040, and SAC051. Afilias staff are active participants in both technical and policy decision making in ICANN, aimed at restricting abusive behavior.

WHOIS STAFF RESOURCING PLANS

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of the .ECO Community TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Within Afilias, there are 11 staff members who develop and maintain the compliant WHOIS systems. They keep pace with access requirements, thwart abuse, and continually develop software. Of these resources, approximately two staffers are typically required for WHOIS-related code customization. Other resources provide quality assurance, and operations personnel maintain the WHOIS system itself. This team will be responsible for the implementation and on-going maintenance of the new TLD WHOIS service.

27. Registration Life Cycle

NOTE: THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (LESS THAN / GREATER THAN CHARACTERS) (THE “ ” and “ ” CHARACTERS, or and), WHICH ICANN INFORMS US (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE ANSWER BELOW AS DISPLAYED IN TAS MAY NOT RENDER THE FULL RESPONSE AS INTENDED. THEREFORE, THE FULL ANSWER TO THIS QUESTION IS ALSO ATTACHED AS A PDF FILE (27-Registration-Lifecycle-response.pdf), ACCORDING TO SPECIFIC GUIDANCE FROM ICANN UNDER CASE ID 11027.
====

Answers for this question (#27) are provided by Afilias, the back-end provider of registry services for the .ECO Community TLD.

Afilias has been managing registrations for over a decade. Afilias has had experience managing registrations for over a decade and supports comprehensive registration lifecycle services including the registration states, all standard grace periods, and can address any modifications required with the introduction of any new ICANN policies.

This TLD will follow the ICANN standard domain lifecycle, as is currently implemented in TLDs such as .ORG and .INFO. The below response includes: a diagram and description of the lifecycle of a domain name in this TLD, including domain creation, transfer protocols, grace period implementation and the respective time frames for each; and the existing resources to support the complete lifecycle of a domain.

As depicted in Figure 27-a, prior to the beginning of the Trademark Claims Service or Sunrise IP protection program[s], Afilias will support the reservation of names in accordance with the new gTLD Registry Agreement, Specification 5.

REGISTRATION PERIOD

After the IP protection programs and the general launch, eligible registrants may choose an accredited registrar to register a domain name. The registrar will check availability on the requested domain name and if available, will collect specific objects such as, the required contact and host information from the registrant. The registrar will then provision the information into the registry system using standard Extensible Provisioning Protocol (“EPP”) commands through a secure connection to the registry backend service provider.

When the domain is created, the standard five day Add Grace Period begins, the domain and contact information are available in WHOIS, and normal operating EPP domain statuses will apply. Other specifics regarding registration rules for an active domain include:
* The domain must be unique;
* Restricted or reserved domains cannot be registered;

* The domain can be registered from 1-10 years;
* The domain can be renewed at any time for 1-10 years, but cannot exceed 10 years;
* The domain can be explicitly deleted at any time;
* The domain can be transferred from one registrar to another except during the first 60 days following a successful registration or within 60 days following a transfer; and, Contacts and hosts can be modified at any time.

The following describe the domain status values recognized in WHOIS when using the EPP protocol following RFC 5731.
* OK or Active: This is the normal status for a domain that has no pending operations or restrictions.
* Inactive: The domain has no delegated name servers.
* Locked: No action can be taken on the domain. The domain cannot be renewed, transferred, updated, or deleted. No objects such as contacts or hosts can be associated to, or disassociated from the domain. This status includes: Delete Prohibited / Server Delete Prohibited, Update Prohibited / Server Update Prohibited, Transfer Prohibited, Server Transfer Prohibited, Renew Prohibited, Server Renew Prohibited.
* Hold: The domain will not be included in the zone. This status includes: Client Hold, Server Hold.
* Transfer Prohibited: The domain cannot be transferred away from the sponsoring registrar. This status includes: Client Transfer Prohibited, Server Transfer Prohibited.

The following describe the registration operations that apply to the domain name during the registration period.
a. Domain modifications: This operation allows for modifications or updates to the domain attributes to include:
i. Registrant Contact
ii. Admin Contact
iii. Technical Contact
iv. Billing Contact
v. Host or nameservers
vi. Authorization information
vii. Associated status values
A domain with the EPP status of Client Update Prohibited or Server Update Prohibited may not be modified until the status is removed.
b. Domain renewals: This operation extends the registration period of a domain by changing the expiration date. The following rules apply:
i. A domain can be renewed at any time during its registration term,
ii. The registration term cannot exceed a total of 10 years.
A domain with the EPP status of Client Renew Prohibited or Server Renew Prohibited cannot be renewed.
c. Domain deletions: This operation deletes the domain from the Shared Registry Services (SRS). The following rules apply:
i. A domain can be deleted at any time during its registration term, f the domain is deleted during the Add Grace Period or the Renew/Extend Grace Period, the sponsoring registrar will receive a credit,
ii. A domain cannot be deleted if it has “child” nameservers that are associated to other domains.
A domain with the EPP status of Client Delete Prohibited or Server Delete Prohibited cannot be deleted.
d. Domain transfers: A transfer of the domain from one registrar to another is conducted by following the steps below.
i. The registrant must obtain the applicable authInfo code from the sponsoring (losing) registrar.
* Every domain name has an authInfo code as per EPP RFC 5731. The authInfo code is a six- to 16-character code assigned by the registrar at the time the name was created. Its purpose is to aid identification of the domain owner so proper authority can be established (it is the ″password″ to the domain).
* Under the Registry-Registrar Agreement, registrars will be required to provide a copy of the authInfo code to the domain registrant upon his or her request.
ii. The registrant must provide the authInfo code to the new (gaining) registrar, who will then initiate a domain transfer request. A transfer cannot be initiated without the

authInfo code.
* Every EPP transfer command must contain the authInfo code or the request will fail. The authInfo code represents authority to the registry to initiate a transfer.
iii. Upon receipt of a valid transfer request, the registry automatically asks the sponsoring (losing) registrar to approve the request within five calendar days.
* When a registry receives a transfer request the domain cannot be modified, renewed or deleted until the request has been processed. This status must not be combined with either Client Transfer Prohibited or Server Transfer Prohibited status.
* If the sponsoring (losing) registrar rejects the transfer within five days, the transfer request is cancelled. A new domain transfer request will be required to reinitiate the process.
* If the sponsoring (losing) registrar does not approve or reject the transfer within five days, the registry automatically approves the request.
iv. After a successful transfer, it is strongly recommended that registrars change the authInfo code, so that the prior registrar or registrant cannot use it anymore.
v. Registrars must retain all transaction identifiers and codes associated with successful domain object transfers and protect them from disclosure.
vi. Once a domain is successfully transferred the status of TRANSFERPERIOD is added to the domain for a period of five days.
vii. Successful transfers will result in a one year term extension (resulting in a maximum total of 10 years), which will be charged to the gaining registrar.
e. Bulk transfer: Afilias, supports bulk transfer functionality within the SRS for situations where ICANN may request the registry to perform a transfer of some or all registered objects (includes domain, contact and host objects) from one registrar to another registrar. Once a bulk transfer has been executed, expiry dates for all domain objects remain the same, and all relevant states of each object type are preserved. In some cases the gaining and the losing registrar as well as the registry must approved bulk transfers. A detailed log is captured for each bulk transfer process and is archived for audit purposes.
Big Room will support ICANN’s Transfer Dispute Resolution Process. Big Room will work with Afilias to respond to Requests for Enforcement (law enforcement or court orders) and will follow that process.

1. Auto-renew grace period
The Auto-Renew Grace Period displays as AUTORENEWPERIOD in WHOIS. An auto-renew must be requested by the registrant through the sponsoring registrar and occurs if a domain name registration is not explicitly renewed or deleted by the expiration date and is set to a maximum of 45 calendar days. In this circumstance the registration will be automatically renewed by the registry system the first day after the expiration date. If a Delete, Extend, or Transfer occurs within the AUTORENEWPERIOD the following rules apply:
i. Delete. If a domain is deleted the sponsoring registrar at the time of the deletion receives a credit for the auto-renew fee. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.
ii. Renew/Extend. A domain can be renewed as long as the total term does not exceed 10 years. The account of the sponsoring registrar at the time of the extension will be charged for the additional number of years the registration is renewed.
iii. Transfer (other than ICANN-approved bulk transfer). If a domain is transferred, the losing registrar is credited for the auto-renew fee, and the year added by the operation is cancelled. As a result of the transfer, the expiration date of the domain is extended by minimum of one year as long as the total term does not exceed 10 years. The gaining registrar is charged for the additional transfer year(s) even in cases where a full year is not added because of the maximum 10 year registration restriction.

2. Redemption grace period
During this period, a domain name is placed in the PENDING DELETE RESTORABLE status when a registrar requests the deletion of a domain that is not within the Add Grace Period. A domain can remain in this state for up to 30 days and will not be included in the zone file. The only action a registrar can take on a domain is to request that it be restored. Any other registrar requests to modify or otherwise update the domain will be rejected. If the domain is restored it moves into PENDING RESTORE and then OK. After 30 days if the domain is not restored it moves into PENDING DELETE SCHEDULED FOR RELEASE before the domain is released back into the pool of available domains.

3. Pending delete
During this period, a domain name is placed in PENDING DELETE SCHEDULED FOR RELEASE status for five days, and all Internet services associated with the domain will remain disabled and domain cannot be restored. After five days the domain is released back into the pool of available domains.

OTHER GRACE PERIODS

All ICANN required grace periods will be implemented in the registry backend service provider’s system including the Add Grace Period (AGP), Renew/Extend Grace Period (EGP), Transfer Grace Period (TGP), Auto-Renew Grace Period (ARGP), and Redemption Grace Period (RGP). The lengths of grace periods are configurable in the registry system. At this time, the grace periods will be implemented following other gTLDs such as .ORG. More than one of these grace periods may be in effect at any one time. The following are accompanying grace periods to the registration lifecycle.

ADD GRACE PERIOD

The Add Grace Period displays as ADDPERIOD in WHOIS and is set to five calendar days following the initial registration of a domain. If the domain is deleted by the registrar during this period, the registry provides a credit to the registrar for the cost of the registration. If a Delete, Renew/Extend, or Transfer operation occurs within the five calendar days, the following rules apply.
i. Delete. If a domain is deleted within this period the sponsoring registrar at the time of the deletion is credited for the amount of the registration. The domain is deleted from the registry backend service provider’s database and is released back into the pool of available domains.
ii. Renew/Extend. If the domain is renewed within this period and then deleted, the sponsoring registrar will receive a credit for both the registration and the extended amounts. The account of the sponsoring registrar at the time of the renewal will be charged for the initial registration plus the number of years the registration is extended. The expiration date of the domain registration is extended by that number of years as long as the total term does not exceed 10 years.
iii. Transfer (other than ICANN-approved bulk transfer). Transfers under Part A of the ICANN Policy on Transfer of Registrations between registrars may not occur during the ADDPERIOD or at any other time within the first 60 days after the initial registration. Enforcement is the responsibility of the registrar sponsoring the domain name registration and is enforced by the SRS.

RENEW / EXTEND GRACE PERIOD

The Renew / Extend Grace Period displays as RENEWPERIOD in WHOIS and is set to five calendar days following an explicit renewal on the domain by the registrar. If a Delete, Extend, or Transfer occurs within the five calendar days, the following rules apply:
i. Delete. If a domain is deleted within this period the sponsoring registrar at the time of the deletion receives a credit for the renewal fee. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.
ii. Renew/Extend. A domain registration can be renewed within this period as long as the total term does not exceed 10 years. The account of the sponsoring registrar at the time of the extension will be charged for the additional number of years the registration is renewed.
iii. Transfer (other than ICANN-approved bulk transfer). If a domain is transferred within the Renew/Extend Grace Period, there is no credit to the losing registrar for the renewal fee. As a result of the transfer, the expiration date of the domain registration is extended by a minimum of one year as long as the total term for the domain does not exceed 10 years.
If a domain is auto-renewed, then extended, and then deleted within the Renew/Extend Grace Period, the registrar will be credited for any auto-renew fee charged and the number of years for the extension. The years that were added to the domain’s expiration as a result of the auto-renewal and extension are removed. The deleted domain is moved to the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.

TRANSFER GRACE PERIOD

The Transfer Grace period displays as TRANSFERPERIOD in WHOIS and is set to five calendar days after the successful transfer of domain name registration from one registrar to another registrar. Transfers under Part A of the ICANN Policy on Transfer of Registrations between registrars may not occur during the TRANSFERPERIOD or within the first 60 days after the transfer. If a Delete or Renew/Extend occurs within that five calendar days, the following rules apply:
i. Delete. If the domain is deleted by the new sponsoring registrar during this period, the registry provides a credit to the registrar for the cost of the transfer. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.
ii. Renew/Extend. If a domain registration is renewed within the Transfer Grace Period, there is no credit for the transfer. The registrar's account will be charged for the number of years the registration is renewed. The expiration date of the domain registration is extended by the renewal years as long as the total term does not exceed 10 years.

SPECIAL CONSIDERATIONS

NONE. COMMUNITY ELIGIBILITY IMPLEMENTATION DOES NOT AFFECT REGISTRATION LIFECYCLE.

Consistent with the requirements of the community-based designation for the .ECO domain, the registry will maintain community eligibility requirements as described in responses #18, #20.

The registry will employ standard registration lifecycle mechanisms, statuses, and states such as HOLD or LOCK functions, or other existing Extensible Provisioning Protocol (EPP) commands, in order to disallow a domain to be active when a registrant is not in compliance with the community eligibility requirements or under related community dispute resolution procedures.

The community-designated .ECO TLD will maintain a domain challenge process, as outlined in response #18(b) and #20(e). The Registry will support a Community Eligibility Dispute Resolution Process (CEDRP) aligned with the Accountability Policy described in the .ECO Policy Consensus. This process will use standard registration lifecycle elements and not require any new capabilities.

The .ECO Community TLD will conduct an auction for certain domain names. Afilias will manage the domain name auction using existing technology. Upon the completion of the auction, any domain name acquired will then follow the standard lifecycle of a domain.

REGISTRATION LIFECYCLE RESOURCES

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way. Virtually all Afilias resource are involved in the registration lifecycle of domains.

There are a few areas where registry staff devote resources to registration lifecycle issues:
a. Supporting Registrar Transfer Disputes. The registry operator will have a compliance staffer handle these disputes as they arise; they are very rare in the existing gTLDs.
b. Afilias has its development and quality assurance departments on hand to modify the grace period functionality as needed, if ICANN issues new Consensus Policies or the RFCs

change.

Afilias has more than 30 staff members in these departments.

28. Abuse Prevention and Mitigation

Big Room, the .ECO Registry Operator, working with Afilias, will take the requisite operational and technical steps to promote WHOIS data accuracy, limit domain abuse, remove outdated and inaccurate data, and other security measures to ensure the integrity of the .ECO Community TLD. The specific measures include, but are not limited to:
* Posting a .ECO Community TLD Anti-Abuse Policy that clearly defines abuse, and provide point-of-contact information for reporting suspected abuse;
* Committing to rapid identification and resolution of abuse, including suspensions;
* Ensuring completeness of WHOIS information at the time of registration;
* Publishing and maintaining procedures for removing orphan glue records for names removed from the zone, and;
* Establishing measures to deter WHOIS abuse, including rate-limiting, determining data syntax validity, and implementing and enforcing requirements from the Registry-Registrar Agreement.

ABUSE POLICY

The Anti-Abuse Policy stated below will be enacted under the contractual authority of the registry operator through the Registry-Registrar Agreement, and the obligations will be passed on to and made binding upon registrants. This policy will be posted on the .ECO Community TLD web site along with contact information for registrants or users to report suspected abuse.

The policy is designed to address the malicious use of domain names. The registry operator and its registrars will make reasonable attempts to limit significant harm to Internet users. This policy is not intended to take the place of the Uniform Domain Name Dispute Resolution Policy (UDRP) or the Uniform Rapid Suspension System (URS), and it is not to be used as an alternate form of dispute resolution or as a brand protection mechanism. Its intent is not to burden law-abiding or innocent registrants and domain users; rather, the intent is to deter those who use domain names maliciously by engaging in illegal or fraudulent activity.

Repeat violations of the abuse policy will result in a case-by-case review of the abuser(s), and the registry operator reserves the right to escalate the issue, with the intent of levying sanctions that are allowed under the TLD anti-abuse policy.

The below policy is a recent version of the policy that has been used by the .INFO registry since 2008, and the .ORG registry since 2009. It has proven to be an effective and flexible tool.

.ECO Anti-Abuse Policy

The following Anti-Abuse Policy is effective upon launch of the .ECO Community TLD. Malicious use of domain names will not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars, and registrants, as well as for users of the Internet in general. The registry operator definition of abusive use of a domain includes, without limitation, the following:
* Illegal or fraudulent actions;
* Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of web sites and Internet forums;
* Phishing: The use of counterfeit web pages that are designed to trick recipients into divulging sensitive data such as personally identifying information, usernames, passwords, or financial data;

* Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or poisoning;
* Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner′s informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and Trojan horses.
* Malicious fast-flux hosting: Use of fast-flux techniques with a botnet to disguise the location of web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities.
* Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or ″zombies,″ or to direct distributed denial-of-service attacks (DDoS attacks);
* Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual′s system (often known as ″hacking″). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Pursuant to the Registry-Registrar Agreement, registry operator reserves the right at its sole discretion to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary: (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of registry operator, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement and this Anti-Abuse Policy, or (5) to correct mistakes made by registry operator or any registrar in connection with a domain name registration. Registry operator also reserves the right to place upon registry lock, hold, or similar status a domain name during resolution of a dispute.

The policy stated above will be accompanied by notes about how to submit a report to the registry operator’s abuse point of contact, and how to report an orphan glue record suspected of being used in connection with malicious conduct (see below).

ABUSE POINT OF CONTACT AND PROCEDURES FOR HANDLING ABUSE COMPLAINTS

The registry operator will establish an abuse point of contact. This contact will be a role-based e-mail address of the form “abuse@registry.ECO”. This e-mail address will allow multiple staff members to monitor abuse reports on a 24x7 basis, and then work toward closure of cases as each situation calls for. For tracking purposes, the registry operator will have a ticketing system with which all complaints will be tracked internally. The reporter will be provided with the ticket reference identifier for potential follow-up. Afilias will integrate its existing ticketing system with the registry operator’s to ensure uniform tracking and handling of the complaint. This role-based approach has been used successfully by ISPs, e-mail service providers, and registrars for many years, and is considered a global best practice.

The .ECO registry operator’s designated abuse handlers will then evaluate complaints received via the abuse system address. They will decide whether a particular issue is of concern, and decide what action, if any, is appropriate.

In general, the registry operator will find itself receiving abuse reports from a wide variety of parties, including security researchers and Internet security companies, financial institutions such as banks, Internet users, and law enforcement agencies among others. Some of these parties may provide good forensic data or supporting evidence of the malicious behavior. In other cases, the party reporting an issue may not be familiar with how to provide such data or proof of malicious behavior. It is expected that a percentage of abuse reports to the registry operator will not be actionable, because there will not be enough evidence to support the complaint (even after investigation), and because some reports or reporters will simply not be credible.

The security function includes a communication and outreach function, with information sharing with industry partners regarding malicious or abusive behavior, in order to ensure coordinated abuse mitigation across multiple TLDs.

Assessing abuse reports requires great care, and the registry operator will rely upon professional, trained investigators who are versed in such matters. The goals are accuracy, good record-keeping, and a zero false-positive rate so as not to harm innocent registrants.

Different types of malicious activities require different methods of investigation and documentation. Further, the registry operator expects to face unexpected or complex situations that call for professional advice, and will rely upon professional, trained investigators as needed.

In general, there are two types of domain abuse that must be addressed:
a) Compromised domains. These domains have been hacked or otherwise compromised by criminals, and the registrant is not responsible for the malicious activity taking place on the domain. For example, the majority of domain names that host phishing sites are compromised. The goal in such cases is to get word to the registrant (usually via the registrar) that there is a problem that needs attention with the expectation that the registrant will address the problem in a timely manner. Ideally such domains do not get suspended, since suspension would disrupt legitimate activity on the domain.
b) Malicious registrations. These domains are registered by malefactors for the purpose of abuse. Such domains are generally targets for suspension, since they have no legitimate use.

The standard procedure is that the registry operator will forward a credible alleged case of malicious domain name use to the domain’s sponsoring registrar with a request that the registrar investigate the case and act appropriately. The registrar will be provided evidence collected as a result of the investigation conducted by the trained abuse handlers. As part of the investigation, if inaccurate or false WHOIS registrant information is detected, the registrar is notified about this. The registrar is the party with a direct relationship with—and a direct contract with—the registrant. The registrar will also have vital information that the registry operator will not, such as:
* Details about the domain purchase, such as the payment method used (credit card, PayPal, etc.);
* The identity of a proxy-protected registrant;
* The purchaser’s IP address;
* Whether there is a reseller involved, and;
* The registrant’s past sales history and purchases in other TLDs (insofar as the registrar can determine this).

Registrars do not share the above information with registry operators due to privacy and liability concerns, among others. Because they have more information with which to continue the investigation, and because they have a direct relationship with the registrant, the registrar is in the best position to evaluate alleged abuse. The registrar can determine if the use violates the registrar’s legal terms of service or the registry Anti-Abuse Policy, and can decide whether or not to take any action. While the language and terms vary, registrars will be expected to include language in their registrar-registrant contracts that indemnifies the registrar if it takes action, and allows the registrar to suspend or cancel a domain name; this will be in addition to the registry Anti-Abuse Policy. Generally, registrars can act if the registrant violates the registrar’s terms of service, or violates ICANN policy, or if illegal activity is involved, or if the use violates the registry’s Anti-Abuse Policy.

If a registrar does not take action within a time period indicated by the registry operator (usually 24 hours), the registry operator might then decide to take action itself. At all times, the registry operator reserves the right to act directly and immediately if the potential harm to Internet users seems significant or imminent, with or without notice to the sponsoring registrar.

The registry operator will be prepared to call upon relevant law enforcement bodies as needed. There are certain cases, for example, Illegal pharmacy domains, where the registry operator will contact the Law Enforcement Agencies to share information about these domains, provide all the evidence collected and work closely with them before any action will be taken for suspension. The specific action is often dependent upon the jurisdiction of which the registry operator, although the operator in all cases will adhere to applicable laws and regulations.

When valid court orders or seizure warrants are received from courts or law enforcement agencies of relevant jurisdiction, the registry operator will order execution in an expedited fashion. Compliance with these will be a top priority and will be completed as soon as possible and within the defined timelines of the order. There are certain cases where Law Enforcement Agencies request information about a domain including but not limited to:
* Registration information
* History of a domain, including recent updates made
* Other domains associated with a registrant’s account
* Patterns of registrant portfolio

Requests for such information is handled on a priority basis and sent back to the requestor as soon as possible. Afilias sets a goal to respond to such requests within 24 hours.

The registry operator may also engage in proactive screening of its zone for malicious use of the domains in the TLD, and report problems to the sponsoring registrars. The registry operator could take advantage of a combination of the following resources, among others:
* Blocklists of domain names and nameservers published by organizations such as SURBL and Spamhaus.
* Anti-phishing feeds, which will provide URLs of compromised and maliciously registered domains being used for phishing.
* Analysis of registration or DNS query data [DNS query data received by the TLD nameservers.]

The registry operator will keep records and track metrics regarding abuse and abuse reports. These will include:
* Number of abuse reports received by the registry’s abuse point of contact described above;
* Number of cases and domains referred to registrars for resolution;
* Number of cases and domains where the registry took direct action;
* Resolution times;
* Number of domains in the TLD that have been blacklisted by major anti-spam blocklist providers, and;
* Phishing site uptimes in the TLD.

REMOVAL OF ORPHAN GLUE RECORDS

By definition, orphan glue records used to be glue records. Glue records are related to delegations and are necessary to guide iterative resolvers to delegated nameservers. A glue record becomes an orphan when its parent nameserver record is removed without also removing the corresponding glue record. (Please reference the ICANN SSAC paper SAC048 at: http://www.icann.org/en/committees/security/sac048.pdf.) Orphan glue records may be created when a domain (example.tld) is placed on EPP ServerHold or ClientHold status. When placed on Hold, the domain is removed from the zone and will stop resolving. However, any child nameservers (now orphan glue) of that domain (e.g., ns1.example.tld) are left in the zone. It is important to keep these orphan glue records in the zone so that any innocent sites using that nameserver will continue to resolve. This use of Hold status is an essential tool for suspending malicious domains.

Afilias observes the following procedures, which are being followed by other registries and are generally accepted as DNS best practices. These procedures are also in keeping with ICANN SSAC recommendations.

When a request to delete a domain is received from a registrar, the registry first checks for the existence of glue records. If glue records exist, the registry will check to see if other domains in the registry are using the glue records. If other domains in the registry are using the glue records then the request to delete the domain will fail until no other domains are using the glue records. If no other domains in the registry are using the glue records then the glue records will be removed before the request to delete the domain is satisfied. If no glue records exist then the request to delete the domain will be satisfied.

If a registrar cannot delete a domain because of the existence of glue records that are being used by other domains, then the registrar may refer to the zone file or the “weekly domain hosted by nameserver report” to find out which domains are using the nameserver in question and attempt to contact the corresponding registrar to request that they stop using the nameserver in the glue record. The registry operator does not plan on performing mass updates of the associated DNS records.

The registry operator will accept, evaluate, and respond appropriately to complaints that orphan glue is being used maliciously. Such reports should be made in writing to the registry operator, and may be submitted to the registry’s abuse point-of-contact. If it is confirmed that an orphan glue record is being used in connection with malicious conduct, the registry operator will have the orphan glue record removed from the zone file. Afilias has the technical ability to execute such requests as needed.

METHODS TO PROMOTE WHOIS ACCURACY

The creation and maintenance of accurate WHOIS records is an important part of registry management. As described in our response to question #26, WHOIS, the registry operator will manage a secure, robust and searchable WHOIS service for the .ECO TLD.

WHOIS data accuracy

The registry operator will offer a “thick” registry system. In this model, all key contact details for each domain name will be stored in a central location by the registry. This allows better access to domain data, and provides uniformity in storing the information. The registry operator will ensure that the required fields for WHOIS data (as per the defined policies for the TLD) are enforced at the registry level. This ensures that the registrars are providing required domain registration data. Fields defined by the registry policy to be mandatory are documented as such and must be submitted by registrars. The Afilias registry system verifies formats for relevant individual data fields (e.g. e-mail, and phone/fax numbers). Only valid country codes are allowed as defined by the ISO 3166 code list. The Afilias WHOIS system is extensible, and is capable of using the VAULT system, described further below.

Similar to the centralized abuse point of contact described above, the registry operator can institute a contact email address which could be utilized by third parties to submit complaints for inaccurate or false WHOIS data detected. This information will be processed by Afilias’ support department and forwarded to the registrars. The registrars can work with the registrants of those domains to address these complaints. Afilias will audit registrars on a yearly basis to verify whether the complaints being forwarded are being addressed or not. This functionality, available to all registry operators, is activated based on the registry operator’s business policy.

Afilias also incorporates a spot-check verification system where a randomly selected set of domain names are checked periodically for accuracy of WHOIS data. Afilias’ .PRO registry system incorporates such a verification system whereby 1% of total registrations or 100 domains, whichever number is larger, are spot-checked every month to verify the domain name registrant’s critical information provided with the domain registration data. With both a highly qualified corps of engineers and a 24x7 staffed support function, Afilias has the capacity to integrate such spot-check functionality into the .ECO TLD, based on the registry operator’s business policy. Note: This functionality will not work for proxy protected WHOIS information, where registrars or their resellers have the actual registrant data. The solution to that problem lies with either registry or registrar policy, or a change in the general marketplace practices with respect to proxy registrations. The .ECO registry does not intend to support proxy registrations.

Finally, Afilias' registry systems have a sophisticated set of billing and pricing functionality which aids registry operators who decide to provide a set of financial incentives to registrars for maintaining or improving WHOIS accuracy. For instance, it is conceivable that the registry operator may decide to provide a discount for the domain registration or renewal fees for validated registrants, or levy a larger cost for the domain registration or renewal of proxy domain names. The .ECO registry does not intend to support proxy registrations. The Afilias system has the capability to support such incentives on a configurable basis, towards the goal of promoting better WHOIS accuracy.

Role of registrars

As part of the RRA (Registry Registrar Agreement), the registry operator will require the registrar to be responsible for ensuring the input of accurate WHOIS data by their registrants. The Registrar/Registered Name Holder Agreement will include a specific clause to ensure accuracy of WHOIS data, and to give the registrar rights to cancel or suspend registrations if the Registered Name Holder fails to respond to the registrar's query regarding accuracy of data. ICANN's WHOIS Data Problem Reporting System (WDPRS) will be available to those who wish to file WHOIS inaccuracy reports, as per ICANN policy (http://wdprs.internic.net/).

CONTROLS TO ENSURE PROPER ACCESS TO DOMAIN FUNCTIONS

Several measures are in place in the Afilias registry system to ensure proper access to domain functions, including authentication provisions in the RRA relative to notification and contact updates via use of AUTH-INFO codes.

IP address access control lists, TLS/SSL certificates and proper authentication are used to control access to the registry system. Registrars are only given access to perform operations on the objects they sponsor.

Every domain will have a unique AUTH-INFO code. The AUTH-INFO code is a 6- to 16-character code assigned by the registrar at the time the name is created. Its purpose is to aid identification of the domain owner so proper authority can be established. It is the "password" to the domain name. Registrars must use the domain's password in order to initiate a registrar-to-registrar transfer. It is used to ensure that domain updates (update contact information, transfer, or deletion) are undertaken by the proper registrant, and that this registrant is adequately notified of domain update activity. Only the sponsoring registrar of a domain has access to the domain's AUTH-INFO code stored in the registry, and this is accessible only via encrypted, password-protected channels.

Information about other registry security measures such as encryption and security of registrar channels are confidential to ensure the security of the registry system. The details can be found in the response to question #30b.

.ECO COMMUNITY ELIGIBILITY AND ABUSE PREVENTION AND MITIGATION

Before DNS resolution is permitted for their domain, .ECO registrants must demonstrate a commitment to the .ECO purpose, principles and policies by agreeing to the registrant agreement, which includes a commitment to the .ECO mission and purpose, affirmation of membership in the environmental community, and answering the mandatory .ECO-profile questions.

Registrants must complete a .ECO-profile that includes a series of mandatory and voluntary questions about commitments, memberships, certification, reporting and other activities undertaken in support of the Community's goals. Responses will form a .ECO-profile web page that will be added to a public online database called the .ECO System. Registrant .ECO-profiles will be linked to the Registrant's .ECO domain via a .ECO logo trust mark, like those in common use (eg, TRUSTe online privacy seal and VeriSign Trust Seal).

The registry will employ standard registration lifecycle mechanisms, statuses, and states such as HOLD or LOCK functions, or other existing Extensible Provisioning Protocol (EPP) commands, in order to disallow a domain to be active when a registrant is not in compliance with the community eligibility requirements or under related community dispute resolution procedures.

Accountability and abuse prevention: The Registry will layer community forums, online complaint and abuse reporting, dispute resolution, mediation, and arbitration as required to ensure policies are enforced in a transparent and accountable way. The Registry will engage the Dot ECO Global Community Organization on matters requiring broader policy decisions.

Beyond the baseline eligibility requirements, abuse prevention and mitigation measures will include:

* Spot checks: reviewing a percent of .ECO-profiles to ensure compliance.
* Risk based audits: reviewing .ECO-profile disclosures (eligibility disclosures) for industries, sectors, or registrant types which are identified as having higher risk of abuse
* Verified .ECO-profiles: verified .ECO-profiles will be offered for a fee (via an internal or outsourced service), akin to the 'Twitter Verified' program, to increase accuracy and further reduce abuse. (See Twitter: FAQ about Verified Accounts: http://goo.gl/WHA7y).
* Community member flagging / comment: If the user believes that a domain is inconsistent with the mission and purpose of the .ECO Community TLD, s/he may 'flag' the domain for review, using the 'flag for review' functionality on the .ECO-profile page. Such 'flagged' domains will be queued for review and assessed as appropriate.

These layers are explained in an Accountability Policy of the .ECO Policy Consensus.

Dispute Resolution Mechanisms: Registrants and rights holders will have access to fair and transparent processes to adjudicate claims to domains that also protect registrants against reverse domain hijacking. Names registered in the Sunrise Period will be subject to a Sunrise Dispute Policy. This policy and procedure will be in effect for a finite time period, to provide special protection of qualified trademark rights. See response to #29 ("Rights Protection Mechanisms").

.ECO domains will be subject to the Uniform Dispute Resolution Policy (UDRP). See response to #29 ("Rights Protection Mechanisms").

.ECO domains will also be subject to the Universal Rapid Suspension (URS) policy. See the URS specifications in Applicant Guidebook Module and response #29 ("Rights Protection Mechanisms") for full details. The Registry will provide systems to take in and administrate cases as per ICANN's Registrar Transfer Dispute Resolutions Policy, allowing registrars to protect registrants by filing disputes about inter-registrar transfers that they believe were unauthorized or improperly executed.

The Registry will support a Community Eligibility Dispute Resolution Process (CEDRP) aligned with the Accountability Policy described in the .ECO Policy Consensus. This dispute process can be initiated by either a member of the .ECO community or a member of the general public to address an alleged violation of the .ECO member policies or operating requirements by a registrant or registrar.

Please see responses #18(b), #20(e) for a description of community eligibility and registration requirements for the .ECO Community TLD.

VALIDATION AND ABUSE MITIGATION MECHANISMS

Afilias has developed advanced validation and abuse mitigation mechanisms. These capabilities and mechanisms are described below. These services and capabilities are discretionary and may be utilized by the registry operator based on their policy and business need.

Afilias has the ability to analyze the registration data for known patterns at the time of registration. A database of these known patterns is developed from domains and other associated objects (e.g., contact information) which have been previously detected and suspended after being flagged as abusive. Any domains matching the defined criteria can be flagged for investigation. Once analyzed and confirmed by the domain anti-abuse team members, these domains may be suspended. This provides proactive detection of abusive domains.

Provisions are available to enable the registry operator to only allow registrations by pre-authorized and verified contacts. These verified contacts are given a unique code that can be used for registration of new domains.

REGISTRANT PRE-VERIFICATION AND AUTHENTICATION

One of the systems that could be used for validity and identity authentication is VAULT (Validation and Authentication Universal Lookup). It utilizes information obtained from a series of trusted data sources with access to billions of records containing data about individuals for the purpose of providing independent age and id verification as well as the ability to incorporate additional public or private data sources as required. At present it has the following: US Residential Coverage - 90% of Adult Population and also International Coverage - Varies from Country to Country with a minimum of 80% coverage (24 countries, mostly European).

Various verification elements can be used. Examples might include applicant data such as name, address, phone, etc. Multiple methods could be used for verification include integrated solutions utilizing API (XML Application Programming Interface) or sending batches of requests.

* Verification and Authentication requirements would be based on TLD operator requirements or specific criteria.
* Based on required WHOIS Data; registrant contact details (name, address, phone)
* If address/ZIP can be validated by VAULT, the validation process can continue (North America +25 International countries)
* If in-line processing and registration and EPP/API call would go to the verification clearinghouse and return up to 4 challenge questions.
* If two-step registration is required, then registrants would get a link to complete the verification at a separate time. The link could be specific to a domain registration and pre-populated with data about the registrant.
* If WHOIS data is validated a token would be generated and could be given back to the registrar which registered the domain.
* WHOIS data would reflect the Validated Data or some subset, i.e., fields displayed could be first initial and last name, country of registrant and date validated. Other fields could be generic validation fields much like a “privacy service”.
* A “Validation Icon” customized script would be sent to the registrants email address. This could be displayed on the website and would be dynamically generated to avoid unauthorized use of the Icon. When clicked on the Icon would should limited WHOIS details i.e. Registrant: jdoe, Country: USA, Date Validated: March 29, 2011, as well as legal disclaimers.
* Validation would be annually renewed, and validation date displayed in the WHOIS.

ABUSE PREVENTION RESOURCING PLANS

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way. Abuse prevention and detection is a function that is staffed across the various groups inside Afilias, and requires a team effort when abuse is either well hidden or widespread, or both. While all of Afilias’ 200+ employees are charged with responsibility to report any detected abuse, the engineering and analysis teams, numbering over 30, provide specific support based on the type of abuse and volume and frequency of analysis required. The Afilias security and support teams have the authority to initiate mitigation.

Afilias has developed advanced validation and abuse mitigation mechanisms. These capabilities and mechanisms are described below. These services and capabilities are discretionary and may be utilized by the registry operator based on their policy and business need.

The .ECO TLD’s anticipated volume of registrations in the first three years of operations is listed in response #46. Afilias and the registry operator’s anti-abuse function anticipates the expected volume and type of registrations, and together will adequately cover the staffing needs for this TLD. The registry operator will maintain an abuse response team, which may be a combination of internal staff and outside specialty contractors, adjusting to the needs of the size and type of TLD. The team structure planned for this TLD is based on several years of experience responding to, mitigating, and managing abuse for TLDs of various sizes. The team will generally consist of abuse handlers (probably internal), a junior analyst, (either internal or external), and a senior security consultant (likely an external resource providing the registry operator with extra expertise as needed). These responders will be specially trained in the investigation of abuse complaints, and will have the latitude to act expeditiously to suspend domain names (or apply other remedies) when called for.

The exact resources required to maintain an abuse response team must change with the size and registration procedures of the TLD. An initial abuse handler is necessary as a point of contact for reports, even if a part-time responsibility. The abuse handlers monitor the abuse email address for complaints and evaluate incoming reports from a variety of sources. A large percentage of abuse reports to the registry operator may be unsolicited commercial email. The designated abuse handlers can identify legitimate reports and then decide what action is appropriate, either to act upon them, escalate to a security analyst for closer investigation, or refer them to registrars as per the above-described procedures. A TLD with rare cases of abuse would conform to this structure.

If multiple cases of abuse within the same week occur regularly, the registry operator will consider staffing internally a security analyst to investigate the complaints as they become more frequent. Training an abuse analyst requires 3-6 months and likely requires the active guidance of an experienced senior security analyst for guidance and verification of assessments and recommendations being made.

If this TLD were to regularly experience multiple cases of abuse within the same day, a full-time senior security analyst would likely be necessary. A senior security analyst capable of fulfilling this role should have several years of experience and able to manage and train the internal abuse response team.

The abuse response team will also maintain subscriptions for several security information services, including the blocklists from organizations like SURBL and Spamhaus and anti-phishing and other domain related abuse (malware, fast-flux etc.) feeds. The pricing structure of these services may depend on the size of the domain and some services will include a number of rapid suspension requests for use as needed.

For a large TLD, regular audits of the registry data are required to maintain control over abusive registrations. When a registrar with a significant number of registrations has been compromised or acted maliciously, the registry operator may need to analyze a set of registration or DNS query data. A scan of all the domains of a registrar is conducted only as needed. Scanning and analysis for a large registrar may require as much as a week of full-time effort for a dedicated machine and team.

Big Room will maintain sufficient staff resources to implement identified abuse mitigation and prevention measures, respond to issues as they arise, and coordinate tier

1 and escalated abuse issues with Afilias. As necessary additional support will be outsourced or contracted in line with registry growth. Please see response #47 for a description of the Community and Policy Director, Customer Service Coordinator, Verification Coordinator, and Customer Support Assistant who are planned for years 1-3 of startup in support of these functions.

29. Rights Protection Mechanisms

Rights protection is a core responsibility of the TLD operator, and is supported by a fully-developed plan for rights protection that includes:
* Establishing mechanisms to prevent unqualified registrations (e.g., registrations made in violation of the registry’s eligibility restrictions or policies);
* Implementing a robust Sunrise program, utilizing the Trademark Clearinghouse, the services of one of ICANN’s approved dispute resolution providers, a trademark validation agent, and drawing upon sunrise policies and rules used successfully in previous gTLD launches;
* Implementing a professional trademark claims program that utilizes the Trademark Clearinghouse, and drawing upon models of similar programs used successfully in previous TLD launches;
* Complying with the URS requirements;
* Complying with the UDRP;
* Complying with the PDDRP, and;
* Including all ICANN-mandated and independently developed rights protection mechanisms (“RPMs”) in the registry-registrar agreement entered into by ICANN-accredited registrars authorized to register names in the TLD.

The response below details the rights protection mechanisms at the launch of the TLD (Sunrise and Trademark Claims Service) which comply with rights protection policies (URS, UDRP, PDDRP, and other ICANN RPMs), outlines additional provisions made for rights protection, and provides the resourcing plans.

Safeguards for rights protection at the launch of the TLD

The launch of this TLD will include the operation of a trademark claims service according to the defined ICANN processes for checking a registration request and alerting trademark holders of potential rights infringement.

Sunrise period

The Registry will provide a fair opportunity for environmental community members to register for .ECO while also minimizing related costs to rights holders.

The Sunrise Period will last a minimum period of 1 month, prior to the opening of public registration, when trademark and service mark holders will be able to reserve marks that are an identical match in the .ECO domain. Following the Sunrise Period, Big Room will open registration to qualified applicants.

The first phase will run for a limited time period prior to the Land-rush and General Availability phases. In the past, Sunrise periods have been used in the launch of numerous TLDs including .INFO, .BIZ, .MOBI, .TEL, .ME, .XXX and others. These efforts have proven the need for a balanced approach that provides intellectual property (IP) holders, as well as an opportunity to register names they feel apply to their IP.

Big Room will hold a Sunrise period where holders of internationally recognized filed trademarks or possibly holders of existing (legacy) gTLD strings that are a perfect match to the .ECO string that they are applying for, will have the opportunity to apply for registration. A qualified third party must verify each trademark and/or legacy gTLD. In addition, the applicant must have a completed .ECO-profile and meet all criteria in order to be accepted as a community member. No application will be accepted without these verifications.

Big Room plans to use the Trademark Clearinghouse to asynchronously check Sunrise applications against registered trademarks. If the trademark is verified and valid, we expect to be able to inform the IP holder that a Sunrise application for their string has been submitted. IP holders are only involved if an application is submitted that is an exact match to their registered trademark.

An auction process will determine the awarding party in the event that there is more than one valid Sunrise application for a given string.

Community-priority & Platform names

Related to the sunrise phase is handling of specific types of names aimed at serving the community, including:

1. Premium Names, including those that could have added community value, in two categories:

A) Community-priority: Prior to launch, the Organization will approve a list of community-priority names. The Registry will, with Organization input, develop rules for a best-use plan competition. Names allocated in the competition will be donated to the winners. All community-priority names will be reviewed biennially by the Registry against their use-plans.

B) Auction-able: The Registry will also publish a list of names available for auction during sunrise. Funds generated from these names will be used to support the Registry.

2. Platform Names: The Registry will reserve a list of names that may be useful to the .ECO System, such as: industry sectors (eg, transportation); environmental issues (e.g. biodiversity); nouns with environmental significance (eg, water); and, other names deemed technically useful to the Registry’s implementation of .ECO as a community TLD (eg, Council).

Sunrise Period Requirements & Restrictions

Those wishing to reserve their marks in the .ECO domain during the Sunrise Period must own a current trademark or service mark listed in the Trademark Clearinghouse or submit evidence of a Trademark of national effect during the application process. Acceptable criteria for submitted Trademarks are modeled directly from the Trademark Clearinghouse guidelines:

“Nationally or regionally registered word marks from all jurisdictions.

- Any word mark that has been validated through a court of law or other judicial proceeding.
- Any word mark protected by a statute or treaty in effect at the time the mark is submitted to the Clearinghouse for inclusion.
- Other marks that constitute intellectual property.
- Protections afforded to trademark registrations do not extend to applications for registrations, marks within any opposition period or registered marks that were the subject of successful invalidation, cancellation or rectification proceedings.”

Notice will be provided to all trademark holders in the Clearinghouse if someone is seeking a Sunrise registration. This notice will be provided to holders of marks in the Clearinghouse that are an Identical Match (as defined in the Trademark Clearing House) to the name to be registered during Sunrise.

Each Sunrise registration will require a minimum term of five years.

Big Room will establish the following Sunrise eligibility requirements (SERs) as minimum requirements, verified by Clearinghouse data, and incorporate a Sunrise Dispute

Resolution Policy (SDRP). The SERs include: (i) ownership of a mark that satisfies the criteria set forth in section 7.2 of the Trademark Clearing House specifications, (ii) description of international class of goods or services covered by registration; (iii) representation that all provided information is true and correct; and (iv) provision of data sufficient to document rights in the trademark.

The SDRP will allow challenges based on the following four grounds: (i) at time the challenged domain name was registered, the registrants did not hold a trademark registration of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; (ii) the domain name is not identical to the mark on which the registrant based its Sunrise registration; (iii) the trademark registration on which the registrant based its Sunrise registration is not of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; or (iv) the trademark registration on which the domain name registrant based its Sunrise registration did not issue on or before the effective date of the Registry Agreement and was not applied for on or before ICANN announced the applications received.

Ongoing rights protection mechanisms

Several mechanisms will be in place to protect rights in this TLD. As described in our responses to questions #27 and #28, measures are in place to ensure domain transfers and updates are only initiated by the appropriate domain holder, and an experienced team is available to respond to legal actions by law enforcement or court orders.

This TLD will conform to all ICANN RPMs including URS (defined below), UDRP, PDDRP, and all measures defined in Specification 7 of the new TLD agreement.

Uniform Rapid Suspension (URS)

The registry operator will implement decisions rendered under the URS on an ongoing basis. Per the URS policy posted on ICANN’s Web site as of this writing, the registry operator will receive notice of URS actions from the ICANN-approved URS providers. These emails will be directed immediately to the registry operator’s support staff, which is on duty 24x7. The support staff will be responsible for creating a ticket for each case, and for executing the directives from the URS provider. All support staff will receive pertinent training.

As per ICANN’s URS guidelines, within 24 hours of receipt of the notice of complaint from the URS provider, the registry operator shall “lock” the domain, meaning the registry shall restrict all changes to the registration data, including transfer and deletion of the domain names, but the name will remain in the TLD DNS zone file and will thus continue to resolve. The support staff will “lock” the domain by associating the following EPP statuses with the domain and relevant contact objects:
* ServerUpdateProhibited, with an EPP reason code of “URS”
* ServerDeleteProhibited, with an EPP reason code of “URS”
* ServerTransferProhibited, with an EPP reason code of “URS”
* The registry operator’s support staff will then notify the URS provider immediately upon locking the domain name, via email.

The registry operator’s support staff will retain all copies of emails from the URS providers, assign them a tracking or ticket number, and will track the status of each opened URS case through to resolution via spreadsheet or database.

The registry operator’s support staff will execute further operations upon notice from the URS providers. The URS provider is required to specify the remedy and required actions of the registry operator, with notification to the registrant, the complainant, and the registrar.

As per the URS guidelines, if the complainant prevails, the “registry operator shall suspend the domain name, which shall remain suspended for the balance of the registration period and would not resolve to the original web site. The nameservers shall be redirected to an informational web page provided by the URS provider about the URS. The WHOIS for the domain name shall continue to display all of the information of the original registrant except for the redirection of the nameservers. In addition, the WHOIS shall reflect that the domain name will not be able to be transferred, deleted or modified for the life of the registration.”

Community TLD considerations

Unqualified registrations (registrations in violation of the registry’s eligibility restrictions or policies)

Before DNS resolution is permitted for their domain, .ECO registrants must demonstrate a commitment to the .ECO purpose, principles and policies by agreeing to the registrant agreement, which includes a commitment to the .ECO mission and purpose, affirmation of membership in the environmental community, and answering the mandatory .ECO-profile questions.

Registrants must complete a .ECO-profile that includes a series of mandatory and voluntary questions about commitments, memberships, certification, reporting and other activities undertaken in support of the Community’s goals. Responses will form a .ECO-profile web page that will be added to a public online database called the .ECO System. Registrant .ECO-profiles will be linked to the Registrant’s .ECO domain via a .ECO logo trust mark, like those in common use (eg, TRUSTe online privacy seal and VeriSign Trust Seal).

The registry will employ standard registration lifecycle mechanisms, statuses, and states such as HOLD or LOCK functions, or other existing Extensible Provisioning Protocol (EPP) commands, in order to disallow a domain to be active when a registrant is not in compliance with the community eligibility requirements or under related community dispute resolution procedures.

Accountability and abuse prevention: The Registry will layer community forums, online complaint and abuse reporting, dispute resolution, mediation, and arbitration as required to ensure policies are enforced in a transparent and accountable way. The Registry will engage the Dot Eco Global Community Organization on matters requiring broader policy decisions.

Beyond the baseline eligibility requirements, abuse prevention and mitigation measures will include:

* Spot checks: reviewing a percent of .ECO-profiles to ensure compliance.
* Risk based audits: reviewing .ECO-profile disclosures (eligibility disclosures) for industries, sectors, or registrant types which are identified as having higher risk of abuse
* Verified .ECO-profiles: verified .ECO-profiles will be offered for a fee (via an internal or outsourced service), akin to the ‘Twitter Verified’ program, to increase accuracy and further reduce abuse. (See Twitter: FAQ about Verified Accounts: http://goo.gl/WHA7y).
* Community member flagging / comment: If the user believes that a domain is inconsistent with the mission and purpose of the .ECO Community TLD, s/he may ‘flag’ the domain for review, using the ‘flag for review’ functionality on the .ECO-profile page. Such ‘flagged’ domains will be queued for review and assessed as appropriate.

Rights protection or other disputes

Dispute Resolution Mechanisms: Registrants and rights holders will have access to fair and transparent processes to adjudicate claims to domains that also protect registrants against reverse domain hijacking. Names registered in the Sunrise Period will be subject to a Sunrise Dispute Policy. This policy and procedure will be in effect for a finite time period, to provide special protection of qualified trademark rights. See response to #29 (“Rights Protection Mechanisms”).

.ECO domains will be subject to the Uniform Dispute Resolution Policy (UDRP).

.ECO domains will also be subject to the Universal Rapid Suspension (URS) policy. See the URS specifications in Applicant Guidebook Module and response #29 (“Rights Protection Mechanisms”) for full details. The Registry will provide systems to take in and administrate cases as per ICANN’s Registrar Transfer Dispute Resolutions Policy, allowing registrars to protect registrants by filing disputes about inter-registrar transfers that they believe were unauthorized or improperly executed.

The Registry will support a Community Eligibility Dispute Resolution Process (CEDRP) aligned with the Accountability Policy described in the .ECO Policy Consensus. This dispute process can be initiated by either a member of the .ECO community or a member of the general public to address an alleged violation of the .ECO member policies or operating requirements by a registrant or registrar.

Please see responses #18(b), #20(e) for a description of community eligibility and registration requirements for the .ECO Community TLD, and response #28 for a review of abuse prevention and mitigation.

Rights protection via the RRA

The following will be memorialized and be made binding via the Registry-Registrar and Registrar-Registrant Agreements:

* The registry may reject a registration request or a reservation request, or may delete, revoke, suspend, cancel, or transfer a registration or reservation under the following criteria:
a. to enforce registry policies and ICANN requirements; each as amended from time to time;
b. that is not accompanied by complete and accurate information as required by ICANN requirements and/or registry policies or where required information is not updated and/or corrected as required by ICANN requirements and/or registry policies;
c. to protect the integrity and stability of the registry, its operations, and the TLD system;
d. to comply with any applicable law, regulation, holding, order, or decision issued by a court, administrative authority, or dispute resolution service provider with jurisdiction over the registry;
e. to establish, assert, or defend the legal rights of the registry or a third party or to avoid any civil or criminal liability on the part of the registry and/or its affiliates, subsidiaries, officers, directors, representatives, employees, contractors, and stockholders;
f. to correct mistakes made by the registry or any accredited registrar in connection with a registration; or
g. as otherwise provided in the Registry-Registrar Agreement and/or the Registrar-Registrant Agreement.

Reducing opportunities for behaviors such as phishing or pharming

In our response to question #28, the registry operator has described its anti-abuse program. Rather than repeating the policies and procedures here, please see our response to question #28 for full details.

In the case of this TLD, Big Room will apply an approach that addresses registered domain names (rather than potentially registered domains). This approach will not infringe upon the rights of eligible registrants to register domains, and allows Big Room internal controls, as well as community-developed UDRP and URS policies and procedures if needed, to deal with complaints, should there be any.

Afilias is a member of various security fora which provide access to lists of names in each TLD which may be used for malicious purposes. Such identified names will be subject to the TLD anti-abuse policy, including rapid suspensions after due process.

Rights protection resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Supporting RPMs requires several departments within the registry operator as well as within Afilias. The implementation of Sunrise and the Trademark Claims service and on-going RPM activities will pull from the 102 Afilias staff members of the engineering, product management, development, security and policy teams at Afilias and the support staff of the registry operator, which is on duty 24x7. A trademark validator will also be assigned within the registry operator, whose responsibilities may require as much as 50% of full-time employment if the domains under management were to exceed several million. No additional hardware or software resources are required to support this as Afilias has fully-operational capabilities to manage abuse today.

Big Room will maintain sufficient staff resources to implement identified abuse mitigation and prevention measures, rights protection mechanisms, and respond to issues as they arise. As necessary additional support will be outsourced or contracted in line with registry growth. Please see response #47 for a description of the Community and Policy Director, Customer Service Coordinator, Verification Coordinator, and Customer Support Assistant who are planned for years 1-3 of startup in support of these functions.

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

The answer to question #30a is provided by Afilias, the back-end provider of registry services for the .ECO Community TLD.

Afilias aggressively and actively protects the registry system from known threats and vulnerabilities, and has deployed an extensive set of security protocols, policies and procedures to thwart compromise. Afilias’ robust and detailed plans are continually updated and tested to ensure new threats are mitigated prior to becoming issues. Afilias will continue these rigorous security measures, which include:
* Multiple layers of security and access controls throughout registry and support systems;
* 24x7 monitoring of all registry and DNS systems, support systems and facilities;
* Unique, proven registry design that ensures data integrity by granting only authorized access to the registry system, all while meeting performance requirements;
* Detailed incident and problem management processes for rapid review, communications, and problem resolution, and;
* Yearly external audits by independent, industry-leading firms, as well as twice-yearly internal audits.

SECURITY POLICIES AND PROTOCOLS

Afilias has included security in every element of its service, including facilities, hardware, equipment, connectivity/Internet services, systems, computer systems, organizational security, outage prevention, monitoring, disaster mitigation, and escrow/insurance, from the original design, through development, and finally as part of production deployment. Examples of threats and the confidential and proprietary mitigation procedures are detailed in our response to question #30(b).

There are several important aspects of the security policies and procedures to note:
* Afilias hosts domains in data centers around the world that meet or exceed global best

practices.
* Afilias’ DNS infrastructure is massively provisioned as part of its DDoS mitigation strategy, thus ensuring sufficient capacity and redundancy to support new gTLDs.
* Diversity is an integral part of all of our software and hardware stability and robustness plan, thus avoiding any single points of failure in our infrastructure.
* Access to any element of our service (applications, infrastructure and data) is only provided on an as-needed basis to employees and a limited set of others to fulfill their job functions. The principle of least privilege is applied.
* All registry components – critical and non-critical – are monitored 24x7 by staff at our NOCs, and the technical staff has detailed plans and procedures that have stood the test of time for addressing even the smallest anomaly. Well-documented incident management procedures are in place to quickly involve the on-call technical and management staff members to address any issues.

Afilias follows the guidelines from the ISO 27001 Information Security Standard (Reference: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103) for the management and implementation of its Information Security Management System. Afilias also utilizes the COBIT IT governance framework to facilitate policy development and enable controls for appropriate management of risk (Reference: http://www.isaca.org/cobit). Best practices defined in ISO 27002 are followed for defining the security controls within the organization. Afilias continually looks to improve the efficiency and effectiveness of our processes, and follows industry best practices as defined by the IT Infrastructure Library, or ITIL (Reference: http://www.itil-officialsite.com/).

The Afilias registry system is located within secure data centers that implement a multitude of security measures both to minimize any potential points of vulnerability and to limit any damage should there be a breach. The characteristics of these data centers are described fully in our response to question #30(b).

The Afilias registry system employs a number of multi-layered measures to prevent unauthorized access to its network and internal systems. Before reaching the registry network, all traffic is required to pass through a firewall system. Packets passing to and from the Internet are inspected, and unauthorized or unexpected attempts to connect to the registry servers are both logged and denied. Management processes are in place to ensure each request is tracked and documented, and regular firewall audits are performed to ensure proper operation. 24x7 monitoring is in place and, if potential malicious activity is detected, appropriate personnel are notified immediately.

Afilias employs a set of security procedures to ensure maximum security on each of its servers, including disabling all unnecessary services and processes and regular application of security-related patches to the operating system and critical system applications. Regular external vulnerability scans are performed to verify that only services intended to be available are accessible.

Regular detailed audits of the server configuration are performed to verify that the configurations comply with current best security practices. Passwords and other access means are changed on a regular schedule and are revoked whenever a staff member’s employment is terminated.

Access to registry system

Access to all production systems and software is strictly limited to authorized operations staff members. Access to technical support and network operations teams where necessary are read only and limited only to components required to help troubleshoot customer issues and perform routine checks. Strict change control procedures are in place and are followed each time a change is required to the production hardware/application. User rights are kept to a minimum at all times. In the event of a staff member’s employment termination, all access is removed immediately.

Afilias applications use encrypted network communications. Access to the registry server is controlled. Afilias allows access to an authorized registrar only if each of the authentication factors matches the specific requirements of the requested authorization. These mechanisms are also used to secure any web-based tools that allow authorized registrars to access the registry. Additionally, all write transactions in the registry (whether conducted by authorized registrars or the registry′s own personnel) are logged.

EPP connections are encrypted using TLS/SSL, and mutually authenticated using both certificate checks and login/password combinations. Web connections are encrypted using TLS/SSL for an encrypted tunnel to the browser, and authenticated to the EPP server using login/password combinations.

All systems are monitored for security breaches from within the data center and without, using both system-based and network-based testing tools. Operations staff also monitor systems for security-related performance anomalies. Triple-redundant continual monitoring ensures multiple detection paths for any potential incident or problem. Details are provided in our response to questions #30(b) and #42. Network Operations and Security Operations teams perform regular audits in search of any potential vulnerability.

To ensure that registrar hosts configured erroneously or maliciously cannot deny service to other registrars, Afilias uses traffic shaping technologies to prevent attacks from any single registrar account, IP address, or subnet. This additional layer of security reduces the likelihood of performance degradation for all registrars, even in the case of a security compromise at a subset of registrars.

There is a clear accountability policy that defines what behaviors are acceptable and unacceptable on the part of non-staff users, staff users, and management. Periodic audits of policies and procedures are performed to ensure that any weaknesses are discovered and addressed. Aggressive escalation procedures and well-defined Incident Response management procedures ensure that decision makers are involved at early stages of any event.

In short, security is a consideration in every aspect of business at Afilias, and this is evidenced in a track record of a decade of secure, stable and reliable service.

INDEPENDENT ASSESSMENT

Supporting operational excellence as an example of security practices, Afilias performs a number of internal and external security audits each year of the existing policies, procedures and practices for:
* Access control;
* Security policies;
* Production change control;
* Backups and restores;
* Batch monitoring;
* Intrusion detection, and
* Physical security.

Afilias has an annual Type 2 SSAE 16 audit performed by PricewaterhouseCoopers (PwC). Further, PwC performs testing of the general information technology controls in support of the financial statement audit. A Type 2 report opinion under SSAE 16 covers whether the controls were properly designed, were in place, and operating effectively during the audit period (calendar year). This SSAE 16 audit includes testing of internal controls relevant to Afilias′ domain registry system and processes. The report includes testing of key controls related to the following control objectives:
* Controls provide reasonable assurance that registrar account balances and changes to the registrar account balances are authorized, complete, accurate and timely.
* Controls provide reasonable assurance that billable transactions are recorded in the Shared Registry System (SRS) in a complete, accurate and timely manner.
* Controls provide reasonable assurance that revenue is systemically calculated by the Deferred Revenue System (DRS) in a complete, accurate and timely manner.
* Controls provide reasonable assurance that the summary and detail reports, invoices, statements, registrar and registry billing data files, and ICANN transactional reports provided to registry operator(s) are complete, accurate and timely.
* Controls provide reasonable assurance that new applications and changes to existing

applications are authorized, tested, approved, properly implemented and documented.
* Controls provide reasonable assurance that changes to existing system software and implementation of new system software are authorized, tested, approved, properly implemented and documented.
* Controls provide reasonable assurance that physical access to data centers is restricted to properly authorized individuals.
* Controls provide reasonable assurance that logical access to system resources is restricted to properly authorized individuals.
* Controls provide reasonable assurance that processing and backups are appropriately authorized and scheduled and that deviations from scheduled processing and backups are identified and resolved.

The last Type 2 report issued was for the year 2010, and it was unqualified, i.e., all systems were evaluated with no material problems found.

During each year, Afilias monitors the key controls related to the SSAE controls. Changes or additions to the control objectives or activities can result due to deployment of new services, software enhancements, infrastructure changes or process enhancements. These are noted and after internal review and approval, adjustments are made for the next review.

In addition to the PricewaterhouseCoopers engagement, Afilias performs internal security audits twice a year. These assessments are constantly being expanded based on risk assessments and changes in business or technology.

Additionally, Afilias engages an independent third-party security organization, PivotPoint Security, to perform external vulnerability assessments and penetration tests on the sites hosting and managing the Registry infrastructure. These assessments are performed with major infrastructure changes, release of new services or major software enhancements. These independent assessments are performed at least annually. A report from a recent assessment is attached with our response to question #30(b).

Afilias has engaged with security companies specializing in application and web security testing to ensure the security of web-based applications offered by Afilias, such as the Web Admin Tool (WAT) for registrars and registry operators.

Finally, Afilias has engaged IBM’s Security services division to perform ISO 27002 gap assessment studies so as to review alignment of Afilias’ procedures and policies with the ISO 27002 standard. Afilias has since made adjustments to its security procedures and policies based on the recommendations by IBM.

SPECIAL TLD CONSIDERATIONS

Afilias’ rigorous security practices are regularly reviewed; if there is a need to alter or augment procedures for the .ECO Community TLD, they will be done so in a planned and deliberate manner. No new procedures are currently anticipated.

COMMITMENTS TO REGISTRANT PROTECTION

With over a decade of experience protecting domain registration data, Afilias understands registrant security concerns. Afilias supports a “thick” registry system in which data for all objects are stored in the registry database that is the centralized authoritative source of information. As an active member of IETF (Internet Engineering Task Force), ICANN’s SSAC (Security & Stability Advisory Committee), APWG (Anti-Phishing Working Group), MAAWG (Messaging Anti-Abuse Working Group), USENIX, and ISACA (Information Systems Audits and Controls Association), the Afilias team is highly attuned to the potential threats and leading tools and procedures for mitigating threats. As such, registrants should be confident that:
* Any confidential information stored within the registry will remain confidential;
* The interaction between their registrar and Afilias is secure;
* The Afilias DNS system will be reliable and accessible from any location;
* The registry system will abide by all polices, including those that address registrant

data;
* Afilias will not introduce any features or implement technologies that compromise access to the registry system or that compromise registrant security.

Afilias has directly contributed to the development of the documents listed below and we have implemented them where appropriate. All of these have helped improve registrants' ability to protect their domains name(s) during the domain name lifecycle.
* [SAC049]: SSAC Report on DNS Zone Risk Assessment and Management (03 June 2011)
* [SAC044]: A Registrant's Guide to Protecting Domain Name Registration Accounts (05 November 2010)
* [SAC040]: Measures to Protect Domain Registration Services Against Exploitation or Misuse (19 August 2009)
* [SAC028]: SSAC Advisory on Registrar Impersonation Phishing Attacks (26 May 2008)
* [SAC024]: Report on Domain Name Front Running (February 2008)
* [SAC022]: Domain Name Front Running (SAC022, SAC024) (20 October 2007)
* [SAC011]: Problems caused by the non-renewal of a domain name associated with a DNS Name Server (7 July 2006)
* [SAC010]: Renewal Considerations for Domain Name Registrants (29 June 2006)
* [SAC007]: Domain Name Hijacking Report (SAC007) (12 July 2005)

To protect any unauthorized modification of registrant data, Afilias mandates TLS/SSL transport (per RFC 5246) and authentication methodologies for access to the registry applications. Authorized registrars are required to supply a list of specific individuals (five to ten people) who are authorized to contact the registry. Each such individual is assigned a pass phrase. Any support requests made by an authorized registrar to registry customer service are authenticated by registry customer service. All failed authentications are logged and reviewed regularly for potential malicious activity. This prevents unauthorized changes or access to registrant data by individuals posing to be registrars or their authorized contacts.

These items reflect an understanding of the importance of balancing data privacy and access for registrants, both individually and as a collective, worldwide user base.

The Afilias 24/7 Customer Service Center consists of highly trained staff who collectively are proficient in 15 languages, and who are capable of responding to queries from registrants whose domain name security has been compromised – for example, a victim of domain name hijacking. Afilias provides specialized registrant assistance guides, including specific hand-holding and follow-through in these kinds of commonly occurring circumstances, which can be highly distressing to registrants

SECURITY RESOURCING PLANS

Please refer to our response to question #30b for security resourcing plans.

BIG ROOM (.ECO REGISTRY OPERATOR) SECURITY POLICY

Big Room maintains a security policy which is commensurate to the nature of the .ECO Community TLD, and which complements the Afilias security policy. In the event that Big Room becomes the .ECO registry operator, we will develop, implement, and appropriately resource the necessary security policy, processes, and infrastructure required to complement those of our registry service provider.

Key elements of Big Room's existing security plan as they relate to vital business functions are outlined in 30(b).

Annex 5.

New gTLD Program
Community Priority Evaluation Report
Report Date: 6 October 2014

Application ID:	1-912-59314
Applied-for String:	ECO
Applicant Name:	Big Room Inc.

Overall Community Priority Evaluation Summary

Community Priority Evaluation Result — **Prevailed**

Thank you for your participation in the New gTLD Program. After careful consideration and extensive review of the information provided in your application, including documents of support, the Community Priority Evaluation panel determined that the application met the requirements specified in the Applicant Guidebook. Your application prevailed in Community Priority Evaluation.

Panel Summary

Overall Scoring — 14 Point(s)

Criteria	Earned	Achievable
#1: Community Establishment	4	4
#2: Nexus between Proposed String and Community	3	4
#3: Registration Policies	4	4
#4: Community Endorsement	3	4
Total	14	16

Minimum Required Total Score to Pass 14

Criterion #1: Community Establishment — 4/4 Point(s)

1-A Delineation — ***2/2 Point(s)***

The Community Priority Evaluation panel has determined that the community as defined in the application met the criterion for Delineation as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook (AGB), as the community defined in the application is clearly delineated, organized and pre-existing. The application received the maximum score of 2 points under criterion 1-A: Delineation.

Delineation

Two conditions must be met to fulfill the requirements for delineation: there must be a clear straightforward membership definition and there must be awareness and recognition of a community (as defined by the applicant) among its members.

The community defined in the application ("ECO") is as follows:

> Members of the Community are delineated from Internet users generally by community-recognized memberships, accreditations, registrations, and certifications that demonstrate active commitment, practice and reporting.

> Community members include:
>
> Relevant not-for-profit environmental organizations (ie, accredited by relevant United Nations (UN) bodies; International Union for Conservation of Nature (IUCN) member; proof of not-for-profit legal entity status with documented environmental mission).
>
> Businesses (ie, members of environmental organizations; UN Global Compact participants; hold internationally-recognized environmental certifications; report to a global sustainability standard).
>
> Government agencies with environmental missions (ie, UN bodies, national⁄sub-national government agencies with environmental responsibilities).
>
> Individuals (ie, members of environmental organizations; academics; certified environmental professionals).

This community definition shows a clear and straightforward membership and is therefore well defined. Membership is determined through formal membership, certification, accreditation and/or a clearly defined mission, a transparent and verifiable membership structure that adequately meets the AGB criteria. Individuals' and organizations' association with, and membership in, the defined community can be verified by way of (1) membership in environmental organizations or certifiable practice in relevant fields in the case of individuals; or (2) accreditation, certification, or environmental mission in the case of organizations. In all cases, the application's membership definition depends on a transparent, explicit, and formal affiliation to an entity with an environmental focus.

In addition, the community as defined in the application has awareness and recognition among its members. According to the application:

> The Community has historically structured and organized itself and its work through an international network of organizations, including millions of individual members with strongly aligned goals, values and interests. As well as collaborating via long-standing international multi-stakeholder fora and membership organizations, members traditionally organize through multi-organization alliances around specific events, geographies, and issues.

According to the AGB, "community" implies "more of cohesion than a mere commonality of interest" and there should be "an awareness and recognition of a community among its members." Based on the Panel's research and materials provided in the application, the community members as defined in the application demonstrate the "cohesion" required by the AGB. The application dictates four types of members, whose cohesion and awareness is founded in their demonstrable involvement in environmental activities and who "demonstrate active commitment, practice and reporting." This involvement may vary among member categories as below:

Not-for-profit environmental organizations and government agencies with environmental missions: These entities must have a demonstrable mission that is directly associated with promoting environmental goals. Their mission and activities therefore align with the community-based purpose of the application, which is to foster transparency and communication in order to advance progress towards environmental goals.

Individuals: These may be members of the organizations included in the above grouping, or are academics or professionals whose degree, license, or other form of certification demonstrates that their area of work falls in a field related to the environment.

Businesses: These are businesses which may be members of one of the organizations referred to in the first grouping of members (such as the UN Global Compact), or have certified compliance with standards that are recognized by such organizations as showing commitment to environmental goals.

In all of the above cases, each individual or entity has a clear, public and demonstrable involvement in environmental activities. The interdependence and active commitment to shared goals among the various membership types are indicative of the "cohesion" that the AGB requires in a CPE-eligible community. The Panel found that entities included in the membership categories defined in the application are shown to cohere in their work towards clearly defined projects and goals that overlap among a wide array of member organizations. For example, Conservation International is a nonprofit organization that falls within the application's delineated community. It shows cohesion with the application's membership by way of its advocacy to and cooperation with both businesses[1] and governments[2] worldwide. Greenpeace, another such organization, has consultative status with the UN and actively involves its thousands of members, volunteers, and experts worldwide in its campaigns.[3] Furthermore, businesses that are included in the applicant's defined community have voluntarily opted to subject themselves to evaluation of their compliance with environmental standards that qualify them for the accreditations referenced in the application. As such, the defined community's membership is found to meet the AGB's standard for cohesion, required for an adequately delineated community.

The Community Priority Evaluation panel determined that the community as defined in the application satisfies both of the conditions to fulfill the requirements for Delineation.

Organization

Two conditions need to be met to fulfill the requirements for organization: there must be at least one entity mainly dedicated to the community, and there must be documented evidence of community activities.

The community as defined in the application has at least one entity mainly dedicated to the community. In fact, several entities are mainly dedicated to the community as defined by the application, such as the International Union for Conservation of Nature (IUCN), World Wide Fund For Nature (WWF), United Nations Environment Program and the Global Reporting Initiative, among others. According to the application:

> All the major international membership organizations (IUCN, WWF, Greenpeace, Friends of the Earth), the biggest global business and environment organizations (World Business Council for Sustainable Development (WBCSD), Green Economy Coalition), the largest international Community alliances (350.org, TckTckTck) and the key global environmental reporting standards (Global Reporting Initiative, Carbon Disclosure Project) support the creation of .ECO as a Community TLD. The United Nations Environment Programme (UNEP) has been an observer to the .ECO community process since 2010.
>
> As the world's largest and longest established organizations and alliances, these institutions represent over 190 countries, 1,000 entities, and more than 10 million individual members.

The international organizations like those above actively include elements from all the application's defined membership categories. The IUCN, for example, engages the private sector[4], individuals like environmental scientists[5], governmental agencies and other member organizations[6]. Its activities include the IUCN's World Conservation Congress that brings together its members, as well members of other organizations and government representatives.[7] The UN Global Compact similarly has regular events held worldwide where its affiliate organizations, governments and private sector partners come together in relation to the organization's environmental goals.[8] These organizational activities are representative of others that the Panel has reviewed that show ample evidence of the organized activity that the AGB requires of a community.

[1] http://www.conservation.org/how/pages/innovating-with-business.aspx
[2] http://www.conservation.org/how/pages/working-with-governments.aspx
[3] http://www.greenpeace.org/usa/en/campaigns/
[4] http://iucn.org/about/work/programmes/business/
[5] http://www.iucn.org/about/union/commissions/
[6] http://www.iucn.org/about/union/members/who_members/
[7] http://www.iucn.org/about/work/programmes/gpap_home/gpap_events/gpap_2012/
[8] https://www.unglobalcompact.org/NewsAndEvents/event_calendar/index.html

The Community Priority Evaluation panel determined that the community as defined in the application satisfies both of the conditions to fulfill the requirements for Organization.

Pre-existence
To fulfill the requirements for pre-existence, the community must have been active prior to September 2007 (when the new gTLD policy recommendations were completed).

The community as defined in the application was active prior to September 2007. The application presents the following as examples:

> 1948: First formal Community institution, the International Union for Conservation of Nature (IUCN), was established. Not-for-profit organizations, businesses and governments came together to address pressing environmental challenges. 1972: Global Environmental Community recognized by the world's governments on creation of the UN Environment Programme (UNEP), the UN's designated authority for addressing environmental issues at the global and regional level.

Many of the organizations that fall within the application's delineation have been active prior to 2007, including the UN Global Compact (founded in 2000)[9], Greenpeace (founded in 1971)[10], and others. The Panel has determined that since organizations like those referenced above are mainly dedicated to the members of the community as defined by the application, and since they and others were active prior to 2007, the community as defined in the application fulfills the requirements for Pre-existence.

1-B Extension ***2/2 Point(s)***

The Community Priority Evaluation panel determined that the community as identified in the application met the criterion for Extension specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the application demonstrates considerable size and longevity for the community. The application received a maximum score of 2 points under criterion 1-B: Extension.

Size
Two conditions must be met to fulfill the requirements for size: the community must be of considerable size, and must display an awareness and recognition of a community among its members.

The community as defined in the application is of a considerable size. The community for .ECO as defined in the application is large in terms of the number of members. According to the applicant:

> 40,000+ Not-for-Profit Organizations, eg, 34,376 US environmental organizations (2011 Internal Revenue Service Exempt Organizations Business Master File, National Center for Charitable Statistics); 6,157 in the UK (March 2012, 1⁄3 of 18,470 Environment/Conservation/Heritage registered charities, Charity Commission);
>
> 148,000+ Businesses, eg, 68,200 US businesses committed to environmental sustainability (Pew Charitable Trust, "The Clean Energy Economy", 2009); 80,000 small and medium enterprises in the EU use certified environmental management systems (Danish Technological Institute, "SMEs and the Environment in the European Union", 2010);
>
> 193+ Environment-focused Governmental Bodies – eg, 193 member states (UN website, March 2012);
>
> 18 million+ Individuals, eg, International: WWF, 5M; Greenpeace, 2.8M; FOE, 2M; Ocean Conservancy, 0.5M. National: National Wildlife Federation, 4M; Sierra Club, 1.4M; National Resources Defense Council, 1.2M; The Nature Conservancy, 1M (Members, 2010).

[9] https://www.unglobalcompact.org/docs/news_events/8.1/UNGC_Annual_Review_2010.pdf
[10] http://www.greenpeace.org/usa/en/campaigns/history/

In addition, as previously stated, the community as defined in the application has awareness and recognition among its members. This is because the community is defined in terms of its association with, and active participation in, environmental activities and environmental conservation and preservation.

The Community Priority Evaluation panel determined that the community as defined in the application satisfies both of the conditions to fulfill the requirements for Size.

Longevity

Two conditions must be met to fulfill the requirements for longevity: the community must demonstrate longevity and must display an awareness and recognition of a community among its members.

Many of the major catalysts of the modern environmental movement have continued or worsened in recent years, and the organizations founded with missions of environmental advocacy have redoubled their efforts. The number and breadth of environmental laws and protocols will continue to grow.[11] The effects of climate change are especially long-term[12] and many of the organizations in the application's delineated community advocate for long-term solutions and measures that they have committed to seeing through.[13] The Panel has therefore determined that the community as defined in the application demonstrates longevity. The pursuits of the .ECO community are of a lasting, non-transient nature.

In addition, as mentioned previously, the community as defined in the application has awareness and recognition of a community among its members. This is because the community is defined in terms of its association with, and active participation in, environmental activities. Its members are actively committed to environmental causes, such as sustainable use of the environment and environmental conservation and preservation.

The Community Priority Evaluation panel determined that the community as defined in the application satisfies both the conditions to fulfill the requirements for Longevity.

Criterion #2: Nexus between Proposed String and Community	3/4 Point(s)
2-A Nexus	***2/3 Point(s)***

The Community Priority Evaluation panel determined that the application met the criterion for Nexus as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook. The string "identifies" the name of the community, without over-reaching substantially beyond the community, but does not "match" the name of the community. The application therefore received a score of 2 out of 3 points under criterion 2-A: Nexus.

To receive the maximum score for Nexus, the applied-for string must "match" the name of the community or be a well-known short-form or abbreviation of the community name. To receive a partial score for Nexus, the applied-for string must "identify" the community. "Identify" means that the applied-for string should closely describe the community or the community members, without over-reaching substantially beyond the community.

The applied-for string (.ECO) identifies the name of the community. According to the applicant,

> The term "eco" has long been used to identify members of the Global Environmental Community (the Community), as well as concepts, products and services associated with the Community's goal of a respectful, responsible and sustainable use of the environment. The term appears in common usage and is clearly associated by consumers with environmentally responsible practices.

[11] http://www.britannica.com/EBchecked/topic/189205/environmentalism/224631/History-of-the-environmental-movement

[12] http://www.epa.gov/climatechange/science/future.html

[13] http://www.oecd.org/env/cc/Outlook%20to%202050_Climate%20Change%20Chapter_HIGLIGHTS-FINA-8pager-UPDATED%20NOV2012.pdf

> The Oxford English Dictionary (OED) offers the following examples:
> Individuals and organizations (eg, eco-activist, eco-charities, eco-group)
> Concepts (eg, eco-advocacy, eco-activism, eco-justice, eco-cultural, eco-historical, eco-literacy, eco-philosophy, eco-minded, eco-savvy, eco-awareness, eco-consciousness)
> Products and services (eg, eco-product, eco-label, eco-house, eco-holiday, eco-resort, eco-bottle, eco-bulb, eco-forestry, eco-car)
> (Oxford English Dictionary, 3rd edition, Mar. 2008; online version Sept. 2011)
> Eco in Consumer Protection Public Policy

The Panel has determined that the string ".ECO," is not a match of the community or a well-known short-form or abbreviation of the community name, as the AGB requires for a score of 3 for Nexus. This is because various organizations that are a part of the community as described by the application name the same community in various ways, but generally by use of the word "environment" or by words related to "eco" but not by "eco" itself or on its own. However, because of the common association of the prefix "eco" with various phrases closely associated with environmental protection, such as those provided in the excerpt of the application above, the Panel has determined that the string does identify the community, without overreaching substantially beyond the community.

Additionally, while the string identifies the name of the core community members (i.e. not-for-profit environmental organizations, government agencies with environmental missions, etc.) the community as defined by the application also includes some entities, such as businesses that use certified environmental management systems, which may not automatically be associated with the gTLD. For example, the applicant includes in the proposed community businesses that are participants in the UN Global Compact[14]. Business participants include China Development Bank, a US-based technology firm, Intel Corporation, a Brazil-based natural resources firm, Vale, and UK-based Unilever, a consumer goods company[15]. These companies, and the many others with the same or similar participation in the UN Global Compact, are not commonly known by the string "ECO" as the AGB requires for a full score on Nexus. However, since these entities comprise only part of one category of the application's community membership, the over-reach is not substantial, as the public will generally associate the string with the community as defined by the applicant. Therefore, the Panel has determined that the application should receive partial credit for Nexus.

The Community Priority Evaluation panel determined that the applied-for string "identifies" the name of the community as defined in the application, but does not "match" it. It therefore partially meets the requirements for Nexus.

2-B Uniqueness ***1/1 Point(s)***

The Community Priority Evaluation panel determined that the application met the criterion for Uniqueness as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the string has no other significant meaning beyond identifying the community described in the application. The application received a maximum score of 1 point under criterion 2-B: Uniqueness.

To fulfill the requirements for Uniqueness, the string must have no other significant meaning beyond identifying the community described in the application. The string as defined in the application demonstrates uniqueness as the string does not have any other meaning beyond identifying the community described in the application. According to Oxford Dictionaries, the prefix "eco-" is defined as "Representing ecology, ecological, etc." The string "eco" as a word or concept itself is defined as "Not harming the environment; [as in] eco-friendly." The application cites, as in the excerpt above, several such uses of the applied-for string that correspond to the environmental focus of the community it defines. As such, the Panel has determined that the concept to which the definition refers is the same as the community purpose of the applied-for

[14] The UN Global Compact is the world's largest corporate citizenship and sustainability initiative, with over 10,000 business participants and other stakeholders from more than 145 countries. See https://www.unglobalcompact.org/ParticipantsAndStakeholders/index.html.

[15] https://www.unglobalcompact.org/HowToParticipate/Lead/lead_participants.html

string and that the applied-for string therefore satisfies the condition to fulfill the requirements for Uniqueness.

Criterion #3: Registration Policies **4/4 Point(s)**

3-A Eligibility ***1/1 Point(s)***

The Community Priority Evaluation panel determined that the application met the criterion for Eligibility as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as eligibility is restricted to community members. The application received a maximum score of 1 point under criterion 3-A: Eligibility.

To fulfill the requirements for Eligibility, the registration policies must restrict the eligibility of prospective registrants to community members. The application demonstrates adherence to this requirement by restricting eligibility to individuals and entities (non-for-profit, businesses and governments) that are members of the global environmental community and that meet recognized standards. (Comprehensive details are provided in Section 20e of the applicant documentation). The Community Priority Evaluation panel determined that the application satisfies the condition to fulfill the requirements for Eligibility.

3-B Name Selection ***1/1 Point(s)***

The Community Priority Evaluation panel determined that the application met the criterion for Name Selection as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as name selection rules are consistent with the articulated community-based purpose of the applied-for gTLD. The application received a maximum score of 1 point under criterion 3-B: Name Selection.

To fulfill the requirements for Name Selection, the registration policies for name selection for registrants must be consistent with the articulated, community-based purpose of the applied-for gTLD. The application demonstrates adherence to this requirement by specifying several categories of name registration policies. The applicant further ensures that any strings "used in a manner inconsistent with the Community's goals, values, and/or interests" (Application, Q18(b)) will be flagged and subject to additional scrutiny. The Community Priority Evaluation panel determined that the application satisfies the condition to fulfill the requirements for Name Selection.

3-C Content and Use ***1/1 Point(s)***

The Community Priority Evaluation panel determined that the application met the criterion for Content and Use as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the rules for content and use are consistent with the articulated community-based purpose of the applied-for TLD. The application received a maximum score of 1 point under criterion 3-C: Content and Use.

To fulfill the requirements for Content and Use, the registration policies must include rules for content and use for registrants that are consistent with the articulated community-based purpose of the applied-for gTLD. The application demonstrates adherence to this requirement by specifying that any approved registrant on the gTLD will post a link to their ECO Profile. This ECO Profile is a repository of registrant-specific information that, according to the application:

> "will cover community-recognized memberships, accreditations, registrations, certifications, and reports that demonstrate active commitment, practice and reporting. Additional questions may: be both qualitative and quantitative; include commitments to environmental and social issues that are considered to be linked to environmental goals; and, reference robust existing environmental standards, requirements, indicators, regulations, codes, and calculators."

Therefore, the applicant has required not only certain specific content (in the form of a link to the above registrant-related information), but such content is clearly consistent with the articulate community-based purpose of the applied-for string. The Panel has therefore determined that the application satisfies the condition to fulfill the requirements for Content and Use.

3-D Enforcement ***1/1 Point(s)***

The Community Priority Evaluation panel determined that the application met the criterion for Enforcement as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the application provided specific enforcement measures as well as appropriate appeal mechanisms. The application received a maximum score of 1 point under criterion 3-D: Enforcement.

Two conditions must be met to fulfill the requirements for Enforcement: the registration policies must include specific enforcement measures constituting a coherent set, and there must be appropriate appeals mechanisms. The applicant outlined policies that include specific enforcement measures constituting a coherent set. The applicant's registry will evaluate complaints against a registrant agreement and decide on an appropriate course of action, which may result in the case being referred to a dispute resolution process. There is also an appeals mechanism, whereby a registrant has the right to seek the opinion of an independent arbiter approved by the registry. The Community Priority Evaluation panel determined that the application satisfies both conditions to fulfill the requirements for Enforcement.

Criterion #4: Community Endorsement **3/4 Point(s)**

4-A Support ***1/2 Point(s)***

The Community Priority Evaluation panel has determined that the application partially met the criterion for Support specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as there was documented support from at least one group with relevance. The application received a score of 1 out of 2 points under criterion 4-A: Support.

To receive the maximum score for Support, the applicant is, or has documented support from, the recognized community institution(s)/member organization(s), or has otherwise documented authority to represent the community. In this context, "recognized" refers to the institution(s)/organization(s) that, through membership or otherwise, are clearly recognized by the community members as representative of the community. To receive a partial score for Support, the applicant must have documented support from at least one group with relevance. "Relevance" refers to the communities explicitly and implicitly addressed by the application's defined community.

The Community Priority Evaluation panel has determined that the applicant was not the recognized community institution(s)/member organization(s), nor did it have documented authority to represent the community, or documented support from the recognized community institution(s)/member organization(s). While organizations like the IUCN and the UN Global Compact are sufficient to meet the AGB's requirement for an "entity mainly dedicated to the community" under Delineation (1-A), it does not meet the standard of a "recognized" organization. The AGB specifies that "recognized" means that an organization must be "clearly recognized by the community members as representative of the community." The IUCN and others, as shown in their mission and activities, are clearly dedicated to the community and it serves the community and its members in many ways, but "recognition" demands not only this unilateral dedication of an organization to the community, but a reciprocal recognition on the part of community members of the organization's authority to represent it. There is no single such organization recognized by the defined community as representative of the community. However, the applicant possesses documented support from many groups with relevance; their verified documentation of support contained a description of the process and rationale used in arriving at the expression of support, showing their understanding of the implications of supporting the application. Despite the wide array of organizational support, however, the applicant does not have the support from the recognized community institution, as noted above, and the Panel has not found evidence that such an organization exists. The Community Priority Evaluation Panel has determined that the applicant partially satisfies the requirements for Support.

4-B Opposition ***2/2 Point(s)***

The Community Priority Evaluation panel determined that the application met the criterion for Opposition specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the application did not receive any relevant opposition. The application received the maximum score of 2 points under criterion 4-B: Opposition.

To receive the maximum score for Opposition, the application must not have received any opposition of relevance. To receive a partial score for Opposition, the application must have received opposition from, at most, one group of non-negligible size.

The application received letters of opposition, which were determined not to be relevant, as they were either from individuals or groups of negligible size, or were not from communities which were not mentioned in the application but which have an association to the applied for string. The Community Priority Evaluation Panel determined that the applicant satisfies the requirements for Opposition.

Disclaimer: Please note that these Community Priority Evaluation results do not necessarily determine the final result of the application. In limited cases, the results might be subject to change. These results do not constitute a waiver or amendment of any provision of the Applicant Guidebook or the Registry Agreement. For updated application status and complete details on the program, please refer to the Applicant Guidebook and the ICANN New gTLDs microsite at <newgtlds.icann.org>.

Annex 6.

Reconsideration Request

1. Requester Information

Name: **Little Birch, LLC and Minds + Machines Group Limited, separate applicants for .eco**

Address: Contact Information Redacted

Email: Contact Information Redacted

Hereinafter: the "Requester".

2. Request for Reconsideration of (check one only):

___ **Board action/inaction**

x **Staff action/inaction**

3. Description of specific action you are seeking to have reconsidered.

Requester seeks the reconsideration of ICANN's Community Priority Evaluation Panel's determination whereby Application ID 1-912-59314 for the .eco gTLD (hereinafter: the "Application") submitted by Big Room (hereinafter: the "Applicant") prevailed in Community Priority Evaluation. This determination was posted on ICANN's website under URL https://www.icann.org/sites/default/files/tlds/eco/eco-cpe-1-912-59314-en.pdf (hereinafter: the "CPE Report").

As a result of this Determination, ICANN has:

- resolved the contention set for the .eco gTLD;
- changing the status of the Application to "In Contracting". Reference is made to the Application's status page, available at https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails/1753;
- changing the status of Requester's application for the .eco gTLD to "Will Not Proceed", as referred to on its status page available at https://gtldresult.icann.org/application-

result/applicationstatus/applicationdetails/790.

4. Date of action/inaction:

6 October 2014

5. On what date did you became aware of the action or that action would not be taken?

7 October 2014

6. Describe how you believe you are materially affected by the action or inaction:

Considering the fact that the Determination states that Big Room's Application prevailed in the context of Community Priority Evaluation, the Requester's application for the .eco gTLD will be no longer considered by ICANN, which will likely result in ICANN not awarding the .eco gTLD to Requester.

7. Describe how others may be adversely affected by the action or inaction, if you believe that this is a concern.

In view of the Requester, the concept "eco" is much broader than the so-called community definition provided by the Applicant, as contained in the determination.

Requester refers to:

- the community definition contained in the Application, which – in Requester's opinion – does not meet the criteria for community-based gTLDs that have been set out in ICANN's Applicant Guidebook;
- the community definition contained in the Application, which misrepresents that "eco" is the name or abbreviation of a community, whilst the meaning of "eco" or the "eco-" prefix is much broader than what has been set out in the Application;
- the registration policies, and in particular the eligibility and enforcement criteria set out in the Application do not meet the standards set out in the New gTLD Applicant Guidebook. In particular, considering the fact that the eligibility criteria contained in the Application for registering domain names under the .eco gTLD as well as the community definition contained therein are contradictory, vague, and ill defined, this may result in:

- third parties who are affiliated with the term or prefix “eco” but who are not a “member” of the “community” purported by the Applicant will be unable to register domain names in the .eco gTLD because they do not meet the eligibility requirements set out in the Application, which seems to be mainly directed to the non-existing “eco community”;
- others, such as but not limited to companies who clearly have no proven track record in relation to “ecological” or “environmental-friendly” behavior, would indeed be eligible to register domain names in this extension.

Further details in this respect are provided below:

As regards Criterion #1: Community Establishment

According to the CPE Report, a “.eco Community” exists, which has been defined in the Application is as follows:

> *“Members of the Community are delineated from Internet users generally by community-recognized memberships, accreditations, registrations, and certifications that demonstrate active commitment, practice and reporting.*
>
> *Community members include:*
> *Relevant not-for-profit environmental organizations (ie, accredited by relevant United Nations (UN) bodies; International Union for Conservation of Nature (IUCN) member; proof of not-for-profit legal entity status with documented environmental mission).*
> *Businesses (ie, members of environmental organizations; UN Global Compact participants; hold internationally-recognized environmental certifications; report to a global sustainability standard).*
> *Government agencies with environmental missions (ie, UN bodies, national/sub-national government agencies with environmental responsibilities).*
> *Individuals (ie, members of environmental organizations; academics; certified environmental professionals).”*

Requester notes that the above is by all means not a definition of a community but a vague overview what its membership is considered by Big Room Inc. to consist of. According to the Requester, absent a clear and unambiguous definition of the “community” a community-based application is intended to serve, the Application needs to be dismissed from the outset.

The CPE Report and the Determination therefore assume the existence of a community, without reviewing whether this is actually the case.

Indeed, based on the above overview, any individual who or business that becomes a member of or a donator to an environmental organization such as Greenpeace or the WWF would, according to the above "definition" be a member of the "community for .eco".

By accepting such an approach, the CPE Report and the Determination are not taking into account the various criteria set out in the Applicant Guidebook (AGB) for community-based applications.

According to the AGB, the term "community" implies "more of cohesion than a mere commonality of interest", and there should be "an awareness and recognition of a community among its members".

Although Big Room Inc. and the CPE Panel attempt to establish that there is a "cohesion" among the members of this so-called "community for .eco", they are in fact only establishing that there is indeed – at maximum – a "mere commonality of interest":

- according to the Application *"[t]he Community has historically structured and organized itself and its work through an international network of organizations, including millions of individual members with strongly aligned goals, values and interests";* (emphasis added)

- furthermore, *"members traditionally organize through multi-organization alliances around specific events, geographies, and issues"*;

- according to the Determination, *"the community is defined in terms of its association with, and active participation in, environmental activities"*.[1]

Whilst the Requester does not negate that the members referred to in the Application share a number of common goals, values and interests (as expressly stated in the Application), this in itself is insufficient to determine that there is an established community. The *"issues"* the members addressed in the Application could be to a certain extent aligned, and some of them may "associate" themselves with these issues and activities, but this does not prove that there is "awareness and recognition" of a community in the sense of the AGB.

According to the Requester, this view is underlined by the CPE Panel's determination that the string ".eco" is *"not a match of the community or a well-known short-form or abbreviation of the community name"*, as required by the AGB for a score of 3 for Nexus: in other words, Requester does not understand how a wide variety of so-called "members" consider themselves part of a "community for eco" or ".eco community" if "eco" is not even recognized as the name or the abbreviation of the community …

[1] CPE Report, Page 5.

This is clear evidence of the fact that being or associating with “eco” as in “ecology” and “environment” is the common goal, value or interest of all the “members” of this community, and demonstrates that none or at most an extremely limited number of them are really convinced that there is a “cohesion” amongst them, considering the fact that they are supporting different projects or causes that are in the environmental sphere.

In addition, the CPE Report and the Application states that *“[T]he term “eco” has been long used to identify members of the Global Environmental Community (the Community), as well as concepts, products and services associated with the Community’s goal of a respectful, responsible and sustainable use of the environment.”*[2] (emphasis added)

Requester therefore does not understand how the CPE Panel has come to the conclusion that an “eco” community can exist if not only the community itself is identified by the term “eco”, but also (i) members of the Global Environmental Community, (ii) concepts, (iii) products, and (iv) services. Again, according to the Requester, this only demonstrates that “eco” is an overarching umbrella term, but not a true community in the sense of the AGB.

Therefore, Requester requests ICANN to reconsider the scoring on Criterion #1: Community Establishment, and provide the Application with a score of 1 or even 0 (zero) on this Criterion.

As regards Criterion #2-A: Nexus between Proposed String and Community

Public information reveals that the string “eco” does not “closely describe” the community or the community members, and that it certainly over-reaches substantially beyond the community referred to in the application.

For instance, according to Wikipedia,[3] the term “eco” may refer to:

- *eco-, a prefix mostly relating to ecological or environmental terms (emphasis added)*
- *.eco, (dot-eco), a proposed top-level domain for the Internet*
- *Eco (currency), a proposed currency*
- *Eco (video game), a computer simulation game*
- *Umberto Eco (born 1932), Italian philosopher, semiotician, novelist*
- *Eco, a character, played by Jacqueline Duncan, on the children's show The Shak*
- *The natural substance of energy and power in the Jak and Daxter games*

[2] CPE Report, Page 5.
[3] http://en.wikipedia.org/wiki/Eco.

Requester notes that no reference is being made to any "*eco community"*, nor does the string apparently seems to identify *"the name of the core community members"* as stated in the determination. If a "community of eco" would exist, this would be one of the elements that would generally be recognized by an important public source such as Wikipedia, to which thousands of people have contributed over the years.

Furthermore, according to the same source, the abbreviation eco has a wide variety of uses:

- *Enterprise Core Objects, software development framework useful for domain-driven design*
- *Economic Cooperation Organization, an international organization involving seven Asian and four Eurasian countries*
- *Electronic Countermeasures Officer, an officer in the reimagined Battlestar Galactica series*
- *Emil Chronicle Online, a 2005 Japanese MMO computer game*
- *Encyclopaedia of Chess Openings, a scheme to classify chess openings*
- *Engineering Change Order, used for changes in documents such as processes and work instructions*
- *English Chamber Orchestra, a chamber orchestra based in London*
- *The Environmental Commissioner of Ontario*
- *Environment and Conservation Organisations of Aotearoa New Zealand*
- *Epichlorohydrin, a synthetic rubber with the ISO code eco*
- *Equity carve-out, a sort of corporate restructuring*
- *Esporte Clube Osasco, a Brazilian football (soccer) club*
- *Eternally Collapsing Objects, an alternate theory of black hole. See Magnetospheric eternally collapsing object*
- *European Communications Office, the permanent secretariat of the Electronic Communications Committee, a part of European Conference of Postal and Telecommunications Administrations*
- *eco (denomination), a Presbyterian denomination (full name eco: A Covenant Order of Evangelical Presbyterians)*
- *Noticias eco, a now defunct 24-hour Spanish-language cable news network, owned and operated by Televisa*
- *Elementaire Commando Opleiding (elementary commando course) of the Korps Commandotroepen (KCT)*

Furthermore, the prefix "eco-" is, next to "ecology" or the "environment" (in the ecological sense) also used in the context of terms relating to "economy".[4]

In the Requester's view, the CPE Panel has therefore not considered the many other meanings of the term "eco", some of which have been outlined above, and

[4] http://en.wiktionary.org/wiki/eco-

has therefore erroneously determined that *"[t]he applied-for string (.eco) identifies the name of the community"* or *"the name of the core community members"*.[5]

Furthermore, the CPE Panel errs when determining that *"the public will generally associate the string with the community as defined by the applicant"*: although "eco" could indeed be considered by the community as the prefix for terms relating to ecology or the environment, the public will not directly or indirectly consider this abbreviation as the identifier of a community or groups, organizations, companies or individuals that has supported the Applicant.

Based on basic Internet research, it is clear that many of the members of the organizations referred to in the Application are far from being liaised with "ecological" or "environmental" activities.

By way of example, the UN Global Compact [6] has the following companies as its members: E.I. du Pont de Nemours,[7] Bayer Group,[8] Dow Chemical,[9] BASF,[10] and General Electric.[11] Requester points out in this respect to the fact that the CPE Panel has recognized the UN Global Compact to be *"sufficient to meet the AGB's standard of a "recognized" organization"*.[12]

These companies are five out of the Top 10 of the Toxic 100 Air Polluters, published by the Political Economy Research Institute, a department of the University of Massachusetts Amherst,[13] which clearly shows that the "community" invoked by the Applicant is fictitious, and that the "membership" of this self-invoked "community" can be easily obtained, without being subject to any scrutiny.

Considering the above, it is unlikely that the public at large will:

1) directly or even indirectly associate the term "eco" or the string ".eco" with the Applicant;

2) directly or even indirectly associate the term "eco" or the string ".eco" with any sort or type of "community" in general, or specifically with an "eco community";

[5] CPE Report, Page 5.
[6] https://www.unglobalcompact.org.
[7] https://www.unglobalcompact.org/participant/3023-DuPont.
[8] https://www.unglobalcompact.org/participant/1212-Bayer-AG.
[9] https://www.unglobalcompact.org/participant/9210-The-Dow-Chemical-Company.
[10] https://www.unglobalcompact.org/participant/1194-BASF-SE.
[11] https://www.unglobalcompact.org/participant/4253-General-Electric-Company.
[12] CPE Report, Page 8.
[13] http://www.peri.umass.edu/toxicair_current/.

3) directly or even indirectly associate the term “eco” or the string “.eco” with many organizations and companies that are considered to be members of the so-called “community” described in the Application; and

4) directly or even indirectly associate the term “eco” or the string “.eco” with the *“name of the core community members”*.

Hence, Requester is of the opinion that the term “eco” substantially over-reaches the so-called “community” the Applicant has attempted to define in the Application.

Therefore, Requester requests ICANN to reconsider the scoring on Criterion #2-A: Nexus, and provide the Application with a score of 0 (zero) on this Criterion.

As regards Criterion #2-B: Uniqueness

As Requester has pointed out in the previous section, the term “eco” has various meanings that are completely unrelated to the “community” determined in the Application or the “names of community members” that are part of such so-called, but non-existing, “community”.

Therefore, Requester requests ICANN to reconsider the scoring on Criterion #2-B: Uniqueness, and provide the Application with a score of 0 (zero) on this Criterion. More in particular, since Requester has substantiated on the basis of public information and independent research that 0 (zero) points should be awarded in relation to Criterion #2-A: Nexus, the score for Criterion #2-B: Uniqueness should be automatically reset to 0 (zero).

As regards Criterion #4-B: Opposition

The CPE Panel has determined that *“the application met the criterion for Opposition specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the application did not receive any relevant opposition. The application received the maximum score of 2 points under criterion 4-B: Opposition”*.

Whilst the CPE Panel has confirmed that the Application received letters of opposition, it does not detail: (i) which letters have been received, (ii) which letters have not been considered in the determination, (iii) which criteria and standards have been used in determining whether these letters were from groups, individuals or communities “of negligible size” that had an association to the applied for string.

Therefore, the Requester is of the opinion that the determination does not meet the appropriate standards of transparency and due process, which renders it impossible for Requester to review whether the Applicant has indeed satisfied the criterion 4-B: Opposition.

Other Submissions by Requester

Requester also refers to its request made under the Documentary Information Disclosure Policy, attached hereto as Annex 1.

In any case, Requester reserves the right to supplement this Reconsideration Request with further information and arguments following the outcome of their request under the Documentary Information Disclosure Policy, even if no additional information would be provided by ICANN.

8. Detail of Board or Staff Action – Required Information

Provide the Required Detailed Explanation here:

In the context of ICANN's New gTLD Program, ICANN has received the following applications for the .eco gTLD:

- the Applicant's application for a community-based gTLD (Application ID 1-912-59314);
- Little Birch's "standard" application (Application ID 1-1434-1370);
- Top Level Domain Holdings Lilmited's "standard" application (Application ID 1-1039-91823).

On October 6, 2014, ICANN's Community Priority Evaluation panel published its Determination stating that the Applicant's Application for the .eco gTLD obtained a passing score of 14 out of 16 points, and hence prevailed in Community Priority Evaluation.

Since Requester is of the opinion that the publication of these Community Priority Evaluation results are considered to be an action by ICANN staff, which is in particular the case for modifying the statuses of each of the respective applications for the .eco gTLD listed below, it is entitled to invoke and utilize ICANN's Reconsideration Request process in relation to this Determination / action by ICANN staff.

The immediate effect of this Determination seems to be that the Requester's application for the .eco gTLD will no longer be considered by ICANN, given the fact that the status of its application has been changed to "Will Not Proceed", as is reflected on their respective Application Status pages published by ICANN.

Reference is made to Little Birch's "standard" application (Application ID 1-1434-1370), published at https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails/790.

Requester therefore requests ICANN in accordance with its Reconsideration Request process to:

- reconsider the Determination, and in particular not award a passing score in view of the Community Priority Evaluation criteria set out in the Applicant Guidebook for the reasons expressed in this Reconsideration Request and any reasons, arguments and information to be supplemented to this Request or forming part of a new Reconsideration Request in the future;
- reconsider ICANN's decision that the Requester's application for the .eco gTLD "Will Not Proceed" to contracting;
- restore the "Application Status" of the Requester's application and the Application submitted by the Applicant to "Evaluation Complete", their respective "Contention Resolution Statuses" to "Active", and their "Contention Resolution Result" to "In Contention".

9. What are you asking ICANN to do now?

Based upon the information contained in the Application, Requests are convinced that the Application does not meet the criteria to qualify as a community-based gTLD set out in ICANN's Applicant Guidebook.

In view of obtaining further insights into the arguments of the Community Priority Evaluation panel and the information on which such panel has relied, Requester has submitted together with this Reconsideration Request and request to obtain further information under ICANN's Documentary Information Disclosure Policy.

Based upon the information and arguments included in this Reconsideration Request, for which the Requester reserves the right to submit additional arguments and information following the outcome of their request submitted to ICANN in accordance with the Documentary Information Disclosure Policy, Requester requests ICANN to:

- acknowledge receipt of this Reconsideration Request;
- suspend this Reconsideration Request in view of possible supplementary arguments and information to be provided by Requester on the basis of ICANN's responses to Requester's Documentary Information Disclosure Policy;
- in the meantime, suspend the process for awarding the .eco gTLD to the Applicant;

- reverse the “Application Status” of Requester’s application and the Application submitted by the Applicant to “Evaluation Complete”, their respective “Contention Resolution Statuses” to “Active”, and their “Contention Resolution Result” to “In Contention”;
- ultimately, unless Requester withdraws this Reconsideration Request or does not provide ICANN with additional information or arguments within a timeframe of 15 days following receipt of ICANN’s responses to Requester’s request under the Documentary Information Disclosure policy, if any.

10. Please state specifically the grounds under which you have the standing and the right to assert this Request for Reconsideration, and the grounds or justifications that support your request.

Requester is an applicant for the .eco gTLD.

Reference is made to ICANN’s status page for its application with ID 1-1434-1370), published at https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails/790.

Given the fact that due to the Determination, the Requester’s application for the .eco gTLD will not proceed to the contracting phase with ICANN, which will likely result in ICANN not awarding the .eco gTLD to Requester, it is clear that the Determination materially affects Requester’s applications for this string.

As a consequence, Requester has standing to file this Reconsideration Request in relation to the Determination by the Community Priority Evaluation, as well as ICANN’s subsequent decision to change the status of Requester’s application from “In Contention” to “Will Not Proceed”.

11. Are you bringing this Reconsideration Request on behalf of multiple persons or entities? (Check one)

____ Yes

__x_ No

11a. If yes, Is the causal connection between the circumstances of the Reconsideration Request and the harm the same for all of the complaining parties? Explain.

Yes. Requester is an applicant for the .eco gTLD and is directly affected by the Determination, which – ultimately – would cause irreparable harm to Requester if such Determination would be final.

However, Requester acknowledges that, most likely and ultimately, only one of the contenders for the .eco gTLD will effectively become the Registry Operator for such gTLD.

Do you have any documents you want to provide to ICANN?

Pending Requester's request under the Documentary Information Disclosure Policy, Requester is not providing any specific documents to ICANN, but reserve the right to do so as a follow-up to this Reconsideration Request or in the context of one or more new Reconsideration Requests. Requester recognizes and acknowledges that any such additional Reconsideration Requests may be consolidated by the Board Governance Committee.

Terms and Conditions for Submission of Reconsideration Requests

The Board Governance Committee has the ability to consolidate the consideration of Reconsideration Requests if the issues stated within are sufficiently similar.

The Board Governance Committee may dismiss Reconsideration Requests that are querulous or vexatious.

Hearings are not required in the Reconsideration Process, however Requestors may request a hearing. The BGC retains the absolute discretion to determine whether a hearing is appropriate, and to call people before it for a hearing.

The BGC may take a decision on reconsideration of requests relating to staff action/inaction without reference to the full ICANN Board. Whether recommendations will issue to the ICANN Board is within the discretion of the BGC.

The ICANN Board of Director's decision on the BGC's reconsideration recommendation is final and not subject to a reconsideration request.

______________________________ ____________________

Signature Date

Annex 7.

ICANN
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA

22 October 2014

By email: didp@icann.org

Dear Madam,
Dear Sir,

.ECO Community Priority Evaluation for Application ID 1-912-59314
Request under ICANN's Documentary Information Disclosure Policy

This request is submitted under ICANN's Documentary Information Disclosure Policy on by Little Birch LLC, one of the applicants for the .ECO gTLD (hereinafter referred to as "Requester") in relation to ICANN's Community Priority Evaluation panel's ("CPE Panel") determination that Big Room Inc.'s application for the .ECO gTLD (Application ID: 1-912-59314; hereinafter referred to as the "Application") prevailed in Community Priority Evaluation according to the Community Priority Evaluation report available at https://www.icann.org/sites/default/files/tlds/eco/eco-cpe-1-912-59314-en.pdf (hereinafter: the "CPE Report").

Context

Reference is made to the CPE Report that has been released by ICANN and published on the ICANN website as referred to above, and ICANN's decision to change the Contention Resolution Status of the Application to "In Contracting" and the Contention Resolution Result to "Resolved" (hereinafter: the "Determination").

According to the CPE Report: *"[t]he Community Priority Evalation panel has determined that the application met the requirements specified in the Applicant Guidebook"*, hereby confirming that the application for the .ECO gTLD that has been submitted by Big Room Inc. *"prevailed in Community Priority Evaluation"*.

Considering the fact that, according to the processes and procedures set out in ICANN's Applicant Guidebook, this Determination would result in ICANN (i) awarding the .ECO gTLD to Big Room Inc., and – hence – (ii) not allowing the Requester to proceed with its application for this string, this decision materially impacts the application submitted by the latter.

According to ICANN, *"ICANN's Documentary Information Disclosure Policy (DIDP) is intended to ensure that information contained in documents concerning ICANN's operational activities, and within ICANN's possession, custody, or control, is made available to the public unless there is a compelling reason for confidentiality."*[1]

[1] See https://www.icann.org/resources/pages/didp-2012-02-25-en.

Requester therefore invokes ICANN's accountability mechanisms in order to understand on which information the CPE Panel have relied in developing the CPE Report and ICANN in making the Determination.

Request

In view of transparency of ICANN's decision-making process, the Requester would like to obtain the following information from ICANN under the Documentary Information Disclosure Policy:

1) the agreement(s) between ICANN and the organizations and individuals involved in the Community Priority Evaluation, in particular the representations and warranties given and quality standards to be applied by such organizations and individuals;

2) policies, guidelines, directives, instructions or guidance given by ICANN relating to the Community Priority Evaluation process;

3) internal reports, notes, meeting minutes drawn up by or on behalf of ICANN, the Community Priority Panels, and other individuals or organizations involved in the Community Priority Evaluation in relation to the Application;

4) input provided by the Applicant or organizations, governmental authorities, businesses and individuals having supported the Applicant's application for the .ECO gTLD, including the Applicant's responses to Clarifying Questions (if any), or other communications that have not been made public but have been reviewed and/or considered by the CPE Panel and ICANN in this respect;

5) detailed information in relation to (i) the information reviewed, (ii) criteria and standards used, (iii) arguments exchanged, (iv) information disregarded or considered irrelevant, and (v) scores given by the Community Priority Evaluation panel in view of the criteria set out in the Applicant Guidebook, and more in particular:

I. In relation to the criterion "Community Establishment"

According to the CPE Report, a ".ECO Community" exists, which has been defined in the Application is as follows:

"Members of the Community are delineated from Internet users generally by community-recognized memberships, accreditations, registrations, and certifications that demonstrate active commitment, practice and reporting.

Community members include:
Relevant not-for-profit environmental organizations (ie, accredited by relevant United Nations (UN) bodies; International Union for Conservation of Nature (IUCN) member; proof of not-for-profit legal entity status with documented environmental mission).
Businesses (ie, members of environmental organizations; UN Global Compact participants; hold internationally-recognized environmental certifications; report to a global sustainability standard).
Government agencies with environmental missions (ie, UN bodies, national/sub-national government agencies with environmental responsibilities).

> *Individuals (ie, members of environmental organizations; academics; certified environmental professionals)."*
>
> Requester notes that the above is by all means not a definition of a community but a vague overview what its membership is considered by Big Room Inc. to consist of.
>
> Requester therefore requests ICANN to provide further details relating to:
>
> (i) the actual definition of the community that has been assessed by the CPE Panel, if any;
>
> (ii) the (independent) review carried out by the CPE Panel in accepting the existence of the community, and which information has been relied on in this respect by the CPE Panel;
>
> (iii) the criteria and standards that have been used in assuming the existence of an "ECO" or ".ECO" community;
>
> (iv) the additional factors that have been taken into account by the CPE Panel in determining that the "community for ECO", apparently consisting of organizations, businesses, individuals, and government agencies, (i) are aware that they are part of a community, (ii) that they are recognized as a member of a community, and (iii) that this so-called community implies more "of cohesion than a mere commonality of interest", and (iv) which have been the standards and criteria that have been used to make a distinction between "cohesion" and "commonality of interest".

II. In relation to the criteria "Nexus" and "Uniqueness":

According to the Determination:

> *"The Community Priority Evaluation panel determined that the application met the criterion for Nexus as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook. The string "identifies" the name of the community, without over-reaching substantially beyond the community, but does not "match" the name of the community."*

and

> *"The Community Priority Evaluation panel determined that the application met the criterion for Uniqueness as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the string has no other significant meaning beyond identifying the community described in the application."*

First of all, Requester would like to obtain further information on the criteria and standards that have been used by the CPE Panel in determining that "ECO" "identifies" the name of the community: which independent research has been carried out in order to come to such a conclusion, and more in particular which information has been relied on and which information has been discarded by the CPE Panel.

Public information reveals that the string "ECO" does not "closely describe" the community or the community members, and that it certainly over-reaches substantially beyond the community referred to in the application.

For instance, according to Wikipedia,[2] the term "eco" may refer to:

- *eco-, a prefix mostly relating to ecological or environmental terms (emphasis added)*
- *.eco, (dot-eco), a proposed top-level domain for the Internet*
- *Eco (currency), a proposed currency*
- *Eco (video game), a computer simulation game*
- *Umberto Eco (born 1932), Italian philosopher, semiotician, novelist*
- *Eco, a character, played by Jacqueline Duncan, on the children's show The Shak*
- *The natural substance of energy and power in the Jak and Daxter games*

Requester notes that no reference is being made to any "eco community", nor does the string apparently seems to identify "the name of the core community members" (in addition to concepts, products and services) as stated in the determination.

Furthermore, according to the same source, the abbreviation ECO has a wide variety of uses:

- *Enterprise Core Objects, software development framework useful for domain-driven design*
- *Economic Cooperation Organization, an international organization involving seven Asian and four Eurasian countries*
- *Electronic Countermeasures Officer, an officer in the reimagined Battlestar Galactica series*
- *Emil Chronicle Online, a 2005 Japanese MMO computer game*
- *Encyclopaedia of Chess Openings, a scheme to classify chess openings*
- *Engineering Change Order, used for changes in documents such as processes and work instructions*
- *English Chamber Orchestra, a chamber orchestra based in London*
- *The Environmental Commissioner of Ontario*
- *Environment and Conservation Organisations of Aotearoa New Zealand*
- *Epichlorohydrin, a synthetic rubber with the ISO code ECO*
- *Equity carve-out, a sort of corporate restructuring*
- *Esporte Clube Osasco, a Brazilian football (soccer) club*
- *Eternally Collapsing Objects, an alternate theory of black hole. See Magnetospheric eternally collapsing object*
- *European Communications Office, the permanent secretariat of the Electronic Communications Committee, a part of European Conference of Postal and Telecommunications Administrations*
- *ECO (denomination), a Presbyterian denomination (full name ECO: A Covenant Order of Evangelical Presbyterians)*
- *Noticias ECO, a now defunct 24-hour Spanish-language cable news network, owned and operated by Televisa*
- *Elementaire Commando Opleiding (elementary commando course) of the Korps Commandotroepen (KCT)*

Furthermore, the prefix "eco-" is, next to "ecology" or the "environment" (in the ecological sense) also used in the context of terms relating to "economy".[3]

Therefore, the Requester would like to obtain further information from ICANN regarding:

[2] http://en.wikipedia.org/wiki/Eco.

[3] http://en.wiktionary.org/wiki/eco-

(i) the information considered by the CPE Panel and ICANN in the CPE Report and the Determination in assessing the uniqueness of the term, prefix or abbreviation "ECO";

(ii) the independent research performed by the CPE Panel and ICANN in this respect;

(iii) more in particular, the reasons for discarding the many other meanings and uses of the term "ECO" outside of the environmental and ecological fields, especially those referred to above.

III. In relation to the criterion "Community Endorsement":

The Community Priority Evaluation panel determined that the Application *"partially met the criterion for Support specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as there was documented support from at least one group with relevance."* – Determination, Page 7.

Requesters would like to obtain further information concerning:

- which letters of endorsement and/or support have been considered by the CPE Panel in making its Determination;

- which criteria and/or standards have been used by the CPE Panel in order to determine which group is "of relevance" in relation to the organizations, companies and individuals that have provided letters of endorsement and/or support in relation to the Application;

IV. In relation to the criterion "Opposition":

Requesters would like to obtain further information as to the reasons why and the criteria against which the public comments, submitted by many third parties to ICANN in relation to the Application, which all contained strong oppostion against ICANN awarding the .ECO gTLD to the Applicant have obviously been considered "of no relevance" and that each of these have been considered as a "group of negligible size".

Standards for Disclosure

Requesters are of the opinion that none of the information requested by them meet any of the defined conditions for non-disclosure as set out in ICANN's Documentary Information Disclosure Policy:

- Information provided by or to a government or international organization, or any form of recitation of such information, in the expectation that the information will be kept confidential and/or would or likely would materially prejudice ICANN's relationship with that party.

  Considering the nature and contents of Requesters' requests, this standard is not met.

- Internal information that, if disclosed, would or would be likely to compromise the integrity of ICANN's deliberative and decision-making process by inhibiting the candid exchange of ideas and communications, including internal documents, memoranda, and other similar communications to or from ICANN Directors, ICANN Directors' Advisors, ICANN staff, ICANN consultants, ICANN contractors, and ICANN agents.

Considering the nature and contents of Requesters' requests, this standard is not met. Since these requests are made in view of assessing Requesters' respective positions and (legal) actions in relation to ICANN potentially awarding the .ECO gTLD to the REQUESTER, and considering the impact such award may have upon Requesters, they believe that it is essential for ICANN to provide supplemental information and motivations for its determination to give the Application a passing score in the context of Community Priority Evalation.

- Information exchanged, prepared for, or derived from the deliberative and decision-making process between ICANN, its constituents, and/or other entities with which ICANN cooperates that, if disclosed, would or would be likely to compromise the integrity of the deliberative and decision-making process between and among ICANN, its constituents, and/or other entities with which ICANN cooperates by inhibiting the candid exchange of ideas and communications.

  Considering the nature and contents of Requesters' requests, this standard is not met. Since these requests are made in view of assessing Requesters' respective positions and (legal) actions in relation to ICANN potentially awarding the .ECO gTLD to the REQUESTER, and considering the impact such award may have upon Requesters, they believe that it is essential for ICANN to provide supplemental information and motivations for its determination to give the Application a passing score in the context of Community Priority Evalation.

- Personnel, medical, contractual, remuneration, and similar records relating to an individual's personal information, when the disclosure of such information would or likely would constitute an invasion of personal privacy, as well as proceedings of internal appeal mechanisms and investigations.

  Requesters believe that this condition does not apply in relation to this request.

- Information provided to ICANN by a party that, if disclosed, would or would be likely to materially prejudice the commercial interests, financial interests, and/or competitive position of such party or was provided to ICANN pursuant to a nondisclosure agreement or nondisclosure provision within an agreement.

  Requesters believe that this condition does not apply in relation to this request.

- Confidential business information and/or internal policies and procedures.

  Requesters believe that this condition does not apply in relation to this request.

- Information that, if disclosed, would or would be likely to endanger the life, health, or safety of any individual or materially prejudice the administration of justice.

  Requesters believe that this condition does not apply in relation to this request.

- Information subject to the attorney– client, attorney work product privilege, or any other applicable privilege, or disclosure of which might prejudice any internal, governmental, or legal investigation.

Requesters believe that this condition does not apply in relation to this request.

- Drafts of all correspondence, reports, documents, agreements, contracts, emails, or any other forms of communication.

  Requesters believe that this condition does not apply in relation to this request. The Requesters' requests relate to the information, final criteria, standards, arguments and considerations used in view of drafting a determination that lacks clarity and is insufficiently motivated.

- Information that relates in any way to the security and stability of the Internet, including the operation of the L Root or any changes, modifications, or additions to the root zone.

  Requesters believe that this condition does not apply in relation to this request.

- Trade secrets and commercial and financial information not publicly disclosed by ICANN.

  Requesters believe that this condition does not apply in relation to this request.

- Information requests: (i) which are not reasonable; (ii) which are excessive or overly burdensome; (iii) complying with which is not feasible; or (iv) are made with an abusive or vexatious purpose or by a vexatious or querulous individual.

  As stated above, considering the impact of ICANN awarding the .ECO gTLD may have upon Requesters, they believe that it is essential for ICANN to provide supplemental information and motivations for its determination to give the Application a passing score in the context of Community Priority Evalation.

ICANN's transparency obligations, created by ICANN's Bylaws and Articles of Incorporation require the publication of information related to the process, facts and analysis used by individual members of the Community Priority Evaluation panel in preparation of the Determination.

Bylaw Article III, Section 1 provides as follows:

> *"ICANN and its constituent bodies shall operate to the maximum extent feasible in an open and transparent manner and consistent with procedures designed to use fairness."*

Furthermore, Requesters refer to ICANN's core mission and values, set out in their by-laws, and in particular, they intend to review the information provided and to be provided by ICANN following this request on the basis of the following values of ICANN:

> *7. Employing open and transparent policy development mechanisms that (i) promote well-informed decisions based on expert advice, and (ii) ensure that those entities most affected can assist in the policy development process.*
>
> *8. Making decisions by applying documented policies neutrally and objectively, with integrity and fairness.*
>
> *And*

> *10. Remaining accountable to the Internet community through mechanisms that enhance ICANN's effectiveness.*

Furthermore, Article 4 of ICANN's Articles of Incorporation provides:

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

Considering the potentially irreparable harm that will be done if ICANN would not take into account the position taken by the Requesters as legitimate competitors for the .ECO gTLD, we respectfully request ICANN to disclose the additional information, criteria, and standards set out above, which have formed the basis of the Determination.

Respectfully submitted,

Reg Levy
VP Compliance + Policy
Minds + Machines

Annex 8.

Response to Documentary Information Disclosure Policy Request

To: Reg Levy, Minds + Machines

Date: 31 October 2014

Re: Request No. 20141022-1

Thank you for your Request for Information dated 22 October 2014 (the "Request"), which was submitted through the Internet Corporation for Assigned Names and Numbers' ("ICANN's") Documentary Information Disclosure Policy ("DIDP"). For reference, a copy of your Request is attached to the email forwarding this Response.

Items Requested:

Your Request seeks the following:

(1) the agreement(s) between ICANN and the organizations and individuals involved in the Community Priority Evaluation, in particular the representations and warranties given and quality standards to be applied by such organizations and individuals;

(2) policies, guidelines, directives, instructions or guidance given by ICANN relating to the Community Priority Evaluation process;

(3) internal reports, notes, meeting minutes drawn up by or on behalf of ICANN, the Community Priority Panels, and other individuals or organizations involved in the Community Priority Evaluation in relation to the Application [from Big Room Inc. for .ECO that prevailed in the CPE];

(4) input provided by the Applicant or organizations, governmental authorities, businesses and individuals having supported the Applicant's application for the .ECO gTLD, including the Applicant's responses to the Clarifying Questions (if any), or other communications that have not been made public but have been reviewed and/or considered by the CPE Panel and ICANN in this respect;

(5) detailed information in relation to (i) the information reviewed, (ii) criteria and standards used, (iii) arguments exchanged, (iv) information disregarded or considered irrelevant, and (v) scores given by the Community Priority Evaluation panel in view of the criteria set out in the Applicant Guidebook, and more in particular: [relating to the panel's determination of each individual criterion].

Response

Community Priority Evaluations ("CPEs") are performed by an independent community panel that is coordinated by the Economist Intelligent Unit ("EIU"), an independent, third-party company that contracts with ICANN to perform that coordination role. The

CPE standards set forth in Section 4.2 of the Applicant Guidebook ("Guidebook") are available at http://newgtlds.icann.org/en/applicants/agb. The CPE Panel Process Document (at http://newgtlds.icann.org/en/applicants/cpe) and the CPE Guidelines (at http://newgtlds.icann.org/en/applicants/cpe) provide more information on the CPE process. The Guidebook, CPE Panel Process Document, and the CPE Guidelines set forth the guidelines, procedures, standards and criteria applied to CPEs, and make clear that the EIU and its designated panelists are the only persons or entities involved in the provision of CPEs.

For item 1, there is a single contract at issue, the contract between ICANN and the EIU for the coordination of the independent community panels to perform CPEs in the New gTLD Program. ICANN does not contract with individuals or individual panelists to perform CPEs. The contract between ICANN and the EIU is not appropriate for public disclosure through the DIDP. The contract includes a confidentiality clause barring ICANN from disclosing the agreement as requested. The following Defined Conditions for Nondisclosure apply to the requested contract:

- Internal information that, if disclosed, would or would be likely to compromise the integrity of ICANN's deliberative and decision-making process by inhibiting the candid exchange of ideas and communications, including internal documents, memoranda, and other similar communications to or from ICANN Directors, ICANN Directors' Advisors, ICANN staff, ICANN consultants, ICANN contractors, and ICANN agents.

- Information provided to ICANN by a party that, if disclosed, would or would be likely to materially prejudice the commercial interests, financial interests, and/or competitive position of such party or was provided to ICANN pursuant to a nondisclosure agreement or nondisclosure provision within an agreement.

- Confidential business information and/or internal policies and procedures.

For item 2, which seeks "policies, guidelines, directives, instructions or guidance given by ICANN relating to" the CPE process, to the extent that this is seeking information external to the types of directives that would be incorporated into a contract, much of that information is already incorporated into the publicly available documents identified above. Similarly, for items 2, 3, 4 and 5, ICANN has previously indicated in response to Request No. 20140804-1 that ICANN has communications with persons at EIU that are not involved in the scoring of a CPE (but otherwise assist in the facilitation of a particular CPE), and also previously indicated that those communications are not appropriate for public disclosure.

Items 3 and 5 seek extensive, detailed information regarding the analysis conducted by the CPE Panel in making its determination that Big Room Inc.'s application for .ECO prevailed in the CPE. For instance, the Requester seeks "internal reports," "detailed information in relation to […] information disregarded or considered irrelevant," and specific information regarding the CPE Panel's determination as to each criterion.[1] To help assure independence of the process and evaluation of CPEs, ICANN (either Board or staff) is not involved with the CPE Panel's evaluation of criteria, scoring decisions, or underlying analyses. The coordination of the CPE Panel, as explained in the CPE Panel Process Document, is entirely within the work of the EIU's team. ICANN does not have, nor does it collect or maintain, the work papers of the individual CPE Panels (including the .ECO CPE Panel). The end result of the CPE Panel's analysis is the CPE Report on Big Room's application for .ECO, which explains the CPE Panel's determinations and scoring, and is available at https://www.icann.org/sites/default/files/tlds/eco/eco-cpe-1-912-59314-en.pdf.

Item 4 seeks disclosure of "input provided by" Big Room Inc. ("BRI") and other organizations or individuals in support of the .ECO applications, BRI's responses to Clarifying Questions (if any) from the CPE Panel, as well as "other communications that have not been made public but have been reviewed and/or considered by the CPE Panel." In accordance with the Panel Process Document, the CPE Panel reviews documents and communications that are publicly available through a number of resources, such as: (a) BRI's application for .ECO available at https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails/1753; (b) the New gTLD Correspondence webpage[2] available at http://newgtlds.icann.org/en/program-status/correspondence; and (c) the Applicant Comment Forum[3] available at https://gtldcomment.icann.org/comments-feedback/applicationcomment/viewcomments.

[1] ICANN is not aware of any "other individuals or organizations" outside of the EIU and the CPE Panel that were "involved in the Community Priority Evaluation" of Big Room Inc.'s .ECO application.

[2] Some examples of communications from the Correspondence webpage relating to Big Room Inc.'s .ECO application include: Jim Leape, WWF International - https://www.icann.org/en/system/files/correspondence/leape-to-icann-26mar14-en.pdf; and Don Moody, Esq., The IP & Technology Legal Group, P.C., on behalf of Little Birch, LLC - https://www.icann.org/en/system/files/correspondence/moody-to-cpe-panel-26mar14-en.pdf.

[3] Some examples of comments from the Applicant Comment Forum relating to the Big Room Inc.'s .ECO application include: David Tunnah, Deloitte - https://gtldcomment.icann.org/comments-feedback/applicationcomment/commentdetails/11603; Peter ter Weeme, Junxion Strategy - https://gtldcomment.icann.org/comments-feedback/applicationcomment/commentdetails/5775; Gareth Hughes, Beetle Capital - https://gtldcomment.icann.org/comments-feedback/applicationcomment/commentdetails/4487; Adrian Dove, Congress of Racial Equality of California (CORE-CA) - https://gtldcomment.icann.org/comments-feedback/applicationcomment/commentdetails/12432; and John Adams - https://gtldcomment.icann.org/comments-feedback/applicationcomment/commentdetails/12423.

The CPE Panel also has the opportunity to ask Clarifying Questions of an applicant. To the extent such questions are asked and answered, the impact of those questions is then reflected within the CPE Report. The Clarifying Questions, part of the working methods of the CPE Panel, are not appropriate for ICANN to release.

As such, to the extent that ICANN has documentation responsive to Items 2, 3, 4 and 5, such documents are either already public or subject to certain of the Defined Conditions for Nondisclosure set forth in the DIDP:

- Internal information that, if disclosed, would or would be likely to compromise the integrity of ICANN's deliberative and decision-making process by inhibiting the candid exchange of ideas and communications, including internal documents, memoranda, and other similar communications to or from ICANN Directors, ICANN Directors' Advisors, ICANN staff, ICANN consultants, ICANN contractors, and ICANN agents.

- Information exchanged, prepared for, or derived from the deliberative and decision-making process between ICANN, its constituents, and/or other entities with which ICANN cooperates that, if disclosed, would or would be likely to compromise the integrity of the deliberative and decision-making process between and among ICANN, its constituents, and/or other entities with which ICANN cooperates by inhibiting the candid exchange of ideas and communications.

- Information provided to ICANN by a party that, if disclosed, would or would be likely to materially prejudice the commercial interests, financial interests, and/or competitive position of such party or was provided to ICANN pursuant to a nondisclosure agreement or nondisclosure provision within an agreement.

- Confidential business information and/or internal policies and procedures.

- Drafts of all correspondence, reports, documents, agreements, contracts, emails, or any other forms of communication.

Although your analysis in the Request concluded that no Conditions for Nondisclosure should apply, ICANN must independently undertake the analysis of each Condition as it applies to the documentation at issue, and make the final determination as to whether any Nondisclosure Conditions apply. Here, for example, ICANN cannot violate contractual conditions that require ICANN to maintain items as confidential solely because the Request proffers that no such conditions apply. Similarly, ICANN does not release draft documentation – particularly if draft documentation was shared for the purpose of facilitating deliberations or decision making – because drafts are not reliable sources of information regarding what actually occurred or standards that were actually applied.

For each of the items identified above as subject to Defined Conditions of Nondisclosure, ICANN has determined that there are no particular circumstances for which the public interest in disclosing the information outweighs the harm that may be caused to ICANN, its contractual relationships and its contractors' deliberative processes by the requested disclosure.

About DIDP

ICANN's DIDP is limited to requests for information already in existence within ICANN that is not publicly available. In addition, the DIDP sets forth Defined Conditions of Nondisclosure. To review a copy of the DIDP, please see https://www.icann.org/resources/pages/didp-2012-02-25-en. ICANN makes every effort to be as responsive as possible to the entirety of your Request.

We hope this information is helpful. If you have any further inquiries, please forward them to didp@icann.org.

Annex 9.

DETERMINATION
OF THE BOARD GOVERNANCE COMMITTEE (BGC)
RECONSIDERATION REQUEST 14-46

18 November 2014

The Requesters, Little Birch, LLC and Minds + Machines Group Limited (two of the four applicants for the .ECO string), seek reconsideration of the Community Priority Evaluation ("CPE") Panel's Report, and ICANN's acceptance of that Report, finding that Big Room Inc.'s ("Big Room's") application for .ECO prevailed in CPE for that string.[1] In light of the CPE results, the contention set for .ECO has been resolved and only Big Room's application will proceed.

I. Brief Summary.

The Requesters each submitted a standard (meaning not community-based) application for .ECO. Those applications were placed in a contention set with the other applications for .ECO, including Big Room's community-based application (the "Application"). As Big Room's Application was community-based, Big Room was invited to, and did, participate in CPE. Big Room's Application prevailed in CPE. As a result, the contention set for the .ECO string has been resolved and only Big Room's Application will proceed.

The Requesters do not identify any misapplication of any policy or procedure by ICANN or the CPE Panel. Rather, the Requesters simply disagree with the CPE Panel's determination and scoring of the Application, and challenge the substantive merits of the CPE Panel's Report.

[1] Reconsideration Request 14-46 lists both Little Birch, LLC and Minds + Machines Group Limited as Requesters. (Request, § 1, Pg. 1.) Accordingly, the Board Governance Committee treats this Request as having been submitted by both parties, notwithstanding the later representation that the Request is "not" brought on behalf of multiple persons or entities. (*Id.*, § 11, Pg. 11.)

Specifically, the Requesters contend that the CPE Panel improperly applied the first, second and fourth CPE criteria set forth in the Applicant Guidebook (the "Guidebook").[2]

Substantive disagreement with the CPE Panel's Report, however, is not a basis for reconsideration. Since the Requesters have failed to demonstrate that the CPE Panel acted in contravention of any established policy or procedure in rendering the Report, the BGC concludes that Request 14-46 be denied.

II. Facts.

A. Background Facts.

The Requesters each submitted a standard application for .ECO.[3] Those applications were placed in a contention set with other applications for .ECO, including Big Room's community-based application.[4]

On 12 March 2014, Big Room's Application for .ECO was invited to participate in CPE.[5] CPE is a method of resolving string contention, described in section 4.2 of the Guidebook. It will occur only if a community application is in contention and if that applicant elects to pursue CPE.

Big Room elected to participate in CPE for .ECO, and its Application was forwarded to the Economist Intelligence Unit ("EIU"), the CPE provider, for evaluation. On 7 October 2014, the Panel issued its report on Big Room's Application. The Report explained that the

[2] Request, §§ 7-8, Pgs. 3-10.

[3] *See* https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails/790; https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails/1523. Minds + Machines Group Limited is a wholly-owned subsidiary of Top Level Domain Holdings, Ltd, which is listed as the applicant for .ECO.

[4] *See* Contention Resolution Status, *available at* https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails/ 790.

[5] *See* http://newgtlds.icann.org/en/applicants/cpe.

Application met the CPE requirements specified in the Guidebook and therefore concluded that the Application prevailed in CPE.[6]

On 22 October 2014, the Requesters filed Request 14-46, requesting reconsideration of the Report, and ICANN's acceptance of that Report. The same day, Requester Little Birch, LLC filed a request pursuant to ICANN's Document Information Disclosure Policy ("DIDP"), seeking documents related to the CPE Panel's Report.[7]

On 31 October 2014, ICANN responded to the DIDP request.[8] ICANN identified and provided links to all publicly available documents, including comments and correspondence regarding the Application, which were posted on ICANN's website and considered by the CPE Panel.[9] ICANN noted that documents responsive to the requests were either: (1) already public; (2) not in ICANN's possession; or (3) not appropriate for public disclosure because they were subject to certain DIDP Nondisclosure Conditions.[10]

B. Relief Requested.

The Requesters ask the Board to: (a) "reconsider the Determination [by the CPE Panel], and in particular not award a passing score" to Big Room's Application; (b) "reconsider ICANN's decision that the Requester[s'] application[s] for the .eco gTLD 'Will Not Proceed' to contracting"; and (c) "restore the 'Application Status' of Requester[s'] application[s] and the Application submitted by [Big Room] to 'Evaluation Compete,' their respective 'Contention Resolution Statuses' to 'Active,' and their 'Contention Resolution Result' to 'In Contention.'"[11]

[6] *See* Report, *available at* https://www.icann.org/sites/default/files/tlds/eco/eco-cpe-1-912-59314-en.pdf.

[7] *See* DIDP Request, *available at* https://www.icann.org/en/system/files/files/levy-request-22oct14-en.pdf.

[8] *See* DIDP Response, *available at* https://www.icann.org/en/system/files/files/levy-response-31oct14-en.pdf.

[9] *Id.*, Pg. 3.

[10] *Id.*, Pgs. 2-5.

[11] Request, §§ 8-9, Pgs. 10-11. The Requesters "reserve[d] the right to supplement [their] Reconsideration Request with further information and arguments following the outcome of their [DIDP Request], even if no additional information would be provided by ICANN." (*Id.*, § 7, Pg. 11.) ICANN responded to the DIDP Request on 31 October 2014, and asked that the Requesters submit supplemental materials, if any, by 11 November 2014. The Requesters did not submit any supplemental materials by that date.

III. Issues.

In view of the claims set forth in the Request, the issues for reconsideration are whether the CPE Panel violated established policy or procedure by failing to properly apply the CPE criteria in evaluating Big Room's Application.[12]

IV. The Relevant Standards for Evaluating Reconsideration Requests and Community Priority Evaluation.

ICANN's Bylaws provide for reconsideration of a Board or staff action or inaction in accordance with specified criteria.[13] Dismissal of a request for reconsideration of staff action or inaction is appropriate if the BGC concludes, and the Board or the NGPC[14] agrees to the extent that the BGC deems that further consideration by the Board or NGPC is necessary, that the requesting party does not have standing because the party failed to satisfy the reconsideration criteria set forth in the Bylaws. The reconsideration process can properly be invoked for challenges to determinations rendered by panels formed by third party service providers, such as the EIU, where it can be stated that a panel failed to follow the established policies or procedures in reaching its determination, or that staff failed to follow its policies or procedures in accepting that determination.[15]

In the context of the New gTLD Program, the reconsideration process does not call for the BGC to perform a substantive review of CPE reports. Accordingly, the BGC does not

[12] Request, § 8, Pgs. 3-10.

[13] Bylaws, Art. IV, § 2. Article IV, § 2.2 of ICANN's Bylaws states in relevant part that any entity may submit a request for reconsideration or review of an ICANN action or inaction to the extent that it has been adversely affected by:

> (a) one or more staff actions or inactions that contradict established ICANN policy(ies); or
> (b) one or more actions or inactions of the ICANN Board that have been taken or refused to be taken without consideration of material information, except where the party submitting the request could have submitted, but did not submit, the information for the Board's consideration at the time of action or refusal to act; or
> (c) one or more actions or inactions of the ICANN Board that are taken as a result of the Board's reliance on false or inaccurate material information.

[14] New gTLD Program Committee.

[15] *See* http://www.icann.org/en/groups/board/governance/reconsideration/recommendation-booking-01aug13-en.doc, BGC Recommendation on Reconsideration Request 13-5.

evaluate the CPE Panel's substantive conclusion that the Application prevailed in CPE. Rather, the BGC's review is limited to whether the CPE Panel violated any established policy or procedure.

The standards governing CPE are set forth in Section 4.2 of the Guidebook. In addition, the EIU – the firm selected to perform CPE – has published supplementary guidelines (the "CPE Guidelines") that provide more detailed scoring guidance, including scoring rubrics, definitions of key terms, and specific questions to be scored.[16]

CPE will occur only if a community-based applicant selects CPE and after all applications in the contention set have completed all previous stages of the gTLD evaluation process.[17] CPE is performed by an independent community priority panel appointed by the EIU.[18] A CPE panel's role is to determine whether the community-based applicant fulfills the four community priority criteria set forth in Section 4.2.3 of the Guidebook. The four criteria include: (i) community establishment; (ii) nexus between proposed string and community; (iii) registration policies; and (iv) community endorsement.[19] To prevail in CPE, an applicant must receive a minimum of 14 points on the scoring of the foregoing four criteria, each of which is worth a maximum of four points (for a total of 16 points).[20]

V. Analysis and Rationale.

The Requesters object to the CPE Panel's decision to award 14 out of the possible 16 points to Big Room's Application, a score sufficient for the Application to prevail in CPE. As noted above, in the context of the New gTLD Program, the reconsideration process does not call for the BGC to evaluate the CPE Panel's substantive conclusion that the Application prevailed in

[16] *See* CPE Guidelines, *available at* http://newgtlds.icann.org/en/announcements-and-media/announcement-27sep13-en.
[17] Guidebook, § 4.2.
[18] *Id*., § 4.2.2.
[19] *Id*., § 4.2.3.
[20] *Id*.

CPE. Rather, the BGC's review is limited to whether the Panel (or staff) violated any established policy or procedure. As discussed below, insofar as the Requesters claim that the number of points awarded by the CPE Panel for various criteria was "wrong," the Requesters do not claim that the CPE Panel violated established policy or procedure, but instead challenge the substantive determinations of the Panel. That is not a basis for reconsideration.

1. The CPE Panel Properly Applied the First CPE Criterion.

The Requesters claim that the CPE Panel improperly awarded the Application four out of four points on the first criterion, which assesses the community identified in an application.[21] Specifically, this criterion evaluates "the community as explicitly identified and defined according to statements in the application" through the scoring of two elements, each worth two points—1-A, "Delineation," and 1-B, "Extension."[22]

In awarding four out of four points for the first criterion, the CPE Panel accurately described and applied the Guidebook scoring guidelines and CPE Guidelines.[23] The Guidebook defines community as "implying more [] cohesion than a mere commonality of interest," and requiring "an awareness and recognition of a community among its members."[24] The CPE Panel found that "based on [its] research and the materials provided in the application, the community members as defined in the application demonstrate the 'cohesion' required by the [Guidebook]."[25] Specifically, the CPE Panel noted that each of the four categories of members defined in the Application—not-for profit environmental associations, government agencies with environmental missions, individuals, and businesses—have "cohesion and awareness [] founded in their demonstrable involvement in environmental activities" and "demonstrate active

[21] Guidebook, § 4.2.3; *see also* Request, § 8, Pgs. 3-5.
[22] Guidebook, § 4.2.3.
[23] Report, Pgs. 1-5.
[24] Guidebook, § 4.2.3.
[25] Report, Pg. 2.

commitment, practice and reporting."[26]

In challenging the Report, the Requesters do not identify any policy or procedure that the CPE Panel misapplied in scoring the first criterion. Rather, the Requesters argue that the Application's community definition "is [] not a definition of a community but a vague overview [of] what its membership is considered by Big Room [] to consist of."[27] In the Requesters' view, the community does not have, as required by the Guidebook, "more cohesion than a mere commonality of interest."[28] They contend that while members of the defined community "may 'associate' themselves with [the] issues and activities [identified in the Application], [] this does not prove that there is an 'awareness and recognition' of a community in the sense of the [Guidebook]."[29] However, the Requesters' arguments reflect only a substantive disagreement with the CPE Panel's conclusions. As discussed, such a substantive disagreement is not a proper basis for reconsideration.

2. The CPE Panel Properly Applied the Second CPE Criterion.

The Requesters claim that the CPE Panel improperly awarded the Application two out of three points on element 2-A of the second criterion, "Nexus."[30] Pursuant to Section 4.2.3 of the Guidebook, to receive a maximum score for element 2-A, "Nexus," the applied-for string must "match[ ] the name of the community or [be] a well-known short-form or abbreviation of the community name."[31] An application is eligible for two points on element 2-A if the applied-for string "identifies the community, but does not qualify for a score of 3."[32]

In scoring element 2-A, the CPE Panel accurately described and applied the Guidebook

[26] *Id*.
[27] Request, § 8, Pg. 3.
[28] *Id*., § 8, Pg. 4 (quoting Guidebook, § 4.3.2).
[29] *Id*.
[30] Request, § 8, Pgs. 5-8.
[31] Guidebook, § 4.2.3.
[32] *Id*.

scoring guidelines and CPE Guidelines.[33] The CPE Panel determined that the Application did not merit a score of three points because .ECO was "not a match of the name of the community or a well-known short-form or abbreviation of the community name."[34] However, the CPE Panel determined that "because of the common association of the prefix 'eco' with various phrases closely associated with environmental protection . . . [the applied-for string] d[id] identify the community, without substantially overreaching beyond the community."[35] As such, the CPE Panel determined that, pursuant to the Guidebook, the Application merited a score of two points.[36]

In challenging the Report, the Requesters do not identify any policy or procedure that the CPE Panel misapplied in scoring element 2-A. Instead, the Requesters disagree with the CPE Panel's analysis, asserting that "the string 'eco' does not 'closely describe' the community or the community members, and that it certainly over-reaches substantially beyond the community referred to in the application."[37] The Requesters contend that "many of the members of the organizations referred to in the Application are far from being liaised with 'ecological' or 'environmental' activities."[38] They also argue that "[i]n [their] view, the CPE Panel [did not] consider[] the many other meanings of the term 'eco'" and therefore "erroneously determined" that the applied-for string identified that community.[39] Again, however, the Requesters' substantive disagreement with the CPE Panel's findings is not a proper basis for reconsideration.

3. The CPE Panel Properly Applied the Fourth CPE Criterion.

Finally, the Requesters claim that the CPE Panel improperly awarded the Application two

[33] Report, Pgs. 5-6.
[34] *Id.*, Pg. 6.
[35] *Id.*
[36] *Id.*
[37] Request, § 8, Pg. 5.
[38] *Id.*, § 8, Pg. 7.
[39] *Id.*, § 8, Pgs. 6-7.

out of two points on element 4-B of the fourth criterion.[40] Element 4-B, "Opposition," evaluates the existence or absence of community opposition to an application. In order to receive the maximum score on element 4-B, an application must have received "no opposition of relevance."[41] Relevant opposition must come from a group of "non-negligible size," which is part of a community "explicitly or implicitly addressed" by the applied-for string.[42]

In awarding two out of two points for element 4-B, the CPE Panel accurately described and applied the Guidebook scoring guidelines and CPE Guidelines.[43] The CPE Panel determined that while the Application had received letters of opposition, those letters were not relevant, "as they were either from individuals or groups of negligible size" or from communities "which were not mentioned in the application" and "have no association to the applied-for string."[44]

In challenging the Report, the Requesters do not identify any policy or procedure that the CPE Panel misapplied in scoring element 4-B. Instead, they argue that the Panel did not detail "which criteria and standards have been used in determining whether [the] letters [of opposition] were from groups, individuals or communities 'of negligible size' that had an association to the applied for string."[45] However, as noted above, in scoring element 4-B, the CPE Panel correctly described the Guidebook scoring guidelines and answered the mandatory questions listed in the CPE Guidelines.[46]

The Requesters also argue that because the CPE Panel did not identify the letters of opposition it considered, "it is impossible for [the Requesters] to review whether the

[40] *Id.*, § 8, Pgs. 8-9.
[41] Guidebook, § 4.2.3.
[42] *Id.*
[43] Report, Pgs. 8-9.
[44] *Id.*, Pg. 9.
[45] Request, § 8, Pg. 8.
[46] Report, Pgs. 8-9; *see also* CPE Guidelines, Pgs. 19-20.

[Application] had indeed satisfied [element 4-B]."[47] It should be noted that all of the letters of opposition are publicly available to the Requester, either in the Application Comments[48] or ICANN's New gTLD Correspondence.[49] Moreover, the Requesters identify no policy or procedure requiring CPE panels to identify in the CPE reports the names of objectors (because none exists). As such, the Requesters have not identified a proper basis for reconsideration with respect to the CPE Panel's scoring of element 4-B.

VI. Determination.

Based on the foregoing, the BGC concludes that the Requesters have not stated proper grounds for reconsideration, and therefore denies Request 14-46. As there is no indication that either the CPE Panel or ICANN violated any ICANN policy or procedure with respect to the Report, or ICANN's acceptance of the Report, Request 14-46 should not proceed. If the Requesters believe that they have somehow been treated unfairly in the process, the Requesters are free to ask the Ombudsman to review this matter.

The Bylaws provide that the BGC is authorized to make a final determination for all Reconsideration Requests brought regarding staff action or inaction and that no Board (or NGPC) consideration is required.[50] As discussed above, Request 14-46 seeks reconsideration of a staff action or inaction. As such, after consideration of this Request, the BGC concludes that this determination is final and that no further consideration by the Board is warranted.

[47] Request, § 8, Pgs. 8-9.

[48] *See* https://gtldcomment.icann.org/applicationcomment/viewcomments.

[49] *See* http://newgtlds.icann.org/en/program-status/correspondence.

[50] Bylaws, Art. IV, § 2.15.

crowell moring

Annex 10.

Translations Français Español العربية

Русский

Log In Sign Up

Search ICANN.org

ICANN

GET STARTED NEWS & MEDIA POLICY PUBLIC COMMENT **RESOURCES**

COMMUNITY IANA STEWARDSHIP & ACCOUNTABILITY

Resources

- About ICANN
- Board
- Accountability & Transparency
- Governance
- Groups
- Contractual Compliance
- Registrars
- Registries
- Operational Metrics
- Identifier Systems

Minutes | Board Governance Committee (BGC) Meeting

18 Nov 2014

BGC Attendees: Mike Silber, Suzanne Woolf, Gonzalo Navarro, Bruce Tonkin, and Chris Disspain – Chair

BGC Member Apologies: Cherine Chalaby and Erika Mann

Other Board Member Attendees: Steve Crocker

Executive and Staff Attendees: John Jeffrey (General Counsel and Secretary), Megan Bishop (Board Support Coordinator), Michelle Bright (Board Support Manager), Christine Willet (Vice President, gTLD Operations), and Amy Stathos (Deputy General Counsel)

The following is a summary of discussions, actions taken, and actions identified:

1. Minutes – The BGC approved the minutes from the meeting on 23 October 2014.
2. Reconsideration Request 14-43 – Suzanne Woolf abstained

Security, Stability and Resiliency (IS-SSR)

- ccTLDs
- Internationalized Domain Names
- Universal Acceptance Initiative
- Policy
- Public Comment
- Contact
- Help

from participation in this matter noting potential conflicts; Suzanne indicated that she provides consulting services for an interested applicant and, while not material to this particular decision, she would abstain to prevent any perception of bias. Staff briefed the BGC regarding the city of Spa, Belgium's ("Requester's") request seeking reconsideration of ICANN's decision to process the applications for the gTLD string .SPA as non-geographic name applications. On 21 October 2014, the Requester filed Reconsideration Request 14-43 claiming that ICANN's conduct violated applicable policies and procedures because it contends that: (i) ICANN violated provisions of the new gTLD Applicant Guidebook; and (ii) ICANN contravened the GAC's advice. After discussion and consideration of the Reconsideration Request, the BGC concluded that the Requester has not demonstrated that ICANN acted in contravention of established policy or procedure and, therefore, determined that Request 14-43 be denied. The Bylaws authorize the BGC to make a final determination on Reconsideration Requests brought regarding staff action or inaction and the BGC concluded that its determination on Request 14-43 is final; no consideration by the NGPC is warranted.

3. Reconsideration Request 14-45 – Suzanne Woolf and Bruce Tonkin abstained from participation in this matter noting potential conflicts. Suzanne indicated that she provides consulting services for an interested applicant and Bruce indicated that his employer uses another interested applicant as a significant supplier. While these affiliations are not material to this particular decision, Suzanne and Bruce abstained in order to prevent any perception of bias. Staff briefed the BGC regarding .music LLC's ("Requester's") request seeking reconsideration of the Community Priority Evaluation ("CPE") Panel's report (the "Report), and ICANN's acceptance of that Report, finding that the Requester did not prevail in CPE for .MUSIC. On 22 October 2014, the Requester filed Reconsideration Request 14-45 claiming that the CPE Panel: (i) improperly applied the CPE criteria; and (ii) failed to ask the Requester clarifying questions and give it an opportunity to respond to letters submitted in opposition to the Requester's application for .MUSIC. After discussion and consideration of

the Reconsideration Request, the BGC concluded that the Requester has not demonstrated that the CPE Panel acted in contravention of established policy or procedure in rendering the Report and, therefore, determined that Request 14-45 be denied. The Bylaws authorize the BGC to make a final determination on Reconsideration Requests brought regarding staff action or inaction and the BGC concluded that its determination on Request 14-45 is final; no consideration by the NGPC is warranted.

4. Reconsideration Request 14-46 – Suzanne Woolf abstained from participation in this matter noting potential conflicts; Suzanne indicated that she provides consulting services for an interested applicant and, while not material to this particular decision, she would abstain to prevent any perception of bias. Staff briefed the BGC regarding Little Birch, LLC and Minds + Machines Group Limited's ("Requesters'") request seeking reconsideration of the Community Priority Evaluation ("CPE") Panel's report (the "Report), and ICANN's acceptance of that Report, finding that Big Room Inc.'s application for .ECO prevailed in CPE for that string. On 22 October 2014, the Requesters filed Reconsideration Request 14-46 claiming that the CPE Panel improperly applied the first, second and fourth CPE criteria set forth in the Applicant Guidebook. After discussion and consideration of the Reconsideration Request, the BGC concluded that the Requester has not demonstrated that the CPE Panel acted in contravention of established policy or procedure in rendering the Report and, therefore, determined that Request 14-46 be denied. The Bylaws authorize the BGC to make a final determination on Reconsideration Requests brought regarding staff action or inaction and the BGC concluded that its determination on Request 14-46 is final; no consideration by the NGPC is warranted.

5. Review Conflicts of Interest Disclosure Forms for New Board Members – Staff provided the BGC with an overview of the process and a summary of the conflict of interest disclosure forms and the New gTLD questionnaires submitted by the newest Board members— Rinalia Abdul Rahim, Asha Hemrajani, and Markus Kummer. The BGC reviewed the forms submitted by the new Board members and noted that, based

upon the disclosures presented, there are no issues requiring further evaluation.

- Action: Staff to inform the new Board members of the on-going need to notify the General Counsel's office if they or their employers become affiliated with new entities that may create a actual, potential or potentially perceived perception of conflict or interest related to ICANN.

6. Reconstitution of the BGC Sub-Committee on Conflicts and Ethics Relating To New gTLDs – Staff provided an overview of the prior membership of the BGC Sub-Committee on Conflicts and Ethics relating to New gTLDs ("Sub-Committee"). The BGC discussed the matter and decided that the new membership of the Sub-Committee would consist of Chris Disspain, Gonzalo Navarro and Cherine Chalaby. The BGC also discussed the current scope of the Charter of the Sub-Committee and potentially broadening the scope of the Charter.

   - Action: Staff to draft proposed adjustments to the Charter of the Sub-Committee for BGC consideration at a future meeting.

7. Upcoming Reconsideration Requests – Staff provided an overview and the BGC briefly discussed the upcoming Reconsideration Requests and information that staff would provide to the BGC in advance of review of those Requests.

Published on 20 January 2015

You Tube

Tw tter

L nkedIn

F ckr

Facebook

RSS Feeds

Commun ty W k

ICANN B og

Privacy Policy Terms of Service

Cookie Policy

Who We Are

Get Started

Learning

Participate

Groups

Board

President's Corner

Staff

Careers

Newsletter

Contact Us

Offices

Customer Service

Security Team

PGP Keys

Certificate Authority

Registry Liaison

AOC Review

Organizational Reviews

Request a Speaker

For Journalists

Accountability & Transparency

Accountability Mechanisms

Independent Review Process

Request for Reconsideration

Ombudsman

Governance

Documents

Agreements

AOC Review

Annual Report

Financials

Document Disclosure

Planning

Dashboard

RFPs

Litigation

Correspondence

Help

Dispute Resolution

Domain Name Dispute Resolution

Name Collision

Registrar Problems

WHOIS

crowell moring

Annex 11.

Government of Canada Gouvernement du Canada

Canada

Industry Canada

Home > Corporations > Corporations Canada > Search for a Federal Corporation

Corporations Canada

Federal Corporation Information - 6873138

Glossary of Terms used on this page
Return to Search Results

Start New Search

Corporation Number
Confidential Information Redacted

Business Number (BN)
Confidential Information Redacted

Governing Legislation
Canada Business Corporations Act - 2007-11-14

Corporate Name
BIG ROOM INC.

Status
Active

Registered Office Address

Care of: Lawson Lundell LLP
Contact Information Redacted

Active CBCA corporations are required to update this information within 15 days of any change. A corporation key is required.

Directors

Minimum
1
Maximum
12

Directors
DAVID LEVI
Contact Information Redacted

JACOB MALTHOUSE
Contact Information Redacted

NICHOLAS FITZPATRICK
Contact Information
Redacted

Contact Information Redacted

TREVOR BOWDEN
Contact Information Redacted

Active CBCA corporations are required to update director information (names, addresses, etc.) within 15 days of any change. A corporation key is required.

Annual Filings

Anniversary Date (MM-DD)
11-14

Date of Last Annual Meeting
2014-03-30

Annual Filing Period (MM-DD)
11-14 to 01-13

Type of Corporation
Non-distributing corporation with 50 or fewer shareholders

Status of Annual Filings
2015 - Not due
2014 - Filed
2013 - Filed

Corporate History

Corporate Name History

2007-11-14 to 2007-12-04
SOMBRIO NETWORKS INC.

2007-12-04 to Present
BIG ROOM INC.

Certificates and Filings

Certificate of Incorporation
2007-11-14

Certificate of Amendment *
2007-12-04
Amendment details: Corporate name

Certificate of Amendment *
2011-07-25
Amendment details: Other

Certificate of Amendment *
2013-03-11
Amendment details: Other

Certificate of Amendment *
2014-07-30
Amendment details: Other

* Amendment details are only available for amendments effected after 2010-03-20. Some certificates issued prior to 2000 may not be listed. For more information, contact Corporations Canada.