

---

# Application number: 1-1873-71868 for Nameshop

Generated on 30 May 2012

---

## Applied-for gTLD string

---

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

IDN

---

**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, 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.**

---

**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. If an IDN, describe the applicant's efforts to ensure that there are no known operational or rendering problems. If such issues are known, describe steps that will be taken to mitigate these issues in software and other applications.**

Nameshop anticipates the introduction of .IDN without operational or rendering problems. Based on a decade of experience launching and operating new TLDs, Afilias, the back-end provider of registry services for this TLD, is confident the launch and operation of this TLD presents no known challenges. The rationale for this opinion includes:

- The string is not complex and is represented in standard ASCII characters and follows relevant technical, operational and policy standards;
  - The string length is within lengths currently supported in the root and by ubiquitous Internet programs such as web browsers and mail applications;
  - There are no new standards required for the introduction of this TLD;
  - No onerous requirements are being made on registrars, registrants or Internet users, and;
  - The existing secure, stable and reliable Afilias SRS, DNS, WHOIS and supporting systems and staff are amply provisioned and prepared to meet the needs of this TLD.
- 

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

---

**Mission/Purpose**

---

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

The purpose of the proposed gTLD is to offer a bridge for the Internationalized Domain Name Registrant to connect to users beyond their own language communities. This gTLD would be of help in furthering the Internet Community's efforts to preserve the Internet as a unified, Global space.

The proposed gTLD .IDN supports multiple cultural, linguistic and ethnic communities across the world by helping communities connect to the rest of the world across the barrier of language.

---

### **18(b). How proposed gTLD will benefit registrants, Internet users, and others.**

i) The proposed gTLD .IDN supports multiple cultural, linguistic and ethnic communities across the world by helping communities connect to the rest of the world across the barrier of language.

ii) The proposed gTLD, .IDN is intended to serve users of various different languages, irrespective of whether the presence of the language is wide or global. Even if the language or script is completely unfamiliar to the global user, the global user will find it easier to decipher the internationalized domain name in a script completely unfamiliar to him or her.

iii) While Internationalized Domain Names enable users to connect within their language communities, the proposed gTLD would connect users from different communities to connect across communities.

iv) The applicant intends to follow ICANN policies by the book, and is inclined to take advice from Community Members to build up this TLD space as one with high ethical standards.

v) Nameshop would follow the recommendation of the Community whois working groups and ICANN whois policy and privacy policies to protect the privacy and confidential information of the users.

The proposed registry would engage communication experts from various regions in its effort to reach the benefits of this TLD to users across language communities.

---

### **18(c). Describe operating rules to eliminate or minimize social costs or financial resource costs, various types of consumer vulnerabilities.**

1. Nameshop is committed to follow ICANN policies and community recommendations in resolving multiple application issues. The proposed Registry would pay attention to Trade Mark considerations in tune with ICANN's UDRP policy considerations and where there are no conflicts with ICANN policy or community recommendations, would consider auctions where there are more than TWO applications in situations where there is a permitted time-lag between domain application and registration, if permissible. Otherwise the applicant is inclined to follow the first come first served policy where there are no visible indications of an intent to unethically profit from the registration.

2) Nameshop would consider introductory discounts, and would also consider

bulk registration discounts as long as bulk registrations are not done with an intent to squat on domains irrelevant to the apparent Registrant.

3) Nameshop intends to assure Registrants that there would be no abnormal increases in prices out of tune with economic inflation or cost levels, but would consult ethical and long standing business experts from the Domain industry before making contractual commitments that could lead to legal complications or making contractual commitments potentially out of tune with established good business practices.

---

## 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. If this application is included in a community priority evaluation, it will be scored based on the community identified in response to this question.**

---

**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. Policies and enforcement mechanisms are expected to constitute a coherent set.**

---

**20(f). Attach any written endorsements from institutions/groups representative of the community identified in 20(a). An applicant may submit endorsements by multiple institutions/groups, if relevant to the community.**

---

## **Geographic Names**

---

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

No

---

**21(b). If a geographic name, attach documentation of support or non-objection from all relevant governments or public authorities.**

---

## **Protection of Geographic Names**

---

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

Nameshop commits to protect names with national or geographic significance by reserving the country and territory names at the second level and at all other levels within the TLD, as per the requirements in the New TLD Registry Agreement (Specification 5, paragraph 5).

We will employ a series of rules to translate the geographical names required to be reserved by Specification 5, paragraph 5 to a form consistent with the "host names" format used in domain names.

Considering the Governmental Advisory Committee (GAC) advice "Principles regarding new gTLDs", these domains will be blocked, at no cost to governments, public authorities, or IGOs, before the TLD is introduced (Sunrise), so that no parties may apply for them. We will publish a list of these names before Sunrise, so our registrars and their prospective applicants can be aware that these names are reserved.

We will define a procedure so that governments can request the above reserved domain(s) if they would like to take possession of them. This procedure will be based on existing methodology developed for the release of country names in the .INFO TLD. For example, we will require a written request from the country's GAC representative, or a written request from the country's relevant Ministry or Department. We will allow the designated beneficiary

(the Registrant) to register the name, with an accredited Afiliias Registrar, possibly using an authorization number transmitted directly to the designated beneficiary in the country concerned.

As defined by Specification 5, paragraph 5, such geographic domains may be released to the extent that Registry Operator reaches agreement with the applicable government(s). Registry operator will work with respective GAC representatives of the country's relevant Ministry of Department to obtain their release of the names to the Registry Operator.

If internationalized domains names (IDNs) are introduced in the TLD in the future, we will also reserve the IDN versions of the country names in the relevant script(s) before IDNs become available to the public. If we find it advisable and practical, we will confer with relevant language authorities so that we can reserve the IDN domains properly along with their variants.

Regarding GAC advice regarding second-level domains not specified via Specification 5, paragraph 5: All domains awarded to registrants are subject to the Uniform Domain Name Dispute

Resolution Policy (UDRP), and to any properly-situated court proceeding. We will ensure appropriate procedures to allow governments, public authorities or IGO's to challenge abuses of names with national or geographic significance at the second level. In its registry-registrar agreement, and flowing down to registrar-registrant agreements, the registry operator will institute a provision to suspend domains names in the event of a dispute. We may exercise that right in the case of a dispute over a geographic name.

---

## Registry Services

---

**23. Provide name and full description of all the Registry Services to be provided. Descriptions should include both technical and business components of each proposed service, and address any potential security or stability concerns. The following registry services are customary services offered by a registry operator:**

**A. Receipt of data from registrars concerning registration of domain names and name servers.**

**B. Dissemination of TLD zone files.**

**C. Dissemination of contact or other information concerning domain name registrations (Whois service).**

**D. Internationalized Domain Names, where offered.**

**E. DNS Security Extensions (DNSSEC).**

**The applicant must describe whether any of these registry services are intended to be offered in a manner unique to the TLD.**

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

Throughout the technical portion (#23 - #44) of this application, answers are provided directly from Afilias, the back-end provider of registry services for this TLD. Nameshop chose Afilias as its back-end provider 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 this 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. This TLD will utilize an existing, proven team and platform for registry services with:

- A stable and secure, state-of-the-art, EPP-based SRS with ample storage capacity, data security provisions and scalability that is proven with registrars who account for over 95% of all gTLD domain name registration activity (over 375 registrars);
- A reliable, 100% available DNS service (zone file generation, publication and dissemination) tested to withstand severe DDoS attacks and dramatic growth in Internet use;
- A WHOIS service that is flexible and standards compliant, with search capabilities to address both registrar and end-user needs; includes consideration for evolving standards, such as RESTful, or draft-kucherawy-wierds;
- Experience introducing IDNs in the following languages: German (DE), Spanish (ES), Polish (PL), Swedish (SV), Danish (DA), Hungarian (HU), Icelandic (IS), Latvian (LV), Lithuanian (LT), Korean (KO), Simplified and Traditional Chinese (CN), Devanagari (HI-DEVA), Russian (RU), Belarusian (BE), Ukrainian (UK), Bosnian (BS), Serbian (SR), Macedonian (MK) and Bulgarian (BG) across the TLDs it serves;
- A registry platform that is both IPv6 and DNSSEC enabled;
- An experienced, respected team of professionals active in standards development of innovative services such as DNSSEC and IDN support;
- Methods to limit domain abuse, remove outdated and inaccurate data, and ensure the integrity of the SRS, and;
- Customer support and reporting capabilities to meet financial and administrative needs, e.g., 24x7 call center support, integration support, billing, and daily, weekly, and monthly reporting.

Afilias will support this TLD in accordance with the specific policies and procedures of Nameshop (the "registry operator"), leveraging a proven registry infrastructure that is fully operational, staffed with professionals, massively provisioned, and immediately ready to launch and maintain this TLD.

The below response includes a description of the registry services to be provided for this TLD, additional services provided to support registry operations, and an overview of Afilias' approach to registry management.

## Registry services to be provided

To support this TLD, Nameshop and Afiliás 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 Afiliás DNS system, run and managed by Afiliás, is a massively provisioned DNS infrastructure that utilizes among the most sophisticated DNS architecture, hardware, software and redundant design created. Afiliás' 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: Afiliás' 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

Afiliás addresses security in every significant aspect - physical, data and network as well as process. Afiliás' 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 Afiliás mitigation plans are defined in our response to question #30(b); please see that response for complete information. In short, Afiliás is committed to ensuring the confidentiality, integrity, and availability of all information.

## New registry services

No new registry services are planned for the launch of this TLD.



#### Additional services to support registry operation

Numerous supporting services and functions facilitate effective management of the TLD. These support services are also supported by Afilias, including:

- Customer support: 24x7 live phone and e-mail support for customers to address any access, update or other issues they may encounter. This includes assisting the customer identification of the problem as well as solving it. Customers include registrars and the registry operator, but not registrants except in unusual circumstances. Customers have access to a web-based portal for a rapid and transparent view of the status of pending issues.
- Financial services: billing and account reconciliation for all registry services according to pricing established in respective agreements.

Reporting is an important component of supporting registry operations. Afilias will provide reporting to the registry operator and registrars, and financial reporting.

#### Reporting provided to registry operator

Afilias provides an extensive suite of reports to the registry operator, including daily, weekly and monthly reports with data at the transaction level that enable the registry operator to track and reconcile at whatever level of detail preferred. Afilias provides the exact data required by ICANN in the required format to enable the registry operator to meet its technical reporting requirements to ICANN.

In addition, Afilias offers access to a data warehouse capability that will enable near real-time data to be available 24x7. This can be arranged by informing the Afilias Account Manager regarding who should have access. Afilias' data warehouse capability enables drill-down analytics all the way to the transaction level.

#### Reporting available to registrars

Afilias provides an extensive suite of reporting to registrars and has been doing so in an exemplary manner for more than ten years. Specifically, Afilias provides daily, weekly and monthly reports with detail at the transaction level to enable registrars to track and reconcile at whatever level of detail they prefer.

Reports are provided in standard formats, facilitating import for use by virtually any registrar analytical tool. Registrar reports are available for download via a secure administrative interface. A given registrar will only have access to its own reports. These include the following:

- Daily Reports: Transaction Report, Billable Transactions Report, and Transfer Reports;
- Weekly: Domain Status and Nameserver Report, Weekly Nameserver Report, Domains Hosted by Nameserver Weekly Report, and;
- Monthly: Billing Report and Monthly Expiring Domains Report.

Weekly registrar reports are maintained for each registrar for four weeks. Weekly reports older than four weeks will be archived for a period of six months, after which they will be deleted.

#### Financial reporting

Registrar account balances are updated real-time when payments and withdrawals are posted to the registrars' accounts. In addition, the registrar account balances are updated as and when they perform billable transactions at the registry level.

Afilias provides Deposit/Withdrawal Reports that are updated periodically to reflect payments received or credits and withdrawals posted to the registrar accounts.

The following reports are also available: a) Daily Billable Transaction Report, containing details of all the billable transactions performed by all the registrars in the SRS, b) daily e-mail reports containing the number of domains in the registry and a summary of the number and types of billable transactions performed by the registrars, and c) registry operator versions of most registrar reports (for example, a daily Transfer Report that details all transfer activity between all of the registrars in the SRS).

#### Afilias approach to registry support

Afilias, the back end registry services provider for this TLD, is dedicated to managing the technical operations and support of this TLD in a secure, stable and reliable manner. Afilias has worked closely with Nameshop to review specific needs and objectives of this TLD. The resulting comprehensive plans are illustrated in technical responses #24-44, drafted by Afilias given Nameshop requirements. Afilias and Nameshop also worked together to provide financial responses for this application which demonstrate cost and technology consistent with the size and objectives of this TLD.

Afilias is the registry services provider for this and several other TLD applications. Over the past 11 years of providing services for gTLD and ccTLDs, Afilias has accumulated experience about resourcing levels necessary to provide high quality services with conformance to strict service requirements. Afilias currently supports over 20 million domain names, spread across 16 TLDs, with over 400 accredited registrars.

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

With over a decade of registry experience, Afilias has the depth and breadth of experience that ensure existing and new needs are addressed, all while meeting or exceeding service level requirements and customer expectations. This is evident in Afilias' participation in business, policy and technical organizations supporting registry and Internet technology within ICANN and related organizations. This allows Afilias to be at the forefront of security initiatives such as: DNSSEC, wherein Afilias worked with Public Interest Registry (PIR) to make the .ORG registry the first DNSSEC enabled gTLD and the largest TLD enabled at the time; in enhancing the Internet experience for users across the globe by leading development of IDNs; in pioneering the use of open-source technologies by its usage of PostgreSQL, and; being the first to offer near-real-time dissemination of DNS zone data.

The ability to observe tightening resources for critical functions and the capacity to add extra resources ahead of a threshold event are factors that

Afilias is well versed in. Afilias' human resources team, along with well-established relationships with external organizations, enables it to fill both long-term and short-term resource needs expediently.

Afilias' growth from a few domains to serving 20 million domain names across 16 TLDs and 400 accredited registrars indicates that the relationship between the number of people required and the volume of domains supported is not linear. In other words, servicing 100 TLDs does not automatically require 6 times more staff than servicing 16 TLDs. Similarly, an increase in the number of domains under management does not require in a linear increase in resources. Afilias carefully tracks the relationship between resources deployed and domains to be serviced, and pro-actively reviews this metric in order to retain a safe margin of error. This enables Afilias to add, train and prepare new staff well in advance of the need, allowing consistent delivery of high quality services.

---

## **Demonstration of Technical & Operational Capability (External)**

---

**24. Shared Registration System (SRS) Performance: describe the plan for operation of a robust and reliable Shared Registration System. SRS is a critical registry function for enabling multiple registrars to provide domain name registration services in the TLD.**

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS WHICH ICANN INFORMS US (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE, ACCORDING TO SPECIFIC GUIDANCE FROM ICANN UNDER CASE ID 11027.

---

**25. Extensible Provisioning Protocol (EPP): provide a detailed description of the interface with registrars, including how the applicant will comply with Extensible Provisioning Protocol in the relevant RFCs, including but not limited to: RFCs 3735, and 5730-5734. Provide the EPP templates and schemas that will be used. Include resourcing plans (number and description of personnel roles allocated to this area).**

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS, WHICH ICANN INFORMS US (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE, ACCORDING TO SPECIFIC GUIDANCE FROM ICANN UNDER CASE ID 11027.

---

**26. Whois: describe how the applicant will comply with ICANN's Registry Publicly Available Registration Data (Whois) specifications for data objects, bulk access, and lookups as defined in Specifications 4 and 6 to the registry agreement. Describe how the Applicant's Registry Publicly Available Registration Data (Whois) service will comply with RFC 3912. Describe resourcing plans (number and description of personnel roles allocated to this area).**

Answers for this question (#26) are provided by Afiliias, the back-end provider of registry services for this TLD.

Afiliias operates the WHOIS (registration data directory service) infrastructure in accordance with RFCs and global best practices, as it does for the 16 TLDs it currently supports. Designed to be robust and scalable, Afiliias' WHOIS service has exceeded all contractual requirements for over a decade. It has extended search capabilities, and methods of limiting abuse.

The WHOIS service operated by Afiliias meets and exceeds ICANN's requirements. Specifically, Afiliias will:

- Offer a WHOIS service made available on port 43 that is flexible and standards- compliant;
- Comply with all ICANN policies, and meeting or exceeding WHOIS performance requirements in Specification 10 of the new gTLD Registry Agreement;
- Enable a Searchable WHOIS with extensive search capabilities that offers ease of use while enforcing measures to mitigate access abuse, and;
- Employ a team with significant experience managing a compliant WHOIS service.

Such extensive knowledge and experience managing a WHOIS service enables Afiliias to offer a comprehensive plan for this TLD that meets the needs of constituents of the domain name industry and Internet users. The service has been tested by our QA team for RFC compliance, and has been used by registrars and many other parties for an extended period of time. Afiliias' WHOIS service currently serves almost 500 million WHOIS queries per month, with the capacity already built in to handle an order of magnitude increase in WHOIS queries, and the ability to smoothly scale should greater growth be needed.

WHOIS system description and diagram

The Afiliias WHOIS system, depicted in figure 26-a, is designed with robustness, availability, compliance, and performance in mind. Additionally, the system has provisions for detecting abusive usage (e.g., excessive numbers of queries from one source). The WHOIS system is generally intended as a publicly available single object lookup system. Afiliias uses an advanced, persistent caching system to ensure extremely fast query response times.

Afiliias will develop restricted WHOIS functions based on specific domain policy and regulatory requirements as needed for operating the business (as long as they are standards compliant). It will also be possible for contact and registrant information to be returned according to regulatory requirements. The WHOIS database supports multiple string and field searching through a reliable, free, secure web-based interface.

#### Data objects, interfaces, access and lookups

Registrars can provide an input form on their public websites through which a visitor is able to perform WHOIS queries. The registry operator can also provide a Web-based search on its site. The input form must accept the string to query, along with the necessary input elements to select the object type and interpretation controls. This input form sends its data to the Afiliias port 43 WHOIS server. The results from the WHOIS query are returned by the server and displayed in the visitor's Web browser. The sole purpose of the Web interface is to provide a user-friendly interface for WHOIS queries.

Afiliias 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 Afiliias' 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.

Afiliias will also provide sophisticated WHOIS search functionality that includes the ability to conduct multiple string and field searches.

#### Query controls

For all WHOIS queries, a user is required to enter the character string representing the information for which they want to search. The object type and interpretation control parameters to limit the search may also be specified. If object type or interpretation control parameter is not specified, WHOIS will search for the character string in the Name field of the Domain object.

WHOIS queries are required to be either an "exact search" or a "partial search," both of which are insensitive to the case of the input string.

An exact search specifies the full string to search for in the database field. An exact match between the input string and the field value is required.

A partial search specifies the start of the string to search for in the database field. Every record with a search field that starts with the input string is considered a match. By default, if multiple matches are found for a query, then a summary containing up to 50 matching results is presented. A second query is required to retrieve the specific details of one of the matching records.

If only a single match is found, then full details will be provided. Full detail consists of the data in the matching object as well as the data in any associated objects. For example: a query that results in a domain object includes the data from the associated host and contact objects.

WHOIS query controls fall into two categories: those that specify the type of field, and those that modify the interpretation of the input or determine the level of output to provide. Each is described below.

The following keywords restrict a search to a specific object type:

- Domain: Searches only domain objects. The input string is searched in the Name field.
- Host: Searches only nameserver objects. The input string is searched in the Name field and the IP Address field.
- Contact: Searches only contact objects. The input string is searched in the ID field.
- Registrar: Searches only registrar objects. The input string is searched in the Name field.

By default, if no object type control is specified, then the Name field of the Domain object is searched.

In addition, Afiliias WHOIS systems can perform and respond to WHOIS searches by registrant name, postal address and contact names. Deployment of these features is provided as an option to the registry operator, based upon registry policy and business decision making.

Figure 26-b presents the keywords that modify the interpretation of the input or determine the level of output to provide.

By default, if no interpretation control keywords are used, the output will include full details if a single match is found and a summary if multiple matches are found.

#### Unique TLD requirements

There are no unique WHOIS requirements for this TLD.

#### Sunrise WHOIS processes

All ICANN TLDs must offer a Sunrise as part of a rights protection program. Afiliias uses EPP extensions that allow registrars to submit trademark and other intellectual property rights (IPR) data to the registry. The following corresponding data will be displayed in WHOIS for relevant domains:

- Trademark Name: element that indicates the name of the Registered Mark.
- Trademark Number: element that indicates the registration number of the IPR.
- Trademark Locality: element that indicates the origin for which the IPR is established (a national or international trademark registry).
- Trademark Entitlement: element that indicates whether the applicant holds the trademark as the original "OWNER", "CO-OWNER" or "ASSIGNEE".
  - Trademark Application Date: element that indicates the date the Registered Mark was applied for.
  - Trademark Registration Date: element that indicates the date the Registered Mark was issued and registered.
  - Trademark Class: element that indicates the class of the Registered Mark.
  - IPR Type: element that indicates the Sunrise phase the application applies for.

#### IT and infrastructure resources

All the applications and databases for this TLD will run in a virtual environment hosted by a cluster of servers equipped with the latest Intel Westmere multi-core processors (or a more advanced, stable technology available at the time of deployment). The registry data will be stored on storage arrays of solid-state drives shared over a fast storage area network. The virtual environment allows the infrastructure to easily scale both vertically and horizontally to cater to changing demand. It also facilitates effective utilization of system resources thus reducing energy consumption and carbon footprint.

The applications and servers are supported by network firewalls, routers and switches.

The WHOIS system accommodates both IPv4 and IPv6 addresses.

Each of the servers and network devices are equipped with redundant hot-swappable components and multiple connections to ancillary systems. Additionally, 24x7 support agreements with our hardware vendor with a 4-hour response time at all our data centers guarantees replacement of failed parts in the shortest time possible.

Models of system and network devices used are:

- Servers: Cisco UCS B230 blade servers
- SAN storage arrays: IBM Storwize V7000 with Solid State Drives
- Firewalls: Cisco ASA 5585-X
- Load balancers: F5 Big-IP 6900
- Traffic shapers: Procera PacketLogic PL8720
- Routers: Juniper MX40 3D
- Network switches: Cisco Nexus 7010, Nexus 5548, Nexus 2232

There will be at least four virtual machines (VMs) offering WHOIS service. Each VM will run at least two WHOIS server instances - one for registrars and one for the public. All instances of the WHOIS service is made available to registrars and the public are rate limited to mitigate abusive behavior.

#### Frequency of synchronization between servers

Registration data records from the EPP publisher database will be replicated to the WHOIS system database on a near-real-time basis whenever an update occurs.

#### Specifications 4 and 10 compliance

The WHOIS service for this TLD will meet or exceed the performance requirements in the new gTLD Registry Agreement, Specification 10. Figure 26-c provides the exact measurements and commitments. Afilias has a 10 year track record of exceeding WHOIS performance and a skilled team to ensure this continues for all TLDs under management.

The WHOIS service for this TLD will meet or exceed the requirements in the new gTLD Registry Agreement, Specification 4.

#### RFC 3912 compliance

Afilias will operate the WHOIS infrastructure in compliance with RFCs and global best practices, as it does with the 16 TLDs Afilias currently supports.

Afilias maintains a registry-level centralized WHOIS database that contains information for every registered domain and for all host and contact objects.

The WHOIS service will be available on the Internet standard WHOIS port (port 43) in compliance with RFC 3912. The WHOIS service contains data submitted by registrars during the registration process. Changes made to the data by a registrant are submitted to Afiliias 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 Afiliias 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

Afiliias 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, Afiliias WHOIS systems can perform and respond to WHOIS searches by registrant name, postal address and contact names.

Providing the ability to search important and high-value fields such as registrant name, address and contact names increases the probability of abusive behavior. An abusive user could script a set of queries to the WHOIS service and access contact data in order to create or sell a list of names and addresses of registrants in this TLD. Making the WHOIS machine readable, while preventing harvesting and mining of WHOIS data, is a key requirement integrated into the Afiliias WHOIS systems. For instance, Afiliias limits search returns to 50 records at a time. If bulk queries were ever necessary (e.g., to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process), Afiliias makes such query responses available to carefully screened and limited staff members at the registry operator (and customer support staff) via an internal data warehouse. The Afiliias WHOIS system accommodates anonymous access as well as pre-identified and profile-defined uses, with full audit and log capabilities.

The WHOIS service has the ability to tag query responses with labels such as "Do not redistribute" or "Special access granted". This may allow for tiered response and reply scenarios. Further, the WHOIS service is configurable in parameters and fields returned, which allow for flexibility in compliance with various jurisdictions, regulations or laws.

Afiliias offers exact-match capabilities on the following fields: registrar ID, nameserver name, and nameserver's IP address (only applies to IP addresses stored by the registry, i.e., glue records). Search capabilities are fully available, and results include domain names matching the search criteria (including IDN variants). Afiliias manages abuse prevention through rate limiting and CAPTCHA (described below). Queries do not require specialized transformations of internationalized domain names or internationalized data fields

Please see "Query Controls" above for details about search options and capabilities.



## Deterring WHOIS abuse

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 this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Within Afilias, there are 11 staff members who develop and maintain the compliant WHOIS systems. They keep pace with access requirements, thwart abuse, and continually develop software. Of these resources, approximately two staffers are typically required for WHOIS-related code customization.

Other resources provide quality assurance, and operations personnel maintain the WHOIS system itself. This team will be responsible for the implementation and on-going maintenance of the new TLD WHOIS service.

---

**27. Registration Life Cycle: provide a detailed description of the proposed registration lifecycle for domain names in the proposed gTLD. The description must explain the various registration states as well as the criteria and procedures that are used to change state. It must describe the typical registration lifecycle of create/update/delete and all intervening steps such as pending, locked, expired, and transferred that may apply. Any time elements that are involved - for instance details of add-grace or redemption grace periods, or notice periods for renewals or transfers - must also be clearly explained. Describe resourcing plans (number and description of personnel roles allocated to this area).**

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS, WHICH ICANN INFORMS US (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE, ACCORDING TO SPECIFIC GUIDANCE FROM ICANN UNDER CASE ID 11027.

---

**28. Abuse Prevention and Mitigation: Applicants should describe the proposed policies and procedures to minimize abusive registrations and other activities that have a negative impact on Internet users. Answers should include:**

- **safeguards the applicant will implement at the time of registration, policies to reduce opportunities for abusive behaviors using registered domain names in the TLD, and policies for handling complaints regarding abuse. Each registry operator will be required to establish and publish on its website a single abuse point of contact responsible for addressing matters requiring expedited attention and providing a timely response to abuse complaints concerning all names registered in the TLD through all registrars of record, including those involving a reseller.**
- **a description of rapid takedown or suspension systems that will be implemented.**
- **proposed measures for management and removal of orphan glue records for names removed from the zone.**
- **resourcing plans (number and description of personnel roles allocated to this area).**

28 Abuse Prevention and Mitigation

Nameshop, working with Afiliias, will take the requisite operational and technical steps to promote WHOIS data accuracy, limit domain abuse, remove outdated and inaccurate data, and other security measures to ensure the

integrity of the TLD. The specific measures include, but are not limited to:

- Posting a TLD Anti-Abuse Policy that clearly defines abuse, and provide point-of-contact information for reporting suspected abuse;
- Committing to rapid identification and resolution of abuse, including suspensions;
- Ensuring completeness of WHOIS information at the time of registration;
- Publishing and maintaining procedures for removing orphan glue records for names removed from the zone, and;
- Establishing measures to deter WHOIS abuse, including rate-limiting, determining data syntax validity, and implementing and enforcing requirements from the Registry-Registrar Agreement.

#### Abuse policy

The Anti-Abuse Policy stated below will be enacted under the contractual authority of the registry operator through the Registry-Registrar Agreement, and the obligations will be passed on to and made binding upon registrants. This policy will be posted on the TLD web site along with contact information for registrants or users to report suspected abuse.

The policy is designed to address the malicious use of domain names. The registry operator and its registrars will make reasonable attempts to limit significant harm to Internet users. This policy is not intended to take the place of the Uniform Domain Name Dispute Resolution Policy (UDRP) or the Uniform Rapid Suspension System (URS), and it is not to be used as an alternate form of dispute resolution or as a brand protection mechanism. Its intent is not to burden law-abiding or innocent registrants and domain users; rather, the intent is to deter those who use domain names maliciously by engaging in illegal or fraudulent activity.

Repeat violations of the abuse policy will result in a case-by-case review of the abuser(s), and the registry operator reserves the right to escalate the issue, with the intent of levying sanctions that are allowed under the TLD anti-abuse policy.

The below policy is a recent version of the policy that has been used by the .INFO registry since 2008, and the .ORG registry since 2009. It has proven to be an effective and flexible tool.

#### Nameshop Anti-Abuse Policy

The following Anti-Abuse Policy is effective upon launch of the TLD. Malicious use of domain names will not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars, and registrants, as well as for users of the Internet in general. The registry operator definition of abusive use of a domain includes, without limitation, the following:

- Illegal or fraudulent actions;
- Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of web sites and Internet forums;
- Phishing: The use of counterfeit web pages that are designed to trick recipients into divulging sensitive data such as personally identifying information, usernames, passwords, or financial data;
- Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or poisoning;
- Willful distribution of malware: The dissemination of software designed to

infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and Trojan horses.

- Malicious fast-flux hosting: Use of fast-flux techniques with a botnet to disguise the location of web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities.
- Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct distributed denial-of-service attacks (DDoS attacks);
- Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Pursuant to the Registry-Registrar Agreement, registry operator reserves the right at its sole discretion to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary: (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of registry operator, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement and this Anti-Abuse Policy, or (5) to correct mistakes made by registry operator or any registrar in connection with a domain name registration. Registry operator also reserves the right to place upon registry lock, hold, or similar status a domain name during resolution of a dispute.

The policy stated above will be accompanied by notes about how to submit a report to the registry operator's abuse point of contact, and how to report an orphan glue record suspected of being used in connection with malicious conduct (see below).

#### Abuse point of contact and procedures for handling abuse complaints

The registry operator will establish an abuse point of contact. This contact will be a role-based e-mail address of the form "abuse@regisry.nameshop" or any email address in conformity with ICANN's anti-abuse policy. 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. Afiliias will integrate its existing ticketing system with the registry operator's to ensure uniform tracking and handling of the complaint. This role-based approach has been used successfully by ISPs, e-mail service providers, and registrars for many years, and is considered a global best practice.

The registry operator's designated abuse handlers will then evaluate complaints received via the abuse system address. They will decide whether a particular issue is of concern, and decide what action, if any, is appropriate.

In general, the registry operator will find itself receiving abuse reports from a wide variety of parties, including security researchers and Internet

security companies, financial institutions such as banks, Internet users, and law enforcement agencies among others. Some of these parties may provide good forensic data or supporting evidence of the malicious behavior. In other cases, the party reporting an issue may not be familiar with how to provide such data or proof of malicious behavior. It is expected that a percentage of abuse reports to the registry operator will not be actionable, because there will not be enough evidence to support the complaint (even after investigation), and because some reports or reporters will simply not be credible.

The security function includes a communication and outreach function, with information sharing with industry partners regarding malicious or abusive behavior, in order to ensure coordinated abuse mitigation across multiple TLDs.

Assessing abuse reports requires great care, and the registry operator will rely upon professional, trained investigators who are versed in such matters. The goals are accuracy, good record-keeping, and a zero false-positive rate so as not to harm innocent registrants.

Different types of malicious activities require different methods of investigation and documentation. Further, the registry operator expects to face unexpected or complex situations that call for professional advice, and will rely upon professional, trained investigators as needed.

In general, there are two types of domain abuse that must be addressed:

a) Compromised domains. These domains have been hacked or otherwise compromised by criminals, and the registrant is not responsible for the malicious activity taking place on the domain. For example, the majority of domain names that host phishing sites are compromised. The goal in such cases is to get word to the registrant (usually via the registrar) that there is a problem that needs attention with the expectation that the registrant will address the problem in a timely manner. Ideally such domains do not get suspended, since suspension would disrupt legitimate activity on the domain.

b) Malicious registrations. These domains are registered by malefactors for the purpose of abuse. Such domains are generally targets for suspension, since they have no legitimate use.

The standard procedure is that the registry operator will forward a credible alleged case of malicious domain name use to the domain's sponsoring registrar with a request that the registrar investigate the case and act appropriately. The registrar will be provided evidence collected as a result of the investigation conducted by the trained abuse handlers. As part of the investigation, if inaccurate or false WHOIS registrant information is detected, the registrar is notified about this. The registrar is the party with a direct relationship with—and a direct contract with—the registrant. The registrar will also have vital information that the registry operator will not, such as:

- Details about the domain purchase, such as the payment method used (credit card, PayPal, etc.);
- The identity of a proxy-protected registrant;
- The purchaser's IP address;
- Whether there is a reseller involved, and;
- The registrant's past sales history and purchases in other TLDs (insofar as the registrar can determine this).

Registrars do not share the above information with registry operators due to

privacy and liability concerns, among others. Because they have more information with which to continue the investigation, and because they have a direct relationship with the registrant, the registrar is in the best position to evaluate alleged abuse. The registrar can determine if the use violates the registrar's legal terms of service or the registry Anti-Abuse Policy, and can decide whether or not to take any action. While the language and terms vary, registrars will be expected to include language in their registrar-registrant contracts that indemnifies the registrar if it takes action, and allows the registrar to suspend or cancel a domain name; this will be in addition to the registry Anti-Abuse Policy. Generally, registrars can act if the registrant violates the registrar's terms of service, or violates ICANN policy, or if illegal activity is involved, or if the use violates the registry's Anti-Abuse Policy.

If a registrar does not take action within a time period indicated by the registry operator (usually 24 hours), the registry operator might then decide to take action itself. At all times, the registry operator reserves the right to act directly and immediately if the potential harm to Internet users seems significant or imminent, with or without notice to the sponsoring registrar.

The registry operator will be prepared to call upon relevant law enforcement bodies as needed. There are certain cases, for example, Illegal pharmacy domains, where the registry operator will contact the Law Enforcement Agencies to share information about these domains, provide all the evidence collected and work closely with them before any action will be taken for suspension. The specific action is often dependent upon the jurisdiction of which the registry operator, although the operator in all cases will adhere to applicable laws and regulations.

When valid court orders or seizure warrants are received from courts or law enforcement agencies of relevant jurisdiction, the registry operator will order execution in an expedited fashion. Compliance with these will be a top priority and will be completed as soon as possible and within the defined timelines of the order. There are certain cases where Law Enforcement Agencies request information about a domain including but not limited to:

- Registration information
- History of a domain, including recent updates made
- Other domains associated with a registrant's account
- Patterns of registrant portfolio

Requests for such information is handled on a priority basis and sent back to the requestor as soon as possible. Afilias sets a goal to respond to such requests within 24 hours.

The registry operator may also engage in proactive screening of its zone for malicious use of the domains in the TLD, and report problems to the sponsoring registrars. The registry operator could take advantage of a combination of the following resources, among others:

- Blocklists of domain names and nameservers published by organizations such as SURBL and Spamhaus.
- Anti-phishing feeds, which will provide URLs of compromised and maliciously registered domains being used for phishing.
- Analysis of registration or DNS query data [DNS query data received by the TLD nameservers.]

The registry operator will keep records and track metrics regarding abuse and abuse reports. These will include:

- Number of abuse reports received by the registry's abuse point of contact described above;
- Number of cases and domains referred to registrars for resolution;
- Number of cases and domains where the registry took direct action;
- Resolution times;
- Number of domains in the TLD that have been blacklisted by major anti-spam blacklist providers, and;
- Phishing site uptimes in the TLD.

#### Removal of orphan glue records

By definition, orphan glue records used to be glue records. Glue records are related to delegations and are necessary to guide iterative resolvers to delegated nameservers. A glue record becomes an orphan when its parent nameserver record is removed without also removing the corresponding glue record. (Please reference the ICANN SSAC paper SAC048 at: <http://www.icann.org/en/committees/security/sac048.pdf>.) Orphan glue records may be created when a domain (example.tld) is placed on EPP ServerHold or ClientHold status. When placed on Hold, the domain is removed from the zone and will stop resolving. However, any child nameservers (now orphan glue) of that domain (e.g., nsl.example.tld) are left in the zone. It is important to keep these orphan glue records in the zone so that any innocent sites using that nameserver will continue to resolve. This use of Hold status is an essential tool for suspending malicious domains.

Afilias observes the following procedures, which are being followed by other registries and are generally accepted as DNS best practices. These procedures are also in keeping with ICANN SSAC recommendations.

When a request to delete a domain is received from a registrar, the registry first checks for the existence of glue records. If glue records exist, the registry will check to see if other domains in the registry are using the glue records. If other domains in the registry are using the glue records then the request to delete the domain will fail until no other domains are using the glue records. If no other domains in the registry are using the glue records then the glue records will be removed before the request to delete the domain is satisfied. If no glue records exist then the request to delete the domain will be satisfied.

If a registrar cannot delete a domain because of the existence of glue records that are being used by other domains, then the registrar may refer to the zone file or the "weekly domain hosted by nameserver report" to find out which domains are using the nameserver in question and attempt to contact the corresponding registrar to request that they stop using the nameserver in the glue record. The registry operator does not plan on performing mass updates of the associated DNS records.

The registry operator will accept, evaluate, and respond appropriately to complaints that orphan glue is being used maliciously. Such reports should be made in writing to the registry operator, and may be submitted to the registry's abuse point-of-contact. If it is confirmed that an orphan glue record is being used in connection with malicious conduct, the registry operator will have the orphan glue record removed from the zone file. Afilias has the technical ability to execute such requests as needed.

#### Methods to promote WHOIS accuracy

The creation and maintenance of accurate WHOIS records is an important part of registry management. As described in our response to question #26, WHOIS,

the registry operator will manage a secure, robust and searchable WHOIS service for this TLD.

#### WHOIS data accuracy

The registry operator will offer a "thick" registry system. In this model, all key contact details for each domain name will be stored in a central location by the registry. This allows better access to domain data, and provides uniformity in storing the information. The registry operator will ensure that the required fields for WHOIS data (as per the defined policies for the TLD) are enforced at the registry level. This ensures that the registrars are providing required domain registration data. Fields defined by the registry policy to be mandatory are documented as such and must be submitted by registrars. The Afiliias registry system verifies formats for relevant individual data fields (e.g. e-mail, and phone/fax numbers). Only valid country codes are allowed as defined by the ISO 3166 code list. The Afiliias WHOIS system is extensible, and is capable of using the VAULT system, described further below.

Similar to the centralized abuse point of contact described above, the registry operator can institute a contact email address which could be utilized by third parties to submit complaints for inaccurate or false WHOIS data detected. This information will be processed by Afiliias' support department and forwarded to the registrars. The registrars can work with the registrants of those domains to address these complaints. Afiliias will audit registrars on a yearly basis to verify whether the complaints being forwarded are being addressed or not. This functionality, available to all registry operators, is activated based on the registry operator's business policy.

Afiliias also incorporates a spot-check verification system where a randomly selected set of domain names are checked periodically for accuracy of WHOIS data. Afiliias' .PRO registry system incorporates such a verification system whereby 1% of total registrations or 100 domains, whichever number is larger, are spot-checked every month to verify the domain name registrant's critical information provided with the domain registration data. With both a highly qualified corps of engineers and a 24x7 staffed support function, Afiliias has the capacity to integrate such spot-check functionality into this TLD, based on the registry operator's business policy. Note: This functionality will not work for proxy protected WHOIS information, where registrars or their resellers have the actual registrant data. The solution to that problem lies with either registry or registrar policy, or a change in the general marketplace practices with respect to proxy registrations.

Finally, Afiliias' registry systems have a sophisticated set of billing and pricing functionality which aids registry operators who decide to provide a set of financial incentives to registrars for maintaining or improving WHOIS accuracy. For instance, it is conceivable that the registry operator may decide to provide a discount for the domain registration or renewal fees for validated registrants, or levy a larger cost for the domain registration or renewal of proxy domain names. The Afiliias system has the capability to support such incentives on a configurable basis, towards the goal of promoting better WHOIS accuracy.

#### Role of registrars

As part of the RRA (Registry Registrar Agreement), the registry operator will require the registrar to be responsible for ensuring the input of accurate WHOIS data by their registrants. The Registrar/Registered Name Holder Agreement will include a specific clause to ensure accuracy of WHOIS data,



and to give the registrar rights to cancel or suspend registrations if the Registered Name Holder fails to respond to the registrar's query regarding accuracy of data. ICANN's WHOIS Data Problem Reporting System (WDPRS) will be available to those who wish to file WHOIS inaccuracy reports, as per ICANN policy (<http://wdprs.internic.net/>).

#### Controls to ensure proper access to domain functions

Several measures are in place in the 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.

#### Validation and abuse mitigation mechanisms

Afilias has developed advanced validation and abuse mitigation mechanisms. These capabilities and mechanisms are described below. These services and capabilities are discretionary and may be utilized by the registry operator based on their policy and business need.

Afilias has the ability to analyze the registration data for known patterns at the time of registration. A database of these known patterns is developed from domains and other associated objects (e.g., contact information) which have been previously detected and suspended after being flagged as abusive. Any domains matching the defined criteria can be flagged for investigation. Once analyzed and confirmed by the domain anti-abuse team members, these domains may be suspended. This provides proactive detection of abusive domains.

Provisions are available to enable the registry operator to only allow registrations by pre-authorized and verified contacts. These verified contacts are given a unique code that can be used for registration of new domains.

#### Registrant pre-verification and authentication

One of the systems that could be used for validity and identity authentication is VAULT (Validation and Authentication Universal Lookup). It utilizes information obtained from a series of trusted data sources with access to billions of records containing data about individuals for the purpose of providing independent age and id verification as well as the

ability to incorporate additional public or private data sources as required. At present it has the following: US Residential Coverage - 90% of Adult Population and also International Coverage - Varies from Country to Country with a minimum of 80% coverage (24 countries, mostly European).

Various verification elements can be used. Examples might include applicant data such as name, address, phone, etc. Multiple methods could be used for verification include integrated solutions utilizing API (XML Application Programming Interface) or sending batches of requests.

- Verification and Authentication requirements would be based on TLD operator requirements or specific criteria.
- Based on required WHOIS Data; registrant contact details (name, address, phone)
  - If address/ZIP can be validated by VAULT, the validation process can continue (North America +25 International countries)
  - If in-line processing and registration and EPP/API call would go to the verification clearinghouse and return up to 4 challenge questions.
  - If two-step registration is required, then registrants would get a link to complete the verification at a separate time. The link could be specific to a domain registration and pre-populated with data about the registrant.
  - If WHOIS data is validated a token would be generated and could be given back to the registrar which registered the domain.
  - WHOIS data would reflect the Validated Data or some subset, i.e., fields displayed could be first initial and last name, country of registrant and date validated. Other fields could be generic validation fields much like a "privacy service".
  - A "Validation Icon" customized script would be sent to the registrants email address. This could be displayed on the website and would be dynamically generated to avoid unauthorized use of the Icon. When clicked on the Icon would should limited WHOIS details i.e. Registrant: jdoe, Country: USA, Date Validated: March 29, 2011, as well as legal disclaimers.
  - Validation would be annually renewed, and validation date displayed in the WHOIS.

#### Abuse prevention resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way. Abuse prevention and detection is a function that is staffed across the various groups inside Afilias, and requires a team effort when abuse is either well hidden or widespread, or both. While all of Afilias' 200+ employees are charged with responsibility to report any detected abuse, the engineering and analysis teams, numbering over 30, provide specific support based on the type of abuse and volume and frequency of analysis required. The Afilias security and support teams have the authority to initiate mitigation.

Afilias has developed advanced validation and abuse mitigation mechanisms. These capabilities and mechanisms are described below. These services and capabilities are discretionary and may be utilized by the registry operator

based on their policy and business need.

This TLD's anticipated volume of registrations in the first three years of operations is listed in response #46. Afiliias and the registry operator's anti-abuse function anticipates the expected volume and type of registrations, and together will adequately cover the staffing needs for this TLD. The registry operator will maintain an abuse response team, which may be a combination of internal staff and outside specialty contractors, adjusting to the needs of the size and type of TLD. The team structure planned for this TLD is based on several years of experience responding to, mitigating, and managing abuse for TLDs of various sizes. The team will generally consist of abuse handlers (probably internal), a junior analyst, (either internal or external), and a senior security consultant (likely an external resource providing the registry operator with extra expertise as needed). These responders will be specially trained in the investigation of abuse complaints, and will have the latitude to act expeditiously to suspend domain names (or apply other remedies) when called for.

The exact resources required to maintain an abuse response team must change with the size and registration procedures of the TLD. An initial abuse handler is necessary as a point of contact for reports, even if a part-time responsibility. The abuse handlers monitor the abuse email address for complaints and evaluate incoming reports from a variety of sources. A large percentage of abuse reports to the registry operator may be unsolicited commercial email. The designated abuse handlers can identify legitimate reports and then decide what action is appropriate, either to act upon them, escalate to a security analyst for closer investigation, or refer them to registrars as per the above-described procedures. A TLD with rare cases of abuse would conform to this structure.

If multiple cases of abuse within the same week occur regularly, the registry operator will consider staffing internally a security analyst to investigate the complaints as they become more frequent. Training an abuse analyst requires 3-6 months and likely requires the active guidance of an experienced senior security analyst for guidance and verification of assessments and recommendations being made.

If this TLD were to regularly experience multiple cases of abuse within the same day, a full-time senior security analyst would likely be necessary. A senior security analyst capable of fulfilling this role should have several years of experience and able to manage and train the internal abuse response team.

The abuse response team will also maintain subscriptions for several security information services, including the blocklists from organizations like SURBL and Spamhaus and anti-phishing and other domain related abuse (malware, fast-flux etc.) feeds. The pricing structure of these services may depend on the size of the domain and some services will include a number of rapid suspension requests for use as needed.

For a large TLD, regular audits of the registry data are required to maintain control over abusive registrations. When a registrar with a significant number of registrations has been compromised or acted maliciously, the registry operator may need to analyze a set of registration or DNS query data. A scan of all the domains of a registrar is conducted only as needed. Scanning and analysis for a large registrar may require as much as a week of full-time effort for a dedicated machine and team.

---

**29. Rights Protection Mechanisms: Applicants should describe how their proposal will comply with policies and practices that minimize abusive registrations and other activities that affect the legal rights of others. Describe how the registry operator will implement safeguards against allowing unqualified registrations, and reduce opportunities for behaviors such as phishing or pharming. At a minimum, the registry operator must offer either a Sunrise period or a Trademark Claims service, and implement decisions rendered under the URS. Answers may also include additional measures such as abusive use policies, takedown procedures, registrant pre-verification, or authentication procedures, or other covenants. Describe resourcing plans (number and description of personnel roles allocated to this area).**

29 Rights Protection Mechanisms

Rights protection is a core responsibility of the TLD operator, and is supported by a fully-developed plan for rights protection that includes:

- Establishing mechanisms to prevent unqualified registrations (e.g., registrations made in violation of the registry's eligibility restrictions or policies);
- Implementing a robust Sunrise program, utilizing the Trademark Clearinghouse, the services of one of ICANN's approved dispute resolution providers, a trademark validation agent, and drawing upon sunrise policies and rules used successfully in previous gTLD launches;
- Implementing a professional trademark claims program that utilizes the Trademark Clearinghouse, and drawing upon models of similar programs used successfully in previous TLD launches;
- Complying with the URS requirements;
- Complying with the UDRP;
- Complying with the PDDRP, and;
- Including all ICANN-mandated and independently developed rights protection mechanisms ("RPMs") in the registry-registrar agreement entered into by ICANN-accredited registrars authorized to register names in the TLD.

The response below details the rights protection mechanisms at the launch of the TLD (Sunrise and Trademark Claims Service) which comply with rights protection policies (URS, UDRP, PDDRP, and other ICANN RPMs), outlines additional provisions made for rights protection, and provides the resourcing plans.

Safeguards for rights protection at the launch of the TLD

The launch of this TLD will include the operation of a trademark claims service according to the defined ICANN processes for checking a registration request and alerting trademark holders of potential rights infringement.

The Sunrise Period will be an exclusive period of time, prior to the opening of public registration, when trademark and service mark holders will be able to reserve marks that are an identical match in the proposed domain. Following the Sunrise Period, Nameshop will open registration to qualified applicants.

The anticipated Rollout Schedule for the Sunrise Period will be approximately as follows:

Launch of the TLD - Sunrise Period begins for trademark holders and service mark holders to submit registrations for their exact marks in this domain. To maximize fairness registrations will be processed via four queues of a randomized, round robin system, which will close 30 days, 30 days, 30 days and 30 days following the launch date respectively. Following this, Nameshop expects the balance of Sunrise registrations to be awarded in real-time.

Five months after launch -The Sunrise Period will close and will be followed by a Quiet Period for testing and evaluation.

One month after close of Quiet Period - Registration in the TLD domain will be opened to qualified applicants.

Six months after launch - this domain names begin to resolve through standard Web browsers.

#### Sunrise Period Requirements & Restrictions

Those wishing to reserve their marks in this domain during the Sunrise Period must own a current trademark or service mark listed in the Trademark Clearinghouse.

Notice will be provided to all trademark holders in the Clearinghouse if someone is seeking a Sunrise registration. This notice will be provided to holders of marks in the Clearinghouse that are an Identical Match (as defined in the Trademark Clearing House) to the name to be registered during Sunrise.

Each Sunrise registration will require a minimum term of five years.

Nameshop will establish the following Sunrise eligibility requirements (SERs) as minimum requirements, verified by Clearinghouse data, and incorporate a Sunrise Dispute Resolution Policy (SDRP). The SERs include: (i) ownership of a mark that satisfies the criteria set forth in section 7.2 of the Trademark Clearing House specifications, (ii) description of international class of goods or services covered by registration; (iii) representation that all provided information is true and correct; and (iv) provision of data sufficient to document rights in the trademark.

The SDRP will allow challenges based on the following four grounds: (i) at time the challenged domain name was registered, the registrants did not hold a trademark registration of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; (ii) the domain name is not identical to the mark on which the registrant based its Sunrise registration; (iii) the trademark registration on which the registrant based its Sunrise registration is not of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; or (iv) the trademark registration on which the domain name registrant based its Sunrise registration did not issue on or before the effective date of the Registry Agreement and was not applied for on or before ICANN announced the applications received.

#### Ongoing rights protection mechanisms

Several mechanisms will be in place to protect rights in this TLD. As described in our responses to questions #27 and #28, measures are in place to ensure domain transfers and updates are only initiated by the appropriate domain holder, and an experienced team is available to respond to legal actions by law enforcement or court orders.

This TLD will conform to all ICANN RPMs including URS (defined below), UDRP, PDDRP, and all measures defined in Specification 7 of the new TLD agreement.

#### Uniform Rapid Suspension (URS)

The registry operator will implement decisions rendered under the URS on an ongoing basis. Per the URS policy posted on ICANN's Web site as of this writing, the registry operator will receive notice of URS actions from the ICANN-approved URS providers. These emails will be directed immediately to the registry operator's support staff, which is on duty 24x7. The support staff will be responsible for creating a ticket for each case, and for executing the directives from the URS provider. All support staff will receive pertinent training.

As per ICANN's URS guidelines, within 24 hours of receipt of the notice of complaint from the URS provider, the registry operator shall "lock" the domain, meaning the registry shall restrict all changes to the registration data, including transfer and deletion of the domain names, but the name will remain in the TLD DNS zone file and will thus continue to resolve. The support staff will "lock" the domain by associating the following EPP statuses with the domain and relevant contact objects:

- ServerUpdateProhibited, with an EPP reason code of "URS"
- ServerDeleteProhibited, with an EPP reason code of "URS"
- ServerTransferProhibited, with an EPP reason code of "URS"
- The registry operator's support staff will then notify the URS provider immediately upon locking the domain name, via email.

The registry operator's support staff will retain all copies of emails from the URS providers, assign them a tracking or ticket number, and will track the status of each opened URS case through to resolution via spreadsheet or database.

The registry operator's support staff will execute further operations upon notice from the URS providers. The URS provider is required to specify the remedy and required actions of the registry operator, with notification to the registrant, the complainant, and the registrar.

As per the URS guidelines, if the complainant prevails, the "registry operator shall suspend the domain name, which shall remain suspended for the balance of the registration period and would not resolve to the original web site. The nameservers shall be redirected to an informational web page provided by the URS provider about the URS. The WHOIS for the domain name shall continue to display all of the information of the original registrant except for the redirection of the nameservers. In addition, the WHOIS shall reflect that the domain name will not be able to be transferred, deleted or modified for the life of the registration."

#### Rights protection via the RRA

The following will be memorialized and be made binding via the Registry-Registrar and Registrar-Registrant Agreements:

- The registry may reject a registration request or a reservation request, or may delete, revoke, suspend, cancel, or transfer a registration or reservation under the following criteria:
  - a. to enforce registry policies and ICANN requirements; each as amended from time to time;
  - b. that is not accompanied by complete and accurate information as required by ICANN requirements and/or registry policies or where required information

is not updated and/or corrected as required by ICANN requirements and/or registry policies;

- c. to protect the integrity and stability of the registry, its operations, and the TLD system;
- d. to comply with any applicable law, regulation, holding, order, or decision issued by a court, administrative authority, or dispute resolution service provider with jurisdiction over the registry;
- e. to establish, assert, or defend the legal rights of the registry or a third party or to avoid any civil or criminal liability on the part of the registry and/or its affiliates, subsidiaries, officers, directors, representatives, employees, contractors, and stockholders;
- f. to correct mistakes made by the registry or any accredited registrar in connection with a registration; or
- g. as otherwise provided in the Registry-Registrar Agreement and/or the Registrar-Registrant Agreement.

Reducing opportunities for behaviors such as phishing or pharming  
In our response to question #28, the registry operator has described its anti-abuse program. Rather than repeating the policies and procedures here, please see our response to question #28 for full details.

With specific respect to phishing and pharming, it should be noted by ICANN that this will be a single entity TLD in which Nameshop has direct control over each registrant (they are typically on staff or otherwise contractually bound) and how each registration may be used. Further, there will be no open registration period for this TLD, as it will never be an "open" TLD. Since all criminal activity (such as phishing and pharming) is precluded by the mission, values and policies of the registry operator (and its parent organization), criminal activity is not expected to be a problem. If such activity occurs due to hacking or other compromises, the registry operator will take prompt and effective steps to eliminate the activity.

In the case of this TLD, Nameshop 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 Nameshop 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.

---

## **Demonstration of Technical & Operational Capability (Internal)**

---

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

- **indication of any independent assessment reports demonstrating security capabilities;**
- **description of any augmented security levels or capabilities commensurate with the nature of the applied for gTLD string;**
- **lists of commitments made to registrants concerning security levels;**

The answer to question #30a is provided by Afilias, the back-end provider of registry services for this 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:

- Afiliias hosts domains in data centers around the world that meet or exceed global best practices.
- Afiliias' DNS infrastructure is massively provisioned as part of its DDoS mitigation strategy, thus ensuring sufficient capacity and redundancy to support new gTLDs.
- Diversity is an integral part of all of our software and hardware stability and robustness plan, thus avoiding any single points of failure in our infrastructure.
- Access to any element of our service (applications, infrastructure and data) is only provided on an as-needed basis to employees and a limited set of others to fulfill their job functions. The principle of least privilege is applied.
- All registry components - critical and non-critical - are monitored 24x7 by staff at our NOCs, and the technical staff has detailed plans and procedures that have stood the test of time for addressing even the smallest anomaly. Well-documented incident management procedures are in place to quickly involve the on-call technical and management staff members to address any issues.

Afiliias follows the guidelines from the ISO 27001 Information Security Standard (Reference:

[http://www.iso.org/iso/catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=42103](http://www.iso.org/iso/catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103) ) for the management and implementation of its Information Security Management System. Afiliias also utilizes the COBIT IT governance framework to facilitate policy development and enable controls for appropriate management of risk (Reference: <http://www.isaca.org/cobit>). Best practices defined in ISO 27002 are followed for defining the security controls within the organization. Afiliias continually looks to improve the efficiency and effectiveness of our processes, and follows industry best practices as defined by the IT Infrastructure Library, or ITIL (Reference: <http://www.itil-officialsite.com/>).

The Afiliias registry system is located within secure data centers that implement a multitude of security measures both to minimize any potential points of vulnerability and to limit any damage should there be a breach. The characteristics of these data centers are described fully in our response to question #30(b).

The Afiliias registry system employs a number of multi-layered measures to prevent unauthorized access to its network and internal systems. Before reaching the registry network, all traffic is required to pass through a firewall system. Packets passing to and from the Internet are inspected, and unauthorized or unexpected attempts to connect to the registry servers are both logged and denied. Management processes are in place to ensure each request is tracked and documented, and regular firewall audits are performed to ensure proper operation. 24x7 monitoring is in place and, if potential malicious activity is detected, appropriate personnel are notified immediately.

Afiliias employs a set of security procedures to ensure maximum security on

each of its servers, including disabling all unnecessary services and processes and regular application of security-related patches to the operating system and critical system applications. Regular external vulnerability scans are performed to verify that only services intended to be available are accessible.

Regular detailed audits of the server configuration are performed to verify that the configurations comply with current best security practices. Passwords and other access means are changed on a regular schedule and are revoked whenever a staff member's employment is terminated.

#### Access to registry system

Access to all production systems and software is strictly limited to authorized operations staff members. Access to technical support and network operations teams where necessary are read only and limited only to components required to help troubleshoot customer issues and perform routine checks. Strict change control procedures are in place and are followed each time a change is required to the production hardware/application. User rights are kept to a minimum at all times. In the event of a staff member's employment termination, all access is removed immediately.

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 Afiliias, 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, Afiliias 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.

Afiliias 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 Afiliias' domain registry system and processes. The report includes testing of key controls related to the following control objectives:

- Controls provide reasonable assurance that registrar account balances and changes to the registrar account balances are authorized, complete, accurate and timely.
- Controls provide reasonable assurance that billable transactions are recorded in the Shared Registry System (SRS) in a complete, accurate and timely manner.
- Controls provide reasonable assurance that revenue is systemically calculated by the Deferred Revenue System (DRS) in a complete, accurate and timely manner.
- Controls provide reasonable assurance that the summary and detail reports, invoices, statements, registrar and registry billing data files, and ICANN transactional reports provided to registry operator(s) are complete, accurate and timely.
- Controls provide reasonable assurance that new applications and changes to existing applications are authorized, tested, approved, properly implemented and documented.
- Controls provide reasonable assurance that changes to existing system software and implementation of new system software are authorized, tested, approved, properly implemented and documented.
- Controls provide reasonable assurance that physical access to data centers is restricted to properly authorized individuals.
- Controls provide reasonable assurance that logical access to system resources is restricted to properly authorized individuals.
- Controls provide reasonable assurance that processing and backups are appropriately authorized and scheduled and that deviations from scheduled processing and backups are identified and resolved.

The last Type 2 report issued was for the year 2010, and it was unqualified, i.e., all systems were evaluated with no material problems found.

During each year, Afilias monitors the key controls related to the SSAE controls. Changes or additions to the control objectives or activities can result due to deployment of new services, software enhancements, infrastructure changes or process enhancements. These are noted and after internal review and approval, adjustments are made for the next review.

In addition to the PricewaterhouseCoopers engagement, Afilias performs internal security audits twice a year. These assessments are constantly being expanded based on risk assessments and changes in business or technology.

Additionally, Afilias engages an independent third-party security organization, PivotPoint Security, to perform external vulnerability assessments and penetration tests on the sites hosting and managing the Registry infrastructure. These assessments are performed with major infrastructure changes, release of new services or major software enhancements. These independent assessments are performed at least annually. A report from a recent assessment is attached with our response to question #30(b).

Afilias has engaged with security companies specializing in application and web security testing to ensure the security of web-based applications offered by Afilias, such as the Web Admin Tool (WAT) for registrars and registry operators.

Finally, Afilias has engaged IBM's Security services division to perform ISO 27002 gap assessment studies so as to review alignment of Afilias' procedures and policies with the ISO 27002 standard. Afilias has since made adjustments to its security procedures and policies based on the recommendations by IBM.

#### Special TLD considerations

Afilias' rigorous security practices are regularly reviewed; if there is a need to alter or augment procedures for this TLD, they will be done so in a planned and deliberate manner.

#### Commitments to registrant protection

With over a decade of experience protecting domain registration data, Afilias understands registrant security concerns. Afilias supports a "thick" registry system in which data for all objects are stored in the registry database that is the centralized authoritative source of information. As an active member of IETF (Internet Engineering Task Force), ICANN's SSAC (Security & Stability Advisory Committee), APWG (Anti-Phishing Working Group), MAAWG (Messaging Anti-Abuse Working Group), USENIX, and ISACA (Information Systems Audits and Controls Association), the Afilias team is highly attuned to the potential threats and leading tools and procedures for mitigating threats. As such, registrants should be confident that:

- Any confidential information stored within the registry will remain confidential;
- The interaction between their registrar and Afilias is secure;
- The Afilias DNS system will be reliable and accessible from any location;
- The registry system will abide by all polices, including those that address registrant data;
- Afilias will not introduce any features or implement technologies that compromise access to the registry system or that compromise registrant security.

Afilias has directly contributed to the development of the documents listed below and we have implemented them where appropriate. All of these have

helped improve registrants' ability to protect their domains name(s) during the domain name lifecycle.

- [SAC049]: SSAC Report on DNS Zone Risk Assessment and Management (03 June 2011)
- [SAC044]: A Registrant's Guide to Protecting Domain Name Registration Accounts (05 November 2010)
- [SAC040]: Measures to Protect Domain Registration Services Against Exploitation or Misuse (19 August 2009)
- [SAC028]: SSAC Advisory on Registrar Impersonation Phishing Attacks (26 May 2008)
- [SAC024]: Report on Domain Name Front Running (February 2008)
- [SAC022]: Domain Name Front Running (SAC022, SAC024) (20 October 2007)
- [SAC011]: Problems caused by the non-renewal of a domain name associated with a DNS Name Server (7 July 2006)
- [SAC010]: Renewal Considerations for Domain Name Registrants (29 June 2006)
- [SAC007]: Domain Name Hijacking Report (SAC007) (12 July 2005)

To protect any unauthorized modification of registrant data, Afilias mandates TLS/SSL transport (per RFC 5246) and authentication methodologies for access to the registry applications. Authorized registrars are required to supply a list of specific individuals (five to ten people) who are authorized to contact the registry. Each such individual is assigned a pass phrase. Any support requests made by an authorized registrar to registry customer service are authenticated by registry customer service. All failed authentications are logged and reviewed regularly for potential malicious activity. This prevents unauthorized changes or access to registrant data by individuals posing to be registrars or their authorized contacts.

These items reflect an understanding of the importance of balancing data privacy and access for registrants, both individually and as a collective, worldwide user base.

The Afilias 24/7 Customer Service Center consists of highly trained staff who collectively are proficient in 15 languages, and who are capable of responding to queries from registrants whose domain name security has been compromised - for example, a victim of domain name hijacking. Afilias provides specialized registrant assistance guides, including specific hand-holding and follow-through in these kinds of commonly occurring circumstances, which can be highly distressing to registrants

Security resourcing plans

Please refer to our response to question #30b for security resourcing plans.

---

**30(b). Security Policy: provide the security policy and procedures for the proposed registry, including:**

- **system (data, server, application / services) and network access control, ensuring systems are maintained in a secure fashion, including details of how they are monitored, logged and backed up;**
- **resources to secure integrity of updates between registry systems and nameservers, and between nameservers, if any;**

- **independent assessment report to demonstrate security capabilities (if any), and provision for periodic independent assessment reports to test security capabilities;**
- **provisioning and other measures that mitigate risks posed by denial of service attacks;**
- **computer and network incident response policies, plans, and processes;**
- **plans to minimize the risk of unauthorized access to its systems or tampering with registry data;**
- **intrusion detection mechanisms,**
- **details for auditing capability on all network access;**
- **physical security approach;**
- **identification of department or group responsible for the registry's security organization;**
- **background checks conducted on security personnel;**
- **a threat analysis for the proposed registry, the defenses that will be deployed against those threats, and provision for periodic threat analysis updates;**
- **number and description of personnel roles allocated to this area; and**

Answers for this question (#30b) are provided by Afiliias, the back-end provider of registry services for this TLD.

This response is divided into three sections: (1) security policies and procedures; (2) component level analysis of threats and mitigation for seven elements of security: facilities, registry systems, DNS, support infrastructure, connectivity, organization, and outage prevention, and; (3) resources. Answers include descriptions of:

- System and network access control: Section 1, Section 2, Element 2-7
- Resources to secure integrity of updates: Section 3
- Independent assessment reports: Section 1
- Provisioning and other measures that mitigate risk: Section 2, all elements
- Computer and network incident response: Section 1, Section 2, all elements
- Plans to minimize risks of unauthorized access to systems: Section 2, all elements
- Intrusion detection mechanisms: Section 2, Element 2, 3, 4, 5, 7
- Details of auditing capability of network access: Section 1
- Physical security approach: Section 1, Section 2 Element 1, 5 and 6
- Identification of department responsible: Section 3
- Background checks: Section 2 Element 6, Section 3
- Description of main security threats: Section 2, all Elements
- Resourcing plans: Section 3

Afiliias follows the guidelines from the ISO 27001 Information Security Standard (Reference:

[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=42103](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103)) for the management and implementation of its Information Security Management System. Afiliias also utilizes the COBIT IT governance framework to facilitate policy development and enable controls for appropriate management of risk (Reference: <http://www.isaca.org/cobit>). Best practices defined in ISO 27002 are followed for defining the security controls within the

organization. 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/>).

#### Security policies and procedures

The last decade has witnessed an explosive growth in Internet usage, new and ever-more-complicated threats to the DNS, and challenges with domain management. Throughout this exponential increase in threats, Afilias has maintained secure and stable systems, meeting the needs of registrars and end-users across the world. The experience gained has led to refined plans, strengthened protocols, improved procedures, and increases in security personnel - all of which is leveraged to provide high levels of security for this new TLD.

Afilias operates all of its systems in support of this TLD with security in mind and takes utmost care to ensure data confidentiality, integrity and availability. Access to all confidential information or data, whether physical/logical or written/verbal/visual, is strictly limited to authorized personnel. Other types of data are appropriately classified and, when no longer needed, destroyed.

All employees, contractors and other users who are given access to sensitive information must sign a confidentiality or non-disclosure agreement, and any requests for physical and logical access is properly authorized. Users are only given sufficient rights to enable them to perform their job function. Production, staging, development and testing environments are segregated at the physical and logical levels. Administrators for applications/systems have unique logins; generic accounts are banned. Password policies are based on well-defined industry security standards (e.g., ISO 27002). Encryption mechanisms protect management, backup and replication traffic; primary and secondary sites are connected via secure private leased lines. All registrar traffic is encrypted using TLS/SSL. Registrars use unique usernames/passwords for registry authentication; support requires individual passphrases.

Provisions are made to protect systems from virus and other malicious software. All systems and software are appropriately backed up and a disaster recovery and business continuity plan has been developed, documented and tested on a regular basis. Afilias' software development lifecycle ensures that our products are designed, developed and deployed in conformance with security policies. All security processes and procedures are documented and reviewed on a regular basis. Well-documented security incident response procedures are in place to ensure immediate attention to any security issue.

#### Security assessments and audits

Afilias performs a number of internal and external security audits each year of the existing policies, procedures and practices for:

- Access control;
- Security policies (e.g., password 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 Afiliias' 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 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, Afiliias 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, Afiliias performs internal security audits twice a year. These assessments are constantly being expanded based on risk assessments and changes in business or technology.

Additionally, Afiliias 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).

Afiliias has engaged with security companies specializing in application and



web security testing to ensure the security of web-based applications offered by Afiliias, such as the Web Admin Tool (WAT) for registrars and registry operators.

Finally, Afiliias has engaged IBM's Security services division to perform ISO 27002 gap assessment studies so as to review alignment of Afiliias' procedures and policies with the ISO 27002 standard. Afiliias has since made adjustments to its security procedures and policies based on the recommendations by IBM.

#### Background checks

As part of human resources best practices, background checks are performed on all personnel hired by Afiliias (full-time, part-time or consultant). These checks are performed by a third party vendor and include checks for criminal history, Social Security (to match the person's name to the Social Security number provided) and verification of employment for the most recent positions held. If the candidate has no past work experience, the education credentials are verified.

#### Intrusion detection

Each registry system component is monitored for security, performance and stability, both from within the data center and without. All production facilities have 24x7 onsite security staff to mitigate physical security breaches. Closed-circuit video cameras record any activity in and around the facility. Security personnel monitor these recordings and any anomaly detected is investigated and reported. Three different monitoring systems provide triple checks for potential problems. This allows the earliest possible warning of trouble to allow ample preparation in case of a detected fault. On-site and remote network and system monitoring ensure system security, service uptime and performance 24X7. Please see our response to question #42 for complete details about system monitoring and logging.

To effectively manage incidents, Afiliias has implemented a detailed incident management process. The process defines: team members involved; goals; communication plans for internal and external contacts; escalation details; recommendations; and resolution, along with incident report development requirements. In short, these multi-page procedures track an anomaly or potential issue from identification through problem resolution, e.g., change modification. To prevent any incidents related to unauthorized changes into the production system, Afiliias personnel follow well-defined change control procedures that require proper documentation, test plans, execution of test plans and appropriate approvals before a change can be deployed to the production systems or applications. Please see the details about these plans included in our response to question #37.

#### System security overview

Afiliias' EPP systems run with the minimal number of ports accessible by the outside world. All EPP transactions themselves are conducted using TLS/SSL certificates from authorized certification authorities for mutual authentication and encrypted communications. In addition, access to the EPP system is restricted via username and password pairs to authorized IP addresses only.

Afiliias' WHOIS servers rate-limit the number of responses a given set of IP addresses can receive, limiting the ability of spammers to data-mine our WHOIS database. This intelligent rate limiter slowly degrades the responses to systems that repeatedly send in numerous queries, thus making sure that "normal" usage is not affected.

In addition to the rate-limiting described previously, the web-based WHOIS service makes use of CAPTCHAs to mitigate abuse of the system by robots and other automated mechanisms. No AUTH-INFO codes or other high security data are available via the WHOIS.

Access to the zone file, if allowed by the registry policy, is provided over a secure connection and only allowed to authorized users that have signed a zone file access agreement with the registry operator.

External access to internal systems is only permitted via Virtual Private Networks (VPN). Leased lines are present between the registry data centers to ensure encrypted and secure communication of management and database replication traffic.

All network gear is secured by allowing only predetermined, non-standard usernames, using SSH with at least 1024-bit encryption keys. Access is further restrained by the rigorous use of Access Control Lists (ACLs) on all network access points and limiting access to pre-defined IP addresses only.

The Afiliias Intrusion Detection System (IDS) monitors network and system activities for malicious activities or policy violations and produces reports to a management station. This is a passive system.

In addition, the Afiliias Intrusion Prevention System (IPS) is an active/reactive system that responds to suspicious activity by taking necessary mitigation steps to protect the network and the infrastructure from malicious attack.

Alerts are generated for any unusual traffic patterns and sent to the appropriate groups for review and action.

All nameserver access is controlled via our Maintenance and Control Network. The only allowed access by the public is for DNS queries. All login attempts are monitored continuously. Afiliias DNS infrastructure is massively provisioned as an integral part of the DDoS mitigation strategy, thus ensuring sufficient capacity and redundancy to support new gTLDs. Please see our response to question #35 for details about the DNS service and its security.

Super user or "root" access to systems is not allowed. Only access using a logging proxy (such as "sudo") is permitted, and only after users on these systems have been fully authenticated. All sudo logs are monitored continuously. Access is only provided on an 'as needed' basis to staff members that require access to complete their job functions. The principle of least privilege is applied.

In the highly unlikely event of a problem, backups can be accessed to facilitate continuity of service. Afiliias uses an enterprise level backup solution, the IBM Tivoli Storage Manager (TSM), which provides automated data protection and addresses compliance with corporate and regulatory data retention and availability requirements. Afiliias maintains fully redundant backup nodes in each data center that back up data and configuration information from systems within the site on a daily basis. Local backups are maintained on site (for fast recovery) and also in a remote location (for Disaster Recovery purposes). Details regarding the backup policies and procedures are provided in our response to question #37.

The approach to security as described here is illustrated in Figure 30b-a.

#### Limiting data access

Securing the data starts at the first customer interaction with the Afiliias registry system. This begins with the data upload from the registrar using the EPP servers. The entire registrar connection is mutually authenticated and encrypted using TLS/SSL. Registrars accessing the EPP servers must have their systems registered in the Access Control Lists, and then must provide correct EPP credentials before access is granted. All data is checked for correct syntax and for rudimentary semantic errors and other EPP-related errors.

As verified data is received by the system, it is sent via internal networks to the database servers, which sit in an otherwise completely isolated private VLAN (Virtual Local Area Network). No passwords are stored in plain text.

Data destined for the DNS is verified by the EPP server for its syntax and completeness and then re-checked by the DNS Distributor application to ensure that the zone will correctly match the data within the registry. Only data that matches criteria as set by the registry policy will be published (e.g., a minimum of two nameservers for a domain). This data is then securely transported over our management network to the nameservers where the zone is made available for DNS queries. As a redundant measure, regular zone audits are conducted to ensure that the zone matches the registry data.

Access to the production database management system is limited to Database Administrators only and direct data manipulation is not allowed. Changes to the database management system have to be authorized and scheduled following a strict change control policy. Any changes made are logged and audited on a regular basis.

#### Physical security approach

All production facilities have 24x7 onsite security staff to prevent physical security breaches. Closed-circuit video cameras record any activity in and around the facility. The security personnel monitor the cameras and any anomaly detected is investigated and reported. Only authorized users have physical access to the production facilities. Only those personnel with government-issued photo identification and included on the authorized access list are permitted entry. Other visitors to these data centers cannot access our caged areas. An authorized staff member must accompany all visitors. Some production data centers also incorporate weighed man-traps, and access is monitored at all times by security personnel who screen identification. These weighed man-traps record the weights of authorized users on their way in and out. Since only authorized users are allowed to remove equipment from a cage, any major change in weight is noted and any user not authorized to remove equipment from a cage must undergo inspection by security personnel. This is in place to prevent theft of any equipment from the data center. Within the data centers, our own cabinets and cages are securely bolted to the floors.

Physical security is maintained at each Afiliias office. Employees are given access badges that only allow them into areas they are authorized for. For example, only Operations and NOC staff are allowed access into the server room. Cameras are also deployed to record all activities; the NOC staff monitors them. Any issues are quickly identified and escalated. Physical security systems are in place and alert authorities upon activation.

## Component-level analysis of threats and mitigation

Below are seven elements of security. Each element is presented with the following information: service/function, threat type, threat assessment on a scale of 1 (low or statistically improbable event that occurs less than once a year) to 5 (high risk of a threat that occurs at least on a daily basis), and detailed threat mitigation efforts.

### Element 1: Facilities security

Function: Data Centers host all registry systems

Threat types: Physical breach, network breach, power interruption, communications loss.

Threat assessment: 2 - low to moderate physical threat potential, moderate network breach, low to moderate power and/or communications interruption

Monitoring frequency: 24x7 continual monitoring

Threat mitigation efforts: Afiliias operates only in data centers engineered to eliminate any single point of failure, with multiple layers of redundancy in power systems, HVAC, and fire detection and suppression. Currently, Afiliias hosts operations in data centers around the world that meet or exceed these global best practices. All production and fail-over facilities are co-located, and have the following characteristics of world-class data centers:

- 24x7 on-site security personnel and security monitoring;
- Surveillance cameras covering the entire facility;
- Controlled access to the data center. Visitors must show government issued photo ID to be granted access to each facility and once inside must use a card key and bio-scanner to gain access to the data center;
- Two different power substations;
- Dual entry on different sides of the building;
- Automatic power throw-over switches;
- Multiple diesel generators and guaranteed fuel supply, also in a fully redundant array, are available for extended power outages;
- Raised floor space capacity;
- FM-200 fire suppression technology;
- Multiple air conditioning units configured in a fully redundant array;
- Multiple UPS power units with battery backup to provide electrical power;
- Server racks, cases, network cables and components systematically labeled with color-coded identifiers, minimizing human error during plant services work and accelerating trouble-shooting capabilities in the event of equipment failure;
- Redundant Internet connectivity from diverse vendors;
- High-level Service Level Agreements (SLA), and;
- Systems locked in cages in data center accessible only by authorized personnel.

Afiliias intrusion detection mechanisms include:

- Data center access control and identification on entry (ID and/or biometrics), 24x7 on-site security personnel and monitoring;
- Review of daily access logs for systems and network hardware review, and;
- 24x7 monitoring by Afiliias NOC.

Afiliias network monitoring includes a CISCO Intrusion Prevention System as well as firewall monitoring. Netflow software is also utilized to monitor network traffic flow and bandwidth. Alerts are generated for any unusual traffic patterns and sent to the appropriate departments for review and action.

### Element 2: Registry system

Function: Domain management, including updates and transfers

Threat types: Data corruption, data disparity between components of the registry system, unauthorized domain data access, registrar data compromised  
Threat assessment: 2 - moderate risk of unauthorized access or data compromises

Monitoring frequency: 24x7 continual monitoring

Threat mitigation efforts: Afilias electronic security ensures maximum security for its registry system through:

- Correct systems design to ensure that services are offered with minimal exposure;
- Correct authentication design, to ensure only authorized access; and
- Correct defensive design, to ensure that malicious or mistaken uses cannot disrupt operations.

The SRS, its associated support infrastructure, and DNS operations require distinct approaches to security.

Afilias uses a five-tier design to ensure that each service is exposed only to the degree necessary:

- Globally available services are exposed to the Internet in the web server tier. WHOIS and DNS are found in this tier.
  - Services that are available to some limited numbers of authenticated nodes are found in a separate network, which forms part of an extranet. The SRS servers and secure web interface are located in this tier, as are an FTP server for zone file transfers and the interface between the SRS and DNS servers. Additionally, individual application servers are partitioned by virtual networks (VLANS) to inhibit cross-server intrusion.
  - Services that communicate with both the database servers and servers in the web server tier are kept in the application tier (e.g. reports engine and various internal operational services).
  - The databases are isolated on a separate, RFC 1918-compliant network. The databases are not allowed any exit path outside the Afilias network. Similarly, no external systems are allowed inbound access to the databases.
  - Backup and management of the systems are performed via another separate, RFC 1918-compliant network that forms the management and backup tier.
- Afilias uses only strong encryption and multiple authentication methods in all tiers except the Web server tier.
- EPP connections are encrypted using TLS/SSL, and authenticated using both mutual certificate checks and login/password combinations.
  - Registry files are encrypted using OpenPGP as documented in RFC 2440 and sent to the secure servers of the escrow agent. The agent will use internally secure methods to ensure the integrity of all deposits.
  - Web connections are encrypted using TLS/SSL in the browser, and authenticated in the same manner as EPP connections.
  - Connections are limited to pre-approved IP addresses.
  - Bandwidth limitation on connections and number of sessions or requests from source IP address/network limitation (traffic shaping for EPP, rate-limiting for WHOIS, etc.).
  - Load-balancing (EPP, WHOIS, Web server).

To ensure that all registrar communications are secure, Afilias requires passwords from previously authorized contacts to authenticate the originator of every technical support inquiry, whether submitted by phone, fax, e-mail, or online web portal.

Finally, 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 outages for all registrars, even in the case of a security compromise at a subset of registrars.

The system is monitored for security breaches from within the data center and without, using both system-based and network-based testing tools. Operations staff also monitors systems for security-related performance anomalies. Triple-redundant, continual monitoring ensures multiple detection paths for any potential incident or problem. Network and Security Operations teams perform regular audits in search of any potential vulnerability.

The layered design, combined with strong encryption and multiple authentications, ensures both security and availability.

Data integrity is ensured the Afiliias DNS system. Afiliias' DNS system perform updates to nameservers using the Internet standard full transfer protocol (AXFR), defined in RFC 1034, and Internet standard incremental transfer protocol (IXFR), defined in RFC 1995. When transported across networks external to our facilities, these are secured by the use of transaction signatures (RFC 2845), as well as IP address filtering on both ends of the transaction. This helps to ensure a clean, complete transaction through each leg of the update process.

In addition to these standards, Afiliias monitors each zone for radical shifts in data or size, and prohibits these zones from propagation.

#### Element 3: DNS and DNSSEC

Function: Zone generation, publication and distribution

Threat types: DDoS attacks, unauthorized modification

Threat assessment: 5 - high risk of DDoS attacks, daily DNS attacks

Monitoring frequency: 24x7 continual monitoring

Threat mitigation efforts: Afiliias has designed a diverse DNS service. As described in our responses to questions #33 and #34, both our geographic diversity and unique service design offer seamless scaling and ensure 100% availability. In addition to this, the following measures are employed by Afiliias to mitigate DDoS attacks:

- BGP anycast for public read-only services (Afiliias uses several DNS nodes being announced with the same IP address for each zone served);
- Load-balancing for DNS, and;
- Massively provisioned hardware resources that with enough resource to provide service within SLAs under increased load.

Afiliias has never experienced a complete DNS resolution outage. Afiliias guarantees 100% availability of the critical DNS function. Please see our response to question #35 for more details regarding the DNS system and provisioning.

#### Element 4: Support infrastructure

Function: VPN connections, leased lines, remote access

Threat types: Unauthorized access, virus penetration

Threat assessment: 3 - moderate risk of unauthorized access

Monitoring frequency: 24x7 continual monitoring

Threat mitigation efforts: System management of the support infrastructure occurs remotely, for the most part, via high-speed virtual private network (VPN) connections. IPsec and SSH are used in tandem, to provide spoof-resistant, secured connections in all cases. To ensure that the management interfaces do not become a "back door" to the system, strict controls are

placed on anyone authorized to connect to the VPN, and from what locations. Connections are authenticated within the VPN (which includes machines in the operations center, as well as a small number of remote machines) using an IPsec-based public key infrastructure. Private leased lines are implemented between the production registry data centers and the support infrastructure so that any management traffic between these sites is encrypted and secured. Anti-virus software is installed on workstations, which check systems on a real-time basis. Anti-virus software is regularly updated and monitored by security personnel.

Afilias has implemented a variety of security measures to minimize the points of vulnerability in its production software infrastructure. Access to all production systems and software is strictly limited to senior level operations staff. Technical support and network operations staff members are provided read-only access, and limited to components required to help troubleshoot customer issues and perform routine checks. The Afilias network is segregated into multiple VLANs (Virtual Local Area Network) based on job responsibilities and departments within the organization. Each departmental VLAN is allowed access only to those components of the system that is required. Strict change control procedures are in place and are followed each time a change is required to production hardware, applications, or services.

To ensure no access is allowed outside of the controlled authentication system, all production machines are located behind firewalls that block all traffic attempting to reach any port or service that has not been audited.

Afilias deploys a secure replicated PostgreSQL database system. Necessary registry information is stored in the company's secure database and replicated among all its secure network nodes. This not only ensures that the data only exists in a secure location on secure machines, but it also ensures there are multiple live copies of the data, providing overall data security and redundancy. Access to each node is restricted to authorized personnel only.

Element 5: Connectivity/Internet services

Function: Communications

Threat types: Loss of connectivity, inadequate bandwidth

Threat assessment: 2 - low to moderate risk of connectivity loss or inadequate bandwidth

Monitoring frequency: 24x7 continual monitoring

Threat mitigation efforts: As presented in our response to question #31, Afilias has implemented extensive efforts to build redundancy into our systems, use high capacity hardware, employ load balancing, contract with multiple providers across the globe, and utilize numerous facilities technology to ensure environmental stability. Bandwidth is provisioned using multiple providers at each data center. "Burstable" bandwidth contracts are setup so that in the event of increased load, extra bandwidth is provisioned automatically. Alerts are place to ensure early detection of increased load. Automated failover mechanisms are in put place at the network layers using multiple networking protocols like Border Gateway Protocol (BGP), Virtual Router Redundancy Protocol (VRRP) and Hot Standby Router Protocol (HSRP) to ensure failover to the backup bandwidth provider in case of interruption to the main link. In addition to these, private leased lines are also set up between the primary and secondary data centers to ensure continuous operation in case of interruption.

Strict SLAs are in place with the bandwidth providers to ensure 100% network uptime.

Element 6: Organizational security

Function: Staff integrity, asset control

Threat types: Nefarious actors gaining access, asset loss

Threat assessment: 1 -low risk of staff threats

Monitoring frequency: Regular audits, risk assessments

Threat mitigation efforts: Afiliias has established a management framework to initiate and control the implementation of registry security inside and outside the organization. An established management team approves information security policy, assigns security roles and coordinates the implementation of security across the company.

Afiliias manages security with internal staff in the Operations group. All Afiliias new hires, from every department, are subjected to reference and criminal background checks. The security infrastructure ensures that access to organizational information processing facilities and information assets by third parties is controlled and tracked. Third parties are required to sign a confidentiality and non-disclosure agreement and employment contract with Afiliias that restricts their access and use to the information required for them to complete their tasks. Specific organizational security functions include:

- Security of assets: classification and control. All major information assets (such as databases or data files, system documentation and user manuals, training material, operational and support procedures, continuity plans, fallback arrangements and archived information) are tracked and have an assigned owner from the Afiliias security management team. Software assets such as application and systems software, development tools, utilities, as well as physical assets including equipment and parts, and service assets such as general utilities and utility vendors are all tracked to ensure control.

- Personnel security. Security responsibilities are set forth in Afiliias' security policy and are addressed as early as the recruitment of employees; security and information access controls are imposed in all Afiliias and Afiliias employee contracts. All employees and third-party users of Afiliias' registry system are required to sign a confidentiality (non-disclosure) agreement.

- Communications and operations management. To ensure the correct and secure operation of all Afiliias' information processing facilities, the operating procedures for the registry are formalized, and any changes require formal written sign-off from management. The major areas of focus in Operations Management at Afiliias include:

- Operational Change Control
- Incident Management Procedures
- Segregation of Roles and Responsibilities
- Separation of Development and Operational facilities
- Management of third-party access to Operational facilities

Element 7: Outage prevention

Function: All registry components

Threat types: Loss of system functionality, disaster

Threat assessment: 1 - extremely low risk all systems and backups experience an outage

Monitoring frequency: 24x7 continual monitoring

Threat mitigation efforts: Afiliias' system relies upon multiple, high-availability components in order to reduce the risk of failure. The SRS, WHOIS, and DNS services are able to continue to function, even in the event of a total failure of multiple servers or network devices. Subsystems are



interconnected with redundant networks to ensure that a data path is always available. The whole system is designed to avoid single points of failure and leverages our experience supporting both large and small domains.

There are five factors that contribute to Afilias' system being outage-resistant. Specifically, the registry has:

- Selected fault tolerant hardware so that, in most cases, the hardware can function even if part of it is damaged, and can be serviced without interruption.
- Built the system with multiple-redundant subsystems to ensure the entire system remains functional even if whole subsystems fail.
- Placed its data centers at multiple, geographically separated locations to ensure service even upon complete destruction of one data center.
- Used hardware and programming techniques that guard against introduction of bad data and allow multiple audit paths.
- Implemented development and operations policies and procedures to ensure the system always functions.

Afilias deploys infrastructure with redundancy at every level, starting from multiple network interfaces on a server, to secondary data centers that can be activated in the event of a disaster. Afilias deploys load balancing techniques at the application layer to ensure continued service in the event of a complete failure of one or a subset of servers. Multiple database nodes are set up at each location running on a cluster of database servers connected to redundant storage devices. Hardware selected is such that it would disable a failed component from its configuration and continue to operate after sending appropriate alerts. Details are provided in our responses to questions #37 through #41.

#### Security 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. 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. Security is integral to every aspect of Afilias registry operations. Over 40 highly qualified team members have shared responsibilities for defining and implementing security policy. This includes members from the dedicated security team, NOC and operations staff, development, human resources and legal departments.

Afilias operates a dedicated security department, with full time employees and vetted consultants who work on the development and implementation of security policies, security standards and best current practices. The security department works closely with senior management and develops the audit strategy, conducts periodic reviews and risk assessments and presents findings along with recommendations to management. The security team provides

security expertise to the entire company, and is responsible for regular employee training and education on security practices.

---

### **31. Technical Overview of Proposed Registry: provide a technical overview of the proposed registry.**

**The technical plan must be adequately resourced, with appropriate expertise and allocation of costs. The applicant will provide financial descriptions of resources in the next section and those resources must be reasonably related to these technical requirements.**

**The overview should include information on the estimated scale of the registry's technical operation, for example, estimates for the number of registration transactions and DNS queries per month should be provided for the first two years of operation.**

**In addition, the overview should account for geographic dispersion of incoming network traffic such as DNS, Whois, and registrar transactions. If the registry serves a highly localized registrant base, then traffic might be expected to come mainly from one area.**

**This high level summary should not repeat answers to questions below.**

Answers for this question (#31) are provided by Afiliias, the back-end provider of registry services for this TLD.

Afiliias' services are based on the experience of supporting more TLDs than any other provider. This and subsequent sections detail the elements that go into making our registry infrastructure one of the most flexible, distributed, scalable and proven registry services in the world, which includes:

- More than 10 years experience launching, growing and maintaining compliant, secure, stable and reliable TLDs;
- Using an infrastructure based on open standards and interoperability, and leveraging Open Source software (e.g., a PostgreSQL database);
- Integrating this TLD into a proven registry infrastructure that consistently meets or exceeds ICANN SLAs;
- Organizational focus on registry infrastructure that ensures the full interplay of technical, marketing, customer support, business, and policy activities, and;
- Utilizing a team of over 170 technical professionals skilled in operating the gTLDs, and a human resources plan to expand that team as needed.

Below Afiliias presents the holistic approach to our design, maintenance and enhancement of the registry infrastructure, all planning components, discreet TLD forecasts, service performance metrics, and the ample resource plan.

#### Registry system overview

Afiliias, a leading provider of Internet domain registry services, is prepared to provide all operational and technical services. Afiliias will support this TLD with a registry infrastructure that meets ICANN requirements and global standards for availability, efficiency, and security. Afiliias' systems and methodologies are proven, and successfully support the following TLDs: .INFO, .ORG, .AERO, .MOBI, .ASIA, .XXX, .IN, .AG, .VC, .BZ, .GI, .SC, .HN, .ME, .MN, and .LC. Each Afiliias Shared Registration System (SRS) is built to withstand large registration volumes and is among the fastest systems in the world.

This section details a technical plan for operating the registry operator's TLD, including:

- Provision of a state-of-the-art, EPP-based SRS that is reliable, efficient and secure to meet the registry operator's needs. (See our response to question #25 for more detail.)
- Delivery of fast, secure, reliable DNS with nameservers around the world to enable the registry operator's domains to resolve in near-real-time, worldwide. (See our responses to questions #34 and #35 for more detail.)
- Ensuring up-to-date security at every level, from facilities and hardware to software and processes. (See our response to question #30(b) for more detail.)
- Provision of a WHOIS service that is flexible and standards compliant. (See response to Question #26 for more detail)
- Enabling IDNs in alphabetic, ideographic and right-to-left scripts as needed, in addition to ASCII representation at the top level and all levels lower. (See our response to question #44 for more detail.)
- Committing to meeting or exceeding service level agreements (SLAs). (See our responses to questions #25, #26, and #35 for more detail.)
- Provision of a registry infrastructure based on open standards and interoperability. (See our responses to questions #32 and #33 for more detail.)
- Providing efficient design coupled with experience and capacity planning for seamless resource allocation and additions. (See our responses to questions #32 and #35 for more detail.)
- Advanced monitoring to mitigate failures, tested plans to address technical difficulties, and appropriate measures for restoring information. (See our responses to questions #37, #38, #39, #41, and #42 for more detail.)
- Continuing to lead in adoption of next generation technologies, such as DNSSEC and IDNs. (See our responses to questions #43 and #44 for more detail.)
- Skilled, experienced technical team dedicated to excellence in the operation and development of registry technology.

For DNS, Afiliias has built an infrastructure that enables it to guarantee 100% DNS resolution uptime for the TLD. The Afiliias primary DNS system, run and managed solely by Afiliias, is massively provisioned and utilizes sophisticated DNS architecture, hardware, software and redundant design. The overall DNS system also seamlessly incorporates pod (slave) servers from any number of secondary DNS service vendors, including the secondary vendor in used today (Packet Clearing House).

An overview of the registry infrastructure is presented in Figure 31-a, which shows the connection between each important component of operations. It

depicts the type of registry that will be operated and the interfaces that will be provided for registration transactions with Afilias. This description is based on Afilias' current TLD operations in compliance with ICANN requirements, and which exceed new gTLD requirements.

This technology provides a secure, stable and reliable infrastructure to support the TLD's business plans. The Afilias infrastructure is based on open standards and interoperability, and leverages Open Source software (e.g., PostgreSQL database). Access to source code allows better understanding of the workings 'under-the-hood', facilitates requests for features and functions tailored for our application, and provides access to a vast community-based support network. Afilias is also a respected contributor to Open Source, Internet protocol and standardization efforts, especially related to the domain name industry.

#### Size and scale of technical operations

The mission of this TLD is to enable domain internationalized domain name registrants to communicate beyond their script space. Afilias will support this TLD with its existing registry infrastructure, already in operation. Each function of the Afilias technical operation is massively provisioned and ready for immediate support of the TLD. The projected size of the registry for this TLD is presented in Figure 31-b.

Regardless of a gTLD's geographic needs, thanks to current capacity and ability to respond to changes in the geographic distribution of network traffic, Afilias is able to meet or exceed the gTLD's requirements. The traffic from this TLD will likely be a marginal increase to the wide variety of international traffic generated by the variety of gTLDs and ccTLDs currently managed by Afilias. This TLD is global in scope, anticipating look-ups from Internet users around the world. It will benefit from Afilias' highly diverse and geographic network (see responses #34 and #35), Afilias' highly scalable and secure SRS (see response #24) and WHOIS (see response #26) systems; proven load-balancing (see responses #33-35) and DNS architecture (see response to #35), and monitoring (see response #42) are also in place and more than adequate to serve this TLD. Any requisite scaling will be handled through the capacity planning process (see responses #32, #33, and #35). As a further measure of size and scale to meet needs, Afilias' business functions are divided among offices in Dublin, Ireland; Toronto, Canada; Horsham PA, USA; and New Delhi, India, and Afilias has fully operational customer service groups located in Toronto and New Delhi.

#### Afilias resourcing plan

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. Afilias Technical Operations are under the direction of the Executive Vice President/Chief Technical Officer. Afilias employs approximately 170 people in its technical operation (depicted in Figure 31-c) and is supported by the following team and functional areas.

Afilias is the registry service 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 necessary resourcing levels to provide high quality services with conformance to strict service requirements. Afilias currently manages over 20 million domain names under management, spread across 16 TLDs, with over 600 accredited registrars.

#### The HR Function

For an organization the size of Afilias, with its dedicated focus on domain name registry management, it is important to have a human resource function that is able to determine current staff utilization ratios, and to have activation thresholds once utilization exceeds certain values. Afilias' 11 years of experience servicing TLD customers, and managing the rapid growth in (a) the number of TLDs under management, (b) the number of domain names under management, and (c) the number of registrars accessing its systems have provided it with valuable data on what volume and kind of human resources are necessary to fulfill both critical and other essential registry service functions.

#### Triggers and Thresholds

Afilias has set a number of internal metrics that track the consumption of various human resources across the spectrum of domain name registry functions. These take into account both tangible factors such as the amount of time it takes to bring onboard personnel, the time for adequate training, the unique and specialized skills needed in the domain registry area, and intangible factors such as the behavioral attributes that are necessary to function as a high-performing member of the Afilias technical solution team.

The Afilias human resources platform provides its technical managers the ability to evaluate the utilization of resources, both current and planned. If planned utilization ratios exceed pre-set thresholds, they trigger automatic reviews of staffing, budgeting and talent acquisition functions in order to begin the process of augmenting qualified staff in the company.

#### Skills and attributes

Managing a domain name registry is a specialized function; not every engineer is well versed in the intricacies of managing the DNS, working with DNSSEC, or working with the unique characteristics of the domain name lifecycle, including anti-abuse procedures. Afilias maintains a strong working relationship with organizations that have a base of talent who might be relevant to the staffing needs of the company - for example, with local universities, technical schools and staffing companies. In addition, Afilias has a pre-selected list of vendors who have at least 3 to 5 years of experience in the domain name business, whose employees can be used as short-term consultants on projects that are time-critical or business-sensitive.

Each Technology department under the CTO is described below.

#### Product Strategy

The department is comprised of:

- **Product Management:** At Afilias, the Product Management team's role follows the classic definition, encompassing a breadth of disciplines that focus on designing, developing, managing and delivering world-class products. At the strategic level, Product Management gathers and analyzes a variety of data - Market and Competitive Intelligence, Customer and Business Requirements. At the tactical level, Product Management works closely with a broad spectrum of

stakeholders (Customers, Management, Sales and Marketing and Technology), and keeps the business apprised through up-to-date Product and Technology Roadmaps.

- Project Management Office ("PMO"): An Afiliias team that supports management in assessing and prioritizing work projects, as well as managing resource allocation. The PMO implements a best practices approach to project management (project charters, project plans, etc.) and directs the communication of project information between the project teams and the Customer. The project management and system development processes, plans, and other outputs identified are based on the existing Afiliias project management practices. They incorporate other best practices from throughout the IT sector as well as those of the Project Management Institute's Guide to the Project Management Body of Knowledge (PMBOK © Guide 2000 Edition).

#### Technology Department

The Technology Department is comprised of:

- Data Services: An Afiliias team of database administrators and architects responsible for maintaining the production databases for the registry, tools, and products that Afiliias supports.
- Operations: A group of Afiliias teams that design, evaluate, deploy and maintain the core Afiliias infrastructure. There are two subgroups. Network Engineering is responsible for maintaining the infrastructure and controlling access to the whole network. Systems Engineering manages the servers, storage subsystems and Storage Area Network. They are responsible for maintaining the hardware, the operating systems, system security and backups.
- Development: A group of Afiliias teams that design, develop, enhance, and maintain all core technology applications and services. There are two separate groups. Registry Services oversees the registry system and the Deferred Revenue System ("DRS") code, while Application Services oversees web sites and web applications, reporting, data warehousing, and billing.
- Production Control: An Afiliias team that plans production releases in advance of operations, establishes the route of each individual item or part of modules, determines when a release goes into production and when it is complete, is responsible for release control, and initiates the required follow-up to effect the smooth functioning of the enterprise software system.
- Quality Assurance ("QA"): An Afiliias team that tests the company's products. QA's primary responsibility is to ensure the end product meets the criteria defined in the business and technical specifications. The team achieves this by planning, documenting and testing to ensure there are no bugs or faulty processes in an application.

Members of each of these provide support 24 hours a day, 7 days a week.

#### Strategic Relationships and Technical Standards

This department is comprised of the Rapid Development Group, which examines and evaluates new Afiliias business proposals on a technical level and provides advice on these initiatives. The examination and evaluation process usually includes building a prototype to ensure the proposal is practical. Further, strong emphasis is placed on keeping abreast of technical standards

#### Resolution Services

This department is comprised of Content Propagation & Resolution ("CPR"), an Afiliias team responsible for provisioning and managing DNS services. CPR operates all of Afiliias' public-facing DNS infrastructure servers, and distribution masters inside CPR nodes.

#### Customer Care

The Customer Care Department has direct business relationships with registry customers including:

- Customer Support: This Afiliias team is responsible for the day-to-day operational contact between registrars and Afiliias. Customer Support is responsible for answering, investigating or escalating a registrar's business, marketing, billing or technical issues. Customer Support is also responsible for many internal processes, from updating balances to creating registrar accounts, as well as acting on any additional requests from registry operators or account managers.
- Network Operations ("NOC"): This Afiliias team is the primary point of contact for all technical service interruptions at Afiliias. The NOC monitors Afiliias' registry system and related systems, and provides initial investigation and problem identification. The NOC also manages the escalation to the appropriate technical support team for service interruptions and performance aberrations as defined by escalation procedures. The NOC provides the "first line of defense" against operational issues and technical problems, thereby reducing the impact that these problems have on Afiliias products, customers and the Internet community.

#### Account Management

Afiliias' global Account Management team serves as the primary business contact for the registry operators who contract for services with Afiliias, and is responsible for their customer satisfaction. Each Account Manager is expected to consistently provide excellent customer service to his or her TLDs, and represent clients' needs and goals within Afiliias. In addition, the Account Managers offer a consultant-based approach to deliver solutions to customers, enabling them to stay one step ahead in their pursuit of business opportunities.

Account Managers have a key role in the planning and execution of new TLD launches. He/she conducts reviews of all major deliverables (i.e., strategic brief, function specs, technical specifications, etc.) to ensure quality standards and that registry operator expectations are met. Account managers work closely with executives and operational personnel of each registry operator, and with Afiliias Technical Support and project management teams.

#### Security

The Security Department contains full-time employees and professional consultants with specific security skills who work on the development and implementation of security policies, security standards and best current practices. The security department works closely with senior management and develops the audit strategy, conducts periodic reviews and risk assessments and presents findings and recommendations to management. The security team provides security expertise to the entire company, and is responsible for regular employee training and education on security practices.

#### Consolidated Afiliias headcount

The headcount for Afiliias by location is presented in Figure 31-d.

It should be noted that these resources are shared across the TLDs that Afiliias supports, so most team members contribute their functional expertise on multiple TLDs. The Resourcing Plans in our responses for questions #23 - #44 reflect the number of individuals who will contribute in each area and should not be interpreted as "full time equivalents." Afiliias' resources are sufficient today to meet the needs of its new TLD customers and are easily and quickly scalable should the need arise.

Hardware and software resourcing plans

A vital component of successful registry operations is resource planning. Afiliias has detailed planning for every aspect of operations: hardware expansion, software upgrades and version control, staff planning and growth, as well as bandwidth and capacity planning, detailed in our response to question #32. Afiliias' track record speaks for itself - through sustained domain registration growth and traffic growth, resources have always been more than adequate to support all registry operations.

In summary, Afiliias has supported the operations of ICANN TLDs since 2001 and has an unbroken record of exceeding SLA requirements. Further, Afiliias' systems were extensively reviewed by ICANN during the .ORG, .NET, .ASIA, and .XXX application processes and found both compliant and capable. Afiliias has more experience successfully meeting ICANN's technical requirements on new gTLDs than any other provider. This proven technical platform will ensure this TLD will have comparable levels of technical excellence.

---

**32. Architecture: provide documentation for the system and network architecture that will support registry operations for the proposed scale of the registry. System and network architecture documentation must clearly demonstrate the applicant's ability to operate, manage, and monitor registry systems. Documentation may include multiple diagrams or other components sufficient to describe:**

- **Network and associated systems necessary to support registry operations, including:**
- **Anticipated TCP/IP addressing scheme**
- **Hardware (CPU and RAM, Disk space, networking components, virtual machines)**
- **Operating system and versions**
- **Software and applications (with version information) necessary to support registry operations, management, and monitoring**
- **General overview of capacity planning, including bandwidth allocation plans**
- **List of providers / carriers**
- **Number and description of personnel roles allocated to this area**

Answers for this question (#32) are provided by Afiliias, the back-end provider of registry services for this TLD.

Afiliias operates on a secure, stable and reliable architecture that utilizes:

- A highly distributed architecture that maximizes scalability, reliability and extensibility to easily support the operation of the registry;
- A load balancing solution that immediately responds to traffic increases without degradation of service;
- Detailed capacity planning processes for every aspect of the registry, and;
- A team skilled in successful TLD launches, migrations and operations.



This section provides a complete description of a fully-functional, scalable and stable registry and DNS system in the following order: an architecture overview including primary and secondary site hardware, the Afiliias load-balancing solution, and interplay between all registry elements; networking and associated systems to support registry operations; hardware, operating systems; software and applications used, an overview of capacity planning demonstrating ample capacity; a list of providers and carriers used in the registry, and; ample, existing resources to support the proven architecture. Note: Afiliias regularly monitors and upgrades its hardware and software, and the descriptions of machines, vendors and software below are merely indicative of the scale and type of solutions deployed.

#### Architecture description

Figure 32-a illustrates the Afiliias registry architecture described herein.

##### Primary site hardware

Afiliias uses enterprise-class hardware, which is designed with redundant components to tolerate failure, and which can be serviced without removing power. Proactive monitoring and health checks signal potential failures and provide opportunity to take corrective measures. Use of virtual machines allows Afiliias to move any running application and its data to a healthy server and storage without downtime. All data paths within the network are redundant and configured in active-active mode. Failure of a network or storage component would not cause interruption in a data path. Should a server fail unexpectedly, high-availability configuration would automatically restart the failed application on a healthy server without any intervention.

The registry system includes, but is not limited to the following:

- 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

As depicted in Figure 32-a, all networking equipment is duplicated for redundancy. Each data center contains a minimum of 25 blade servers running the registry in a high-availability configuration. Afiliias may adjust the equipment list and/or systems architecture to reflect the continuing advancement of both registry functionality and hardware/operating systems in the marketplace. Any changes therein will not adversely affect the sustained performance, security, stability or reliability of the registry.

##### Secondary site hardware

The hardware list for the secondary site is identical to the list noted above for the primary site. Redundant hardware is installed at the secondary site so that, if services need to run at this site for an extended period of time, there is adequate capacity as well as complete redundancy and fault tolerance in the environment.

The secondary registry facility is both a functional and standby facility, meaning that it would be activated for primary registry services if operational problems ever arose at the primary facility (due to natural disasters, etc.).

In the event of a catastrophe in the primary site, the secondary site would allow the TLD registry to continue to function with a minimum of disruption. In the event of the total failure of the primary data center, registrars would be notified of the decision to move operations to the stand-by center. Except for the change in physical location, nothing will change in the manner of operation. (For more detail, see our response to question #41.)

The secondary facility will be continuously synchronized with the primary. During normal operations, these databases can provide read-only data storage to various services, including the WHOIS servers. In failover mode, any of these systems may be promoted to become the primary database.

Afilias has detailed internal procedures for moving from the primary systems to the secondary. The procedures cover communications with registrars by the tech support team as well as internal coordination with vendors to ensure the primary to secondary cutover is handled properly. It includes database checks to ensure proper synchronization.

During normal operations, all application software will be set up at the secondary site and have the same software versions as the primary site. The load balancers will be set up similarly to the primary site. All firewall and rate limiting rules at the primary site will be set up at the secondary site. Afilias announces its own blocks of IP addresses such that once the applications have been started at the secondary site; all incoming connections can be routed to that site without the need for the registers to reconfigure their client applications.

All reports will be copied over to the secondary site.

#### Load balancing solution

Afilias has engineered its registry as a stateless system, managed with load balancers. This permits dynamic scaling at the application layer for all registry functions. Afilias' applications exercise 5-6% sustained load on the current application servers, with bursted loads of up to 12-13%. The servers are operated with a minimum bursted capacity of 50% over sustained loads. In the event of unexpected load increase, this available overhead permits Afilias to promote additional resources into production without expected degradation of service.

In the event of unexpected or unplanned load that results in contention, Afilias' server complex provides equal access to all registrars for those available resources through the use of a rate-limiting and bandwidth-shaping network appliance. This device limits each registrar from their permitted known IP source addresses to a combined maximum number of concurrent connections to the registry. The total number of connections permitted to each registrar is decided based on the defined connection usage policy.

These devices are also capable of throttling or shaping specific types of packet requests, allowing Afilias to set priorities on not only the number of concurrent connections a registrar is permitted, but to also prioritize the type of traffic.

These devices are part of a design to maintain equivalent access despite periodic attempts by a few aggressive registrars to over-utilize bandwidth and capacity.

Networking and associated systems of the registry architecture

The multi-layered architecture is comprised of the following key components: a collapsed core-aggregation along with service and access layers. The multilayered design allows for modular components or building blocks to be added as the demand and load increases. The perimeter devices provide Layer-3 routing for all traffic in and out of the data center and maintain peering and transit relationships with multiple BGP neighbors on different autonomous systems. The aggregation layer serves as the Layer-3 and Layer-2 boundary for the data center infrastructure as well as being the connection point for the primary data center firewalls. Services such as server load balancers, traffic shaping, intrusion prevention systems, application-based firewalls, network analysis modules, and additional firewall services are deployed at the services layer. The data center access layer serves as a connection point for the virtualized and non-virtualized systems in the server cluster. The virtual-access layer refers to the virtual network that resides in the physical servers and the virtualized servers in the Cisco UCS deployment. Finally, connectivity to database servers from the application server cluster must traverse an additional firewall layer located at the aggregation layer in order to establish the connections.

Figure 32-b is a general overview of the network and computing elements that comprise the registry architecture which is based on industry best practices.

From a routing perspective, the operation of the DNS system is based on anycast, which is the practice of making a particular service address (e.g., the destination address used by DNS resolvers to reach a particular authoritative server) available in multiple discrete autonomous locations.

There are numerous advantages that anycast provides for certain types of traffic, specifically those with very short transaction times such as DNS over UDP transport. The following is a summary of some of those advantages.

- Mitigation of non-distributed denial-of-service attacks by localizing damage to a single anycast node; this is possible because anycasted DNS system queries are mostly answered by the node closer to the source of the query.
- Constraint of distributed denial-of-service attacks or flash crowds to local regions around anycast nodes. The task of dealing with attack traffic whose sources are widely distributed is itself distributed across all the nodes that contribute to the service. Since the problem of sorting between legitimate and attack traffic is distributed, this may lead to better scaling properties than a service that is not distributed.
- In most cases, improvement of query response time is seen, by reducing the network latency between client and server.
- Reduce a list of servers to a single, distributed address. For example, a large number of authoritative nameservers for a zone may be deployed using a small set of anycast service addresses; this approach can increase the accessibility of zone data in the DNS without increasing the size of a referral response from a nameserver authoritative for the parent zone.

Monitoring of the systems is done from probes distributed across the Internet, and the identity of the node answering individual requests is recorded along with performance and availability statistics. The RIPE NCC DNSMON service is an example of the monitoring services used by Afiliis. For more information on the DNS, see our response to question #35.

#### Aggregation layer and firewalls

The aggregation switches used in this design currently are a pair of Cisco Nexus 7000 Series switches. They are used as a high performance 10-Gigabit

aggregation point for data center traffic and services.

The Cisco Nexus 7000 introduces the concept of Virtual Device Context (VDC). The VDC feature allows for the virtualization of the control plane, data plane, and management plane of the Cisco Nexus 7000. From a security standpoint this virtualization capability can provide an enhanced security model. Because the VDCs are logically separate devices, each can have different access, data, and management policies defined.

The design described in this document includes a single pair of data center aggregation switches divided into four separate logical switches. Two VDCs have been created in each Cisco Nexus 7000—VDCA and VDCB. This provides an inside and outside isolation point at the data center aggregation layer. The outside VDC provides Layer-3 connectivity to the data center external perimeter routers. The inside VDC provides Layer-2/3 connectivity to the data center services and server clusters.

For traffic to flow from the outside VDC to the inside VDC, the traffic must be routed or bridged through an external device. In this design, traffic forwarding between the VDCs is performed by external firewalls.

The aggregation layer also provides a filtering point and first layer of protection for the infrastructure. This layer provides a building block for deploying firewall services for ingress and egress filtering between each of the tiers.

Because of the performance requirements, this design uses a pair of Cisco ASA 5585 firewalls connected directly to the aggregation switches. The Cisco ASA5585s provide 10-Gbps of stateful packet inspection.

The Cisco ASA firewalls are configured in routed, active-standby mode with multiple contexts using the virtual context feature. This virtualization feature allows the firewall to be divided into multiple logical firewalls each supporting different interfaces and policies. Due to the modular aspect of this design, additional firewalls can be deployed at the aggregation layer as the server cluster grows and the performance requirements increase.

Access layer, server/network virtualization and network security  
For a complete description of the access layer and the server/network virtualization and network security, please see our response to question #24.

TCP/IP addressing scheme

The DNS uses anycast (as suggested in RFC 4786) to announce "service addresses" for the TLD zone. Typically, Afilias uses four IPv4 and two IPv6 "service" addresses for the TLD nameserver set. These addresses are routed to data centers around the globe to answer DNS queries. As with all Afilias-run zones, all IPv6 traffic is native - Afilias does not have any tunneled IPv6 transit provisioned.

For the registry system, Afilias announces its own blocks of IP addresses such that, once the applications have been started at the secondary site, all incoming connections can be routed to that site without the need for registrars to reconfigure their client applications.

Hardware

Afilias has considered the effects of significant increases of load on all parts of the system and has architected each major piece to be well

provisioned but able to be quickly enhanced if needed.

#### Servers

Afilias' applications and databases run within virtual machines (VM) on a cluster of powerful Intel Westmere [T1] processor-based servers (or more current technology) that allow the processing resource available to a particular VM to change dynamically as demand changes. Nevertheless, every VM is guaranteed minimum processor resource to ensure compliance with performance-based SLA. Processor, memory and input/output demands are proactively monitored, and provisioned to handle occasional high loads adjusted.

Software, applications and support

#### Databases

Afilias uses PostgreSQL for its databases, and uses it to support large TLDs such as .ORG, a registry containing almost 10 million domains and over 100 million contact and nameserver objects.

The current design and load tests of the Afilias database have shown that this TLD can expect no problems in scaling to meet demand. Afilias is prepared to make adjustments if needed, however, and these can be easily incorporated due to the flexibility of the architecture.

Another key feature of PostgreSQL is multi-version concurrency control (MVCC). MVCC ensures that every user sees a view of the database proper to the transaction. Traditional locking makes for slow query times when under high load. MVCC prevents that problem, meaning that queries are just as fast for 1,000 users as for 100 or 10.

#### Backup systems

Afilias uses an enterprise-level backup solution IBM Tivoli Storage Manager (TSM) that provides automated data protection and addresses compliance with corporate and regulatory data retention and availability requirements. Afilias operates fully redundant backup nodes at each data center that backup data and configuration information from systems within the data center on a daily basis. Local backups are maintained on site (for fast recovery) and also at a remote location (for disaster recovery purposes). All backup activities are fully monitored according to best practice standards. Random backups are also restored periodically to check their validity. For more information on backups and data escrow, please see our responses to questions #37 and #38.

#### Support systems

Support systems include WHOIS, financial systems and reporting. WHOIS and financial systems are designed to work from replicated databases, not the publisher database. Excessive production system load will not affect performance of the WHOIS and financial support systems.

#### Maintenance

Ongoing maintenance work is largely focused on optimization of the databases, applying fixes and enhancements to the operating system and updating hardware microcodes. Other uses of maintenance periods include the updating of registry software to add enhanced and improved feature sets. Additional and unexpected loads do not affect the maintenance periods required for code promotion.

Afilias' data structure is designed to be distributed across two or more

databases in the event of unexpected increased load, resulting in a smooth, horizontal scalability to handle very large, orders of magnitude increases in unexpected load..

#### Personnel

In the event of unexpected volumes of registration, the primary staff area that would be affected would be Afiliias' Tech Support staff. These departments have well-documented procedures and training materials providing the ability to rapidly train additional staff. Running on a 24x7 basis, the Tech Support staff has the ability to add personnel on a shift-to-shift basis in response to unexpected loads. In further support of these areas, at any given time two managers are available on call to assist with any unexpected staffing issues.

#### Operating systems and versions

The Afiliias registry system currently uses the following operating systems: Red Hat Enterprise Linux Server v6.1, Free BSD 8.1, and Ubuntu 10.04. Versions are updated as they are validated by the staff and security patches are actively kept current.

#### Software and applications

The Afiliias registry system currently uses the following software and applications: PostgreSQL 9.1, Tivoli 6.1, Slony 2.1, Tomcat 6.0, BIND 9.7.3-P3, NSD 3.2.1 (with internal patches), NagiosXI v2.11-1, OpenNMS 1.8, and Cacti v0.8.7h. Versions are updated as they are validated by the staff and security patches are actively kept current.

#### Capacity planning

Systems and capacity planning are another element of ensuring secure, stable and reliable operation of the registry system. Afiliias has more than adequate bandwidth and a comprehensive capacity management plan to meet the needs of this TLD (and all other applied-for TLDs using Afiliias as back-end registry services provider). The Afiliias approach involves:

- Predictive Analytics tool to forecast capacity needs and anticipate availability problems through predictive trending that allows us to visualize and proactively manage upcoming operational issues and infrastructure requirements;
- Projections of future capacity requirements based on historical and outlook analysis, to reduce the risk of system overload, and automatic capacity increase measures if thresholds are exceeded, and;
- System acceptance parameters, including controls on performance and computer capacity requirements, allocated burn-in periods, ensuring correct patch levels are applied, and subscribing to appropriate Computer Emergency Response Team (CERT) and similar security advisories.

Internet connectivity is provided between registry system data centers as described below:

- Connectivity between the Internet and the primary (and secondary) registry data centers is via multiple redundant connections. In addition, connections between servers on the intra-data center registry system network is via redundant multi-homed 10 Gbps Ethernet. Connectivity between the primary and secondary registry system data center (for replication) is via private leased line with failover to IPsec connections.
- High capacity routers and switches are used to route traffic to registry system servers.
- Load balancing is used for distributing requests across servers to avoid overloading any one server. The load balancers also provide TLS/SSL

offloading (TLS/SSL encryption/decryption).

- Internet connectivity is supplied via a BGP-based solution with fully diverse connections to multiple ISPs. Internet connections at both the primary and secondary sites are provisioned for bursty traffic.

Specific bandwidth provisions by critical registry functions include:

- DNS Servers: Each DNS hub has multiple gigabit transit from at least two providers, and separate bandwidth dedicated to provisioning and zone updates. Additionally, Afilias maintains many arrangements with peering providers such as Equinix, AMSIX and NL-IX.
- Core registry infrastructure (SRS, application servers, database): Each data center has multiple providers with up to 1Gbps of available access.
- WHOIS systems: Each data center has multiple providers providing 30Mbps, burstable to 100Mbps.

Providers and carriers

Figures 32-c through 32-e detail the providers and services for the Afilias registry system. These images and tables demonstrate geographic diversity and redundancy in the Afilias network.

Network numbering

The data-centers hosting the Afilias registration systems are all interconnected by a full mesh of metro links at a speed of 1Gbs, with the ability to support up to 4096 VLANs on each link via the 802.1Q tunneling standard (Q-in-Q).

Figure 32-f depicts the Afilias registry system and internal data center locations along with the available transit providers and their Autonomous System numbers.

The publicly available registry system components are numbered from provider-independent IP address blocks and are originated from Autonomous system 21775. Provider-independent IP address blocks are desirable for implementations where high availability is required. Following are a few of the important benefits that provider-independent blocks provide:

- The registry is decoupled from any particular ISPs and failure of the primary local transit carrier will not cause service disruption. As pointed out earlier, all data center locations are interconnected via high-speed metro links that are used as a backup path to make any of the other carriers available as transit to any of the colocation sites.
- Traffic can be shifted from one data center to the next via traffic engineering by announcing a more specific prefix at the new data center without the need for DNS changes or global traffic load balancers. This dramatically reduces downtime attributable to servicing the infrastructure since an entire data center can be freed very quickly to perform software updates or other maintenance tasks.

The equipment dedicated to handle the perimeter network, peering and metro links are Juniper MX-40 3D series routers.

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. Security is integral to every aspect of Afilias registry operations.

Afilias has 49 technical and operational staff consisting of mostly System Administrators and Database Administrators that will be called upon throughout the implementation and continue on-going maintenance of this TLD. This proven team includes: the Data Services team, QA, various developers, and security staff.

---

### **33. Database Capabilities: provide details of database capabilities including:**

- **database software,**
- **storage capacity (both in raw terms [e.g., MB, GB] and in number of registrations / registration transactions),**
- **maximum transaction throughput (in total and by type of transaction),**
- **scalability,**
- **procedures for object creation, editing, and deletion,**
- **high availability,**
- **change notifications,**
- **registrar transfer procedures,**
- **grace period implementation,**
- **reporting capabilities, and**
- **number and description of personnel roles allocated to this area.**

Answers for this question (#33) are provided by Afilias, the back-end provider of registry services for this TLD.

Afilias supports its TLDs with PostgreSQL, an advanced open-source database, and the same Relational Database Management Systems (RDBMS) Afilias uses in all of the shared registry systems that Afilias operates, including .INFO and .ORG. Afilias' database capabilities include:

- Managing a registry database with 500 million domain, contact, and host objects;
- Running a PostgreSQL database that has large storage capacity, smooth scalability and rapid expandability;
- A technical team with decades of combined experience managing all aspects of object management, updates, maintenance and reporting, and;
- Experience handling both sustained and rapid growth resulting in 150x storage growth over the past nine years.

#### Database software

PostgreSQL is a proven, high-performance relational database system that offers the broad scalability and integration required for a mission-critical environment. This robust solution supports enterprise-scale information management by providing management tools, flexible data access, full SQL support, and integrated globalization support via Unicode.



PostgreSQL provides the following benefits, among others:

- Large data storage capability. Ability to store large volumes of data in a single table (as much as 32 TB in one table) with high performance.
- Smooth scalability. The Afilias PostgreSQL databases successfully scaled from 6,500 domains to over 220,000 domains during the .IN launch (in under 90 days) and currently support nearly 10 million .ORG domain names. A key to its smooth scalability is PostgreSQL's large capacity and ability to handle multiple simultaneous operations quickly and efficiently.
- Extensive database functionality. PostgreSQL performs all the functions required of a modern registry database, as shown by Afilias' success in supporting the .INFO and .ORG TLDs, in addition to 14 others.
- High performance. Afilias' registry service is designed to consistently handle high transaction loads and still deliver excellent response time. One way Afilias accomplishes this is through the PostgreSQL multi-version concurrency control (MVCC). MVCC is a method of ensuring that every database transaction sees a completely consistent view of the database, while at the same time ensuring that very high transaction volumes can be accommodated. PostgreSQL can handle a large amount of data and allow for high concurrency of users.
- Data portability and standards compliance. PostgreSQL offers enhanced flexibility for data integration and portability through SQL standards support. PostgreSQL supports cross-platform processing through options that provide distributed data management and fault-tolerant data replication. Native support for standard protocols such as Java Database Connectivity (JDBC) and Open Database Connectivity (ODBC) allows access from the most popular development tools.

The largest registry that Afilias supports with PostgreSQL is .ORG, which contains nearly 10 million domain names, 106 million contact objects, 250,000 nameserver objects, and handles more than 200 million EPP transactions and queries per month. These transactions exceed the required SLAs.

#### Replication and backup

Afilias uses a sophisticated system to ensure that the registry database is continuously replicated to backup and disaster recovery copies. As registrars make transactions in the system, those records are flowed to the backup and disaster recovery copies in separate data centers. In the event of a disaster at the primary data center, a replicated copy would be used to bring the registry back online.

#### Slony replication - always backed-up database

Afilias' PostgreSQL implementation incorporates an advanced database replication technology called Slony. Slony is a system designed for multiple data centers and multiple backup copies where the normal mode of operation is all copies are available. Slony is an open-source software project with active participation from individuals and production deployment in organizations from around the world. Afilias helped develop this technology which allows the registry database to be run from anywhere in the world and still retain complete availability and backup capabilities. Slony is a real-time "master to multiple replicas" replication system with cascading and failover functionality included.

Slony includes all features and capabilities needed to replicate large databases to many secondary systems. Slony's asynchronous replication innovation enables the single master database to have multiple replicas. Beyond this, each replica may have cascaded replicas, thereby further improving robustness without sacrificing performance.

A representation of a cascaded replica is shown in Figure 33-a.

Slony gives the registry system the following important stability and reliability features:

1. The ability to install, configure, and create a replica and let it join and catch up with a running database. This allows the replacement of master and replica databases with minimal disruption. It also enables cascading replicas that in turn add scalability, distributes the load, and enhances proper handling of failover situations.
2. Allow any node to take over for any other node that fails. In the case of a failure of a replica that provides data to other replicas, the other replicas will continue to replicate from another replica or directly from the master. In the event a master node fails, a replica can receive a promotion to become a master. Any other replicas can then replicate from the new master.

Because Slony is asynchronous, the different replicas may be ahead of or behind each other. When a replica becomes a master, it synchronizes itself with the state of the most recent other replica, ensuring a smooth transition to the most current data—even after a major failure. A graphic showing how replication continues after failure is shown in Figure 33-b.

#### Storage capacity

Current storage infrastructure can provision for the growth of the registry Infrastructure and accommodate new gTLDs for all locations. IBM's Storwize V7000 Unified Disk System has the capability to add additional disk space with new expansion units in real-time with no interruption in service.

PostgreSQL has no limits for the size of databases/tables/records up to the capacity of the hardware (disk space), which can be increased as required. (As much as 32 TB can be held in one table.) Likewise, PostgreSQL has no limits for transaction throughput up to the capacity of the hardware (CPU speed, memory), which can be increased as required.

The forecasted database size for this TLD is under 500 MB . Thus, the database existing software exceeds the requirements for this TLD.

#### Maximum transaction throughput

There is no known limitation to the Afiliias database implementation. Afiliias' system has been designed to be scalable while maintaining reliability, stability and speed. Two historical examples illustrate the ability of the system to absorb sudden large load increases.

1. .INFO Growth: .INFO has grown to be the seventh-largest top-level domain on the Internet. During its growth, Afiliias has managed significant spikes in registrations while continuing to exceed all SLAs.
2. 2005/2006 PPC growth: 2005 and 2006 saw dramatic increases in domain tasting (creating a domain name expressly to test its ability to attract traffic) and PPC (pay-per-click) traffic in the domain industry. On just one day in 2005, Afiliias received and successfully handled a 42x increase in domain transactions - a dramatic and unprecedented increase in traffic in the registry. Registrars, registrants and Internet users saw no degradation in performance - in fact, Afiliias continues to improve its year-over-year performance capabilities, and operates significantly below the demanding SLAs in the .INFO and .ORG contracts with ICANN.

Afiliias' ability to maintain service quality despite variations in load is

critical to the successful performance of the TLD. Afilias' systems have the proven capacity to support the expected volumes and potential peak demands and the ability to scale quickly if the TLD expands faster than anticipated. Afilias' current transactional volume in the registry system represents less than 5% of current capacity and less than 3% capacity of the DNS system. Further, the Afilias architecture is scalable to meet future growth needs, with regular reviews and defined triggers to determine when hardware or system upgrades are necessary.

#### Scalability

Registry system design allows for scalability both horizontally and vertically:

- Systems:
  - Vertical - systems can be upgraded with faster CPU, and more memory to increase their performance. With use of virtualization technology, services can be moved to an upgraded system without any downtime.
  - Horizontal - additional virtual machines can be provisioned on demand to handle increased load for the registry.
  - Afilias has existing contracts with vendors and data center providers to allow this to happen in real-time with no interruption in service.
- Storage:
  - Vertical - faster disks can replace existing disks to reduce access time and increase the performance.
  - Horizontal - more disks can be installed to increase overall performance, improve response time, and expand capacity.
  - Afilias has existing contracts with vendors and data center providers to allow this to happen in real-time with no interruption in service.

PostgreSQL increases the database/table size automatically when required. The Database Services team monitors the disk space usage as part of their production support duties, mitigating any risk with scalability. This existing architecture can scale to well above the high-volume scenario projections of this TLD.

The Afilias registry databases have grown from 30GB under management in 2002 to over 1.5TB in 2011, a 150x growth rate. The number of connections into the registry during this same period has also grown from just over 200 to almost 2500 connections, growth over an order of magnitude.

#### Procedures for object creation, editing and deleting

EPP objects (domains, contacts, hosts) are managed by the EPP server via database transactions. Database objects (tables, etc.) are created using the built-in facilities provided by PostgreSQL (DDL SQL statements). Required additions/changes to the database schema, which usually occur due to application changes, are the result of cooperative effort between software developers and Database Administrators (DBAs).

Schema additions/changes are developed in distinct phases, with a design phase always preceding the implementation phase. As changes are done via standard SQL, databases are set up with special privileges granted only to the DBAs, ensuring that only experts apply changes and thus enhancing the stability and reliability of the database system.

#### User and credential management

The Afilias database system is designed with strict user and credential management. Database users are completely separate from any other system users. Database users are created with specific roles that only allow those

users to perform their job functions. Read only database users are created for reporting and monitoring purposes. Application users are created with write privileges to create and modify objects in the database. Special administrative privileges are assigned to Database Administrators to allow them to manage the database itself (e.g., install, make schema changes and purge) and replication software. These users are audited at a minimum twice per year as part of our regular internal and external audits.

#### High availability

The Afiliias database system is designed to offer a high level of availability, which is especially seen in two principal areas:

- Data center high availability includes:
  - Secondary geographically diverse data center for failover
  - At least two independent bandwidth providers to data centers for network failover
  - Data center redundant power (N+1) minimum configuration
  - Data center redundant cooling (N+1) minimum configuration
- Systems high availability includes:
  - Redundant network connectivity to all systems (bonding/ether channel)
  - Registry application load balanced for high availability for registrars
  - Databases running on virtual machines using VMware vSphere High Availability configuration for automatic failover and restart on a healthy system in the event of hardware or operating system failure
  - Databases continually replicated on-site and to geographically diverse locations
  - Databases on high availability storage disk arrays (IBM Storwize V7000 with 99.9999% availability)

As an additional mitigation, PostgreSQL is capable of recovering from a crash up to the last completed transaction; database replicas are kept up-to-date via a sophisticated replication system (Slony), and can be used to fail-over to them. Database backups are stored on-site and off-site and can be used to recover if required.

#### Change management procedures

The change process is managed in accordance with best practices as defined by the Information Technology Infrastructure Library (ITIL). Changes to the database or any production system are conducted in accordance with the Afiliias Change Management Process. This process ensures that standardized methods and procedures are used for efficient, prompt, stable and reliable handling of all changes to reduce the risk associated with changes to the production environment. The objective of the change management process is to ensure that changes are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.

The Maintenance Advisory Team (MAT) meets to discuss all requested changes to ensure that all changes have been thoroughly tested prior to implementation. Additionally, no change will be approved to proceed by the MAT without the development and testing of a remediation plan to ensure there is no service disruption if the change is unsuccessful.

Finally, the Change Management Process seeks to ensure that no production system changes occur without authorization from the MAT, eliminating the risk of poorly tested or poorly planned changes potentially disrupting services or systems. This process is depicted in Figure 33-c.

#### Reporting capabilities

Afilias offers three types of external reporting: to the registry operator, to registrars and financial. All reporting for ICANN will be in accordance with the requirements listed in the new gTLD Registry Agreement, Specification 3. Afilias will provide the registry operator with all technical data necessary to report to ICANN.

Afilias has several types of performance monitoring, and the database, like every system, is fully monitored on a 24x7 basis by our NOC. For more information, please see our response to question #42.

#### Database 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. Security is integral to every aspect of Afilias registry operations.

There are 72 Afilias team members with knowledge of and support of the database infrastructure. Of this, Afilias has ten resources dedicated to database design, development and architecture. A team of database administrators (DBAs) participate in application development and implementation during business hours, and support production on a 24x7 basis. Some team members also participate in the open source community by contributing code to PostgreSQL and Slony; others conduct testing and verifications of new versions. All of these team members will contribute to the implementation and on-going maintenance of this TLD.

---

### **34. Geographic Diversity: provide a description of plans for geographic diversity of:**

- **a. name servers, and**
- **b. operations centers.**

**This should include the intended physical locations of systems, primary and back-up operations centers (including security attributes), and other infrastructure. This may include Registry plans to use Anycast or other geo-diversity measures. This should include resourcing plans (number and description of personnel roles allocated to this area).**

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS , WHICH ICANN INFORMS US (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE, ACCORDING TO SPECIFIC GUIDANCE FROM ICANN UNDER CASE ID 11027.

---

**35. DNS Service Compliance:** describe the configuration and operation of nameservers, including how the applicant will comply with RFCs. All name servers used for the new gTLD must be operated in compliance with the DNS protocol specifications defined in the relevant RFCs, including but not limited to: 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 3901, 4343, and 4472.

**Describe the DNS services to be provided, the resources used to implement the services, and demonstrate how the system will function. Suggested information includes: Services. Query rates to be supported at initial operation, and reserve capacity of the system. How will these be scaled as a function of growth in the TLD? Similarly, describe how services will scale for name server update method and performance. Resources. Describe complete server hardware and software. Describe how services are compliant with RFCs. Are these dedicated or shared with any other functions (capacity/performance) or DNS zones? Describe network bandwidth and addressing plans for servers. Describe resourcing plans (number and description of personnel roles allocated to this area).**

**Describe how the proposed infrastructure will be able to deliver the performance described in the Performance Specification (Specification 6) attached to the Registry Agreement. Examples of evidence include:**

- **Server configuration standard (i.e., planned configuration)**
- **Network addressing and bandwidth for query load and update propagation**
- **Headroom to meet surges**

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS, WHICH ICANN INFORMS US (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE, ACCORDING TO SPECIFIC GUIDANCE FROM ICANN UNDER CASE ID 11027.

---

**36. IPv6 Reachability:** the registry supports access to Whois, Web-based Whois and any other Registration Data Publication Service as described in Specification 6 to the Registry Agreement. The registry also supports DNS servers over an IPv6 network for at least 2 nameservers. IANA currently has a minimum set of technical requirements for IPv4 name service. These include two nameservers separated by geography and by network topology, each serving a consistent set of data, and are reachable from multiple locations across the globe. Describe how the registry will meet this same criterion for IPv6, requiring IPv6 transport to

**their network. List all services that will be provided over IPv6, and describe the IPv6 connectivity and provider diversity that will be used. Describe resourcing plans (number and description of personnel roles allocated to this area).**

Answers for this question (#36) are provided by Afilias, the back-end provider of registry services for this TLD.

All Afilias-provisioned TLDs support IPv4 and IPv6, as will all new Afilias-supported TLDs. Afilias has met the IANA IPv6 specifications since 2008.

Support of IPv6

The registry will support DNS servers over an IPv6 network for all nameservers, separated by geography and by network topology, each serving a consistent set of data and reachable from multiple locations across the globe.

IPv6 connectivity to Afilias registry services is designed to be highly available, secure and flexible using multi-homed BGP with Afilias advertising its own portable IPv6 address blocks from multiple core routers. IPv6 connectivity to Afilias is provided by multiple Internet service providers natively. These providers include Q9 Networks (AS12188), AT&T (AS17232) and nLayer Communications (AS4436). This is subject to change as conditions dictate over time.

Afilias' intends to provide all of its registry services over IPv6 with the same SLAs currently available on IPv4. IANA currently has a minimum set of technical requirements only for IPv4 name service. Afilias exceeds these requirements and fully supports IPv6.

The descriptions below are based on current operations of services Afilias provides in compliance with ICANN requirements. Afilias will meet or exceed ICANN requirements for new gTLDs.

Specification 6 compliance

Afilias advertises its own portable IPv6 address blocks from multiple core routers. IPv6 connectivity to Afilias is provided by multiple Internet service providers natively. As it is an inherent part of the registry design, no additional implementation or steps are required to enable IPv6.

To be highly available, secure and robust, Afilias' current network infrastructure is comprised of private circuits between the production data centers. This assures the necessary IPv6 highly available connectivity, under Afilias' control, on all data centers by means of the redundant upstream connections that will become available. For example, a failure of the local data center IPv6 provider would not impact registry services, as IPv6 traffic would be re-routed automatically via providers from other data centers utilizing private circuits.

In accordance with Specification 6, 1.5, Afilias will:

- Accept IPv6 addresses as glue records in its registry system and publish them in the DNS;
- Offer public IPv6 transport for at least two of the registry's nameservers listed in the root zone with the corresponding IPv6 addresses registered with IANA;
- Follow "DNS IPv6 Transport Operational Guidelines" as described in BCP 91

and the recommendations and considerations described in RFC 4472;

- Offer public IPv6 transport for its Registration Data Publication Services as defined in Specification 4 of the new gTLD Agreement, e.g., WHOIS (RFC 3912), Web-based WHOIS;
- Offer public IPv6 transport for its SRS to any registrar, no later than six months after receiving the first request in writing from a gTLD accredited registrar willing to operate with the SRS over IPv6.

Afilias' registry systems support IPv6 and meet each of these requirements as part of the core registry offering.

#### Services provided over IPv6

All services, including EPP, Web Admin Tool (WAT), WHOIS, and DNS are provided on IPv6 for all 16 TLDs under management. All TLDs will have multiple native IPv6 subnets dedicated to DNS resolution. Each transit provider is required to carry IPv6 transport natively.

#### IPv6 provider connectivity and diversity

Afilias uses the following transit providers for IPv6:

- Hurricane Electric (AS6939)
- nLayer (AS4436)
- FLAG/Reliance Telecom (AS15412)
- Global Exchange (AS3549)
- NTT America (AS2914), Level3 (AS3356)
- DE-CIX (AS6695) & GLBX (AS3549)

#### IPv6 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 staff in a focused way. A total of 67 team members support this capability.

---

## 37. Data Backup Policies & Procedures: provide

- **details of frequency and procedures for backup of data,**
- **hardware, and systems used for backup**
- **data format,**
- **data backup features,**
- **backup testing procedures,**
- **procedures for retrieval of data/rebuild of database,**
- **storage controls and procedures, and**
- **resource plans (number and description of personnel roles allocated to this area).**



Answers for this question (#37) are provided by Afilias, the back-end provider of registry services for this TLD.

At Afilias, backups are made on an ongoing and regular basis, and periodically for regular quality assurance activities. All backups are run in parallel to the normal operation of the registry so there is no interruption to normal business. Proven backup procedures are seen in:

- A detailed and regularly executed plan for backups that include daily full backups which operate in tandem with registry operations;
- Twice yearly audits to test integrity of back-up files;
- A documented plan for data retrieval and restoration of systems in the event of failure, and;
- No less than annually tested plans for data retrieval and restoration of systems in the event of failure.

As an experienced registry services provider, Afilias provides the following capabilities:

- Complete disaster recovery procedures;
- Redundant systems;
- Backups and registry replication, and;
- Detailed procedures for planned and preventative maintenance.

Afilias' software is designed and the servers are selected in such a way that a complete failure or emergency should never happen. To offer additional insurance, however, and provide a detailed plan for backing up the system in the unlikely event of a failure, Afilias provides a comprehensive backup strategy to ensure continued operations.

Afilias takes all required measures to protect and secure customer data, financial data, and accounting data, as well as customer support information. The database is replicated in real-time on one or more replica servers so that in the event of failure of the master (primary) database server, registry operations can be restored by pointing to the replica (secondary) database server.

Procedures and frequency for backup of data

Afilias maintains geographically separated instances of the registry database to reduce the risk of data loss - a primary instance of the SRS and then a secondary/failover SRS in another location. These are described in earlier responses. The registry data is backed up on a continual ongoing basis from the primary to the secondary site. These instances are connected by private leased lines with failover to IPsec Virtual Private Network (VPN) connections to ensure that the stand-by site is always synchronized with the primary site.

In the event of a catastrophe in the first location, the second location will allow Afilias to continue to function with a minimum of disruption. The secondary location will mirror the primary, using a redundant VPN, to avoid the possibility of data loss. This is depicted in Figure 37-a.

Afilias conducts other routine backup procedures. These are performed in such a way as to not adversely impact any scheduled operations.

Normal backups allow retention of:

- Up to seven versions of database backup (flat file);
- Up to three versions of non-database changed files;
- Weekly full online backups of database files and off-site storage of one

weekly full database backup per month, and;

- Archival of database transaction logs once per day.

Zero-downtime, snapshot backups are performed daily. The backups are performed online as no special procedures are required to place the database in backup mode. The backups are managed by an enterprise-grade IBM Tivoli Storage Manager (TSM). They are made directly to the local redundant-fiber channel-attached Redundant Array of Independent Disks (RAID) at both the primary site and the disaster recovery location for quick restores, if needed, thereby helping to reduce recovery times in case of a disaster. Daily full snapshots are sent to an off-site location electronically, with another copy sent electronically to escrow to assist with recovery, if needed, in case of a catastrophe.

All backups are fully monitored and security is enforced on the entire backup infrastructure. Access permissions are audited at least twice a year. All backup, recovery (including regular recovery testing), monitoring and auditing procedures are documented and followed according to security best practices.

#### Backup hardware and systems

In the event of hardware failure, each data center maintains an inventory of key parts, and systems staff are trained to handle all operations needed to restore the failed machine safely and securely. The supplies are adequate to allow for multiple concurrent component failures. Additional preparedness comes from 24x7 telephone and on-site support from all software and hardware vendors. If replacement parts stock should become exhausted for some reason, additional parts are available within four hours of request.

Full, current copies of the database and operating system are kept in each of the data locations in use. They can be quickly retrieved, installed, and re-started if needed. It should be noted that all unnecessary services and processes are disabled, access is limited, and application of security-related patches to the operating system or critical system applications are regularly performed.

#### Data format

One type of data format used at Afilias is the standard Relational Database Management System (RDBMS) backup output file: Database Schema structure (tables' definitions), followed by their data.

The other type of data format is the RDBMS format which is used for the "master" database as well as the "replicas".

The data format relating to Point in Time Recovery (PITR) backup involves a semi-regular, disk level snapshot, to which a continuous stream of Write Ahead Log (WAL) segments is applied.

#### Data backup features for DNS and PostgreSQL utility

##### DNS backup

The "master location" for creation of DNS zones is within the registry systems. As such, when the registry is backed up, the information needed to re-create the zone is also securely stored. Each Afilias DNS node has several current "hot" copies of the zone, which can be retrieved at any time. In the event of an entire registry system failure, the Afilias DNS infrastructure would continue to answer DNS queries without performance degradation.

If an individual nameserver cluster should somehow corrupt a zone, that node can immediately be taken out of service. Once out of service, the node will have the entire zone removed, and the correct zone will be pushed from the registry or another node from scratch. Once verified, the node can return to service.

#### PostgreSQL backup utility

One type of database backup used at Afiliias is the PostgreSQL backup utility. This utility is automatically invoked daily, at 00:01 UTC. The output of the backup is then compressed and copied to another data center, and seven versions of it (one week) are maintained. The output is also encrypted and then submitted (electronically) as an escrow deposit.

Continuous replication of database transactions is another type of database backup employed at Afiliias. A set of databases is connected via replication software (Slony-I) and one of the databases is designated as the "update database", or the "master". The other databases are a copy of this one, and any update transaction is replicated to all of them. They are, therefore, exact copies of the "master", or "replicas".

Afiliias uses PostgreSQL's continuous PITR, commonly referred to as 'log shipping'. This highly reliable solution for disaster recovery supplements asynchronous replication (Slony-I). Whereas Slony represents an effective solution that guards against individual node failure, PITR effectively protects against the insertion of corrupted data into the DBMS. PITR allows for flexible crash recovery, i.e., to a particular point in time or DBMS checkpoint.

#### Backup testing procedures

All backup procedures are monitored and tested as are other registry systems. Please see our responses to questions #41 and #42 for details of the monitoring and planning. At Afiliias, backups are used on an ongoing basis during regular quality assurance activities. All backups are run in parallel to the normal operation of the registry so there is no interruption to normal business.

Twice a year, Afiliias performs an audit of backup documentation, retention policies and escrow deposits. This involves the Data Services team retrieving a sample of backups during a selected period from the escrow provider, then loading and validating the data.

#### Procedures for retrieval of data/rebuild of database

In the event the primary data server should fail, it would necessitate a brief interruption in service, while data processing was moved to the backup data server. This would be necessary to ensure high fidelity data integrity. Because the data servers use external RAID arrays, a failure of the primary server would not entail the loss of the data stored there; instead, the data could be moved quickly to the secondary server. Only in the case of a complete RAID array failure would any reconfiguration be necessary; and such an interruption would last only briefly, because the data would be replicated on another, identical array.

Restored data sets will be synchronized with the data escrow function to ensure that overlap of data storage exists. Registrar data escrows are not synchronized with registry data escrows. However, the failure of a registrar, with the attendant use of the registrar data escrow could result in a

reconciliation of the of the registrar's data set with the registry's should the failure of the registrar coincide with the restoration from backup of the registry data.

In the event of the total failure of the primary data center, registrars would be notified of the decision to move operations to the stand-by center. Except for the change in physical location, nothing would change in the manner of operation.

#### Storage controls and procedures

Regular reports are generated for registrars and for internal administrative purposes. Reports are available for online retrieval via an encrypted Web interface in an uncompressed format for a two year period. After two years, reports are expunged.

#### Resourcing plans

With respect to hardware, the same type of computers and disk arrays that are used to run the registry (including both the "master" database and all the "replicas") are also used to run the databases' backups and to store the output files. Also, the same type of computers and disk arrays are used in the secondary data center for copying and storing copies of the backup files. For a detailed list of hardware and software components, please see our response to question #32.

Since its founding, Afiliias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afiliias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afiliias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afiliias project management methodology allows efficient and effective use of staff in a focused way.

In terms of staff resources, 61 team members at Afiliias have knowledge of and contribute to successful backups of the registry. This includes a team of nine Database Administrators (DBA) who manage all databases, and one of their responsibilities is backup management. Additionally, Afiliias has five Systems Engineers trained in backup procedures; they support backup administration and are also responsible for daily monitoring of backup logs to ensure any errors are caught in a timely manner. If required, errors causing backups to be missed or incomplete are fixed and run again.

---

### **38. Escrow: describe how the applicant will comply with the escrow arrangements documented in the Registry Data Escrow Specifications (Specification 2 of the Registry Agreement). Describe resourcing plans (including number and description of personnel roles allocated to this area).**

Answers for this question (#38) are provided by Afiliias, the back-end provider of registry services for this TLD.

Afiliias currently performs daily data escrow with an established escrow agent in compliance with existing ICANN registry agreements. This process will be

updated to comply with processes and procedures defined in Specification 2 of the new gTLD Agreement. Afilias' commitment to data security and integrity is seen in:

- Comprehensive data backups which are produced each day and are tightly managed under current escrow and insurance arrangements with reputable companies, with escrow testing twice annually, and;
- Integrating this TLD into Afilias' proven backup and escrow plans in accordance with Specification 2 of the new gTLD Agreement.

For more detail on the escrow file creation procedure, please see the backup process definition in our response to question #37, and specifically Figure 37-a for an explanation of the handoff to an escrow provider. Rather than performing escrow services itself, Afilias has historically deposited data with respected international firms with core expertise in data escrow and storage services. The escrow provider for the new TLD will be selected by the registry operator and Afilias, taking ICANN requirements into consideration.

#### Specification 2 compliance

The registry operator and Afilias will conform to all requirements for the technical specifications of escrow defined in Specification 2, including:

##### 1. Creating and making "full" and "differential" deposits.

- Afilias will ensure that both full and differential deposits are made to the escrow provider chosen by the registry operator. These deposits will include all registry objects needed to offer all of the approved registry services.
- Full deposits will reflect the state of the registry as of 00:00:00 UTC on each Sunday (excluding all transactions that have not yet been committed).
- Differential deposits will include all transactions that were not reflected in the most recent full or differential deposit. Differential deposits will be made as of 00:00:00 UTC of each day (which will exclude Sundays).

##### 2. Following the defined schedule for daily differential and weekly full deposits.

- Afilias will make escrow deposits on a daily basis per the requirements in Specification 2.
- Full deposits will reflect the state of the registry as of 00:00:00 UTC on each Sunday (excluding all transactions that have not yet been committed). The full deposits will be submitted to the Escrow provider no later than 23:59:00 UTC each Sunday.
- Differential deposits will include all transactions that were not reflected in the most recent full or differential deposit. Differential deposits will be made as of 00:00:00 UTC of each day (which will exclude Sundays). Differential deposits will be made no later than 23:59:00 each day.

##### 3. Creating escrow deposits in the defined format.

- Afilias will submit all escrow deposits in a file constructed as described in the IETF draft-arias-noguchi-registry-data-escrow. Although this draft describes some elements as optional, Afilias will include those elements in the deposit if they are available. Further, once the specification is published as an RFC, Afilias will implement to that specification no later than 180 days after.
- Afilias will use UTF-8 character encoding.
- If there are additional registry services offered, Afilias will include that data as well (plus any relevant "extension schemas" required).

##### 4. Processing the deposits with consideration to using file compression,

encryption, digital signatures, secure electronic transfer to the escrow agent, and obtaining confirmation of receipt.

- Afiliias will compress files using ZIP as per RFC 4880. Data will be encrypted using the escrow provider's public key. If necessary, files will be split to accommodate the escrow provider's maximum file size limitations.
- A digital signature file will be generated for every processed file using the registry's private key, in binary OpenPGP format as per RFC 4880. Digital signature files will not be compressed or encrypted.
- All fields will be transmitted to the escrow provider through secure electronic mechanisms such as SFTP, SCP, or HTTPS file upload, as agreed between the registry operator and the escrow provider.
- Afiliias will require a confirmation from the escrow provider for each deposit made.

5. Use specified file naming conventions.

- Afiliias will use the specified naming convention for each and every deposit, specifically: {gTLD}\_{YYYY-MM-DD}\_{type}\_S{#}\_R{rev}.{ext}.

6. Distribute public keys to appropriate parties.

- Afiliias (acting for the registry operator) and the escrow provider will distribute its public key to the other party via email to an email address agreed between the parties.
- Each party will confirm receipt of the other's key via email and will subsequently confirm the authenticity of the transmitted key via offline methods such as a phone call, in-person meeting, or other method.
- The escrow provider, Afiliias (for the registry operator) and ICANN will all exchange keys by the same method.

7. Provide ICANN notification of the escrow deposit, and;

- With each delivery of a deposit, Afiliias (for the registry operator) will deliver to the escrow provider and to ICANN a written statement (which may be via authenticated email) that includes a copy of the report generated upon creation of the deposit and states that the deposit has been inspected by the registry operator and is complete and accurate.
- The statement will include the deposit's "ID" and "resend" attributes.

8. Perform verification measures to ensure the file is formatted correctly and accessible through the encryption methods utilized.

- Upon completion of the deposit, Afiliias will validate the signature of each processed file, combine files if they were split for transmission, decrypt and uncompress each file, validate each file against the defined format, and verify the data.
- If any discrepancies are found, the deposit will be considered incomplete.

#### Legal requirements

The registry operator will conform to the legal requirements defined in Specification 2, including entering into a legal agreement with an escrow agent (see below for more detail), paying all appropriate fees related to data escrow, agreeing to ownership provisions, and holding the escrow agent to high standards of integrity to ensure confidentiality.

#### Escrow arrangements

The full and differential backups will be deposited with Iron Mountain, NCC, or a similar vendor of similar quality selected upon approval of the TLD. The files are encrypted using OpenPGP as documented in RFC 2440 and sent to the secure servers of the escrow agent. The agent will use internally secure methods to ensure the integrity of all deposits.

As noted above, the full structure, naming conventions, formats and encryption will be consistent with Specification 2 of the new gTLD Agreement.

Non-database servers are also backed up daily, and seven versions are maintained of all active files. One backup per week goes to the off-site facility and is recycled when the local copies expire. If a file were to be deleted, all versions would be stored for 60 days; the newest version would be kept for a total of 90 days.

#### Insurance arrangements

To support this TLD, Afilias will employ similar provisions to those included in the .ORG and .INFO gTLD agreement with ICANN. Specifically, the escrow agent will be requested to indemnify Afilias and the registry operator from and against any and all claims, actions, damages, suits, liabilities, obligations, costs, fees, charges, and any other expenses whatsoever, including reasonable attorney's fees and costs, that may be asserted by a third party against any indemnity in connection with the misrepresentation, negligence, or misconduct of the escrow agent.

#### 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 staff in a focused way.

Afilias utilizes an automated process for data escrow and requires minimal resources to add this new TLD. The team attributed to supporting the escrow activities at Afilias includes 25 team members. Existing Database team members will make the appropriate file structure and naming conventions for this TLD; they will be responsible for development and testing prior to launch. The escrow process will be integrated into the monitoring systems and tracked by existing Afilias NOC team members. The Database Administrators and NOC monitor the escrow process and any issues are escalated to the database team for resolution.

---

**39. Registry Continuity: describe how the applicant will comply with registry continuity obligations as described in the Registry Interoperability, Continuity and Performance Specification (Specification 6), attached to the draft Registry Agreement. This includes conducting registry operations using diverse, redundant servers to ensure continued operation of critical functions in the case of technical failure. Describe resourcing plans (number and description of personnel roles allocated to this area).**

Answers for this question (#39) are provided by both Afilias, the back-end provider of registry services for this TLD and Nameshop.

Registry operations are assured continuity through redundancy at all layers of registry operation. Systems are engineered to avoid any single point of failure. This response covers:

- The risks and threats to registry continuity and summarizes mitigation efforts such as high availability and scalability;
- Determination of critical functions, Recovery Point Objectives, and Recovery Time Objectives;
- Compliance with ICANN Specification 6, and;
- The numerous steps Afilias takes to ensure continuity, including a hot stand-by site.

Afilias has incorporated an industry best practices approach (ITIL, ITSM, and COBIT) into its business, technology and processes to ensure proper continuity.

Registry failure can be separated into two major categories. First is a catastrophic failure of the registry, in which the updates of names in DNS may fail and the shared registry system is unavailable (i.e., it is impossible to add or modify names in the registry). Afilias classifies these incidents as "Complete Failures." The primary response to mitigate a catastrophic failure is to sufficiently provision registry systems and ensure diversity at each layer in a geographically diverse manner. Afilias has executed such a strategy.

The second category consists of partial failure of a registry system, prioritized in the order provided below. Afilias classifies these incidents as "Emergencies":

- Failure of the registry to serve already registered names, while other components of the registry system continue to work normally, or
- Failure of the registry to register new names or update information about existing names, while there are no ill effects on propagation or resolution of names or other registry system components, or
- Unauthorized access or exposure of sensitive registry data.

Risks and threats to registry continuity

The following list captures the various risks and threats that have the potential of disrupting the operational infrastructure of Afilias' registry system.

#### 1. Facilities Security

Function: Data Centers host all registry systems

Threat types: Physical breach, network breach, power interruption, communications loss

#### 2. Registry systems

Function: Domain management, including updates and transfers

Threat types: Data corruption, data disparity between registry systems, unauthorized domain data access, registrar data compromised

#### 3. DNS

Function: Zone generation, publication and distribution

Threat types: DDoS attacks, zero-ready exploits, man-in-the-middle attacks

#### 4. Support infrastructure

Function: VPN connections, leased lines, remote access

Threat types: Unauthorized access, virus penetration



#### 5. Connectivity/Internet Services

Function: Communications

Threat types: Loss of connectivity, inadequate bandwidth

#### 6. Organizational Security

Function: Staff integrity, asset control

Threat types: Nefarious actors gaining access, asset loss

#### 7. Outage Prevention

Function: All registry components

Threat types: Loss of system functionality, disaster (earthquake, fire, flood, terrorism)

#### 8. Human Resources

Function: All staff members

Threat types: Unavailability of human resources due to disaster, unfit working environment (mold, flooding, utility outages, gas leaks)

More detailed discussion of the threat mitigation for the above is presented in our response to question #30b.

#### Experience analyzing risk

Afilias has extensive experience in technology risk assessment and threat mitigation. In fact, Afilias' work specific to DNS risk analysis was recognized by the US Department of Homeland Security for our leadership and contributions to the Information Technology Sector Baseline Risk Assessment.

(Please see

[http://www.dhs.gov/xlibrary/assets/nipp\\_it\\_baseline\\_risk\\_assessment.pdf](http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf)).

Afilias continues its efforts in this on-going process.

#### Critical functions determination

Functions that are critical to the operation of a gTLD registry include:

1. DNS resolution for registered domain names
2. Operation of the SRS
3. Provision of WHOIS service
4. Registry data escrow deposits
5. Maintenance of a properly signed zone
6. DNSSEC Keys

#### Recovery point objectives

The recovery point objective ("RPO") for the registry is within one minute of the loss of the original database. There are various methodologies available to recover both within and between data centers. One is Slony, which is described in detail in our responses to questions #31 through #33. The other is storage-based replication. Both options ensure zero data loss (except in the case of severe catastrophe) and application consistent recovery. Both of these options allow failover testing without impacting the production systems.

Details are below on synchronization timing of various event types. The most likely RPO scenario is 0-2 seconds for intra-data center disruptions, and 2-10 seconds for inter-data center disruptions.

#### Testing and planning

Afilias annually tests systems and disaster plans. For a complete plan, please see our response to question #41.

#### Core success factors

The Afiliias Registry continuity program is four-dimensional, to ensure success:

1. People (Organization, Roles, Skill-sets, Training)
2. Process (Business Operations; Engineering, Production, HR, IT)
3. Technology (Infrastructure, Applications, Tools)
4. Financial (Budget, TCO, ROI, Risk Management)

#### Continuity plan compliance

As described in our responses to questions #37 and #38, all critical registry services data and relevant support systems data are subject to regularly scheduled backup processes and stored with a third-party reputable escrow agent. In the highly unlikely event of a complete failure, Afiliias will act in conjunction with ICANN's gTLD Registry Continuity plan in following the measures:

- Information Sharing;
- Situation Handling and Event Management: all incidents will be handled according to detailed incident management processes (see our response to question #35) that are consistent with ICANN's high-level plan;
- Coordinate with ICANN's Crisis Response Team;
- Openly communicate with ICANN on the nature and status of an event;
- Take all measures to assure business continuity;
- Assist ICANN in invoking Data Security & Data Escrow agreements;
- Cooperate with the transition of the TLD (more information in our response to question #40), and;
- Regularly test and modify the Continuity Plan as required.

Nameshop will also cooperate with ICANN on Continuity Plan Compliance.

#### High availability

Registry services are delivered from a platform comprised of multiple redundant systems. All network equipment (routers, firewalls, switches, rate-limiters, load-balancers) and application and database servers are connected in a multi-path configuration to a pair of core network switches. Care is taken to ensure that if any one component fails, a network path remains available through the standby unit. Similarly, availability of data path is also ensured through the use of redundant fiber-channel host adapters, SAN switches, and storage controllers.

Critical registry functions of EPP and WHOIS are delivered from multiple application servers that sit behind a pair of redundant load-balancers.

Registry traffic is balanced between application servers so that the load is distributed evenly among multiple servers. In the event of a server failure, load-balancers detect that the server is unreachable and route traffic to the remaining available servers, preventing major (or even discernable) disruption to the system.

All registry data is stored on highly redundant disk array systems in RAID 10 configuration. Disk array subsystems include multiple controller mechanisms and redundant power and fiber channel connections.

The registry database is replicated in near real-time to multiple subscribed database copies within a single data center. Each of these subscribed database copies is served by a separate database backend, running on a separate physical server and stored on a separate disk array subsystem.

Performance of these databases is constantly monitored.

In the event of a database server failure, a high availability feature will move the impacted resources automatically to available redundant hardware. If this scenario is executed successfully, then disruption to the registry (the RTO) will be no longer than five minutes and as there will be no data lost when service is restored (the RPO).

In addition to in-site replication of data, database replication also occurs to multiple remote-site database copies.

#### Extraordinary event continuity management

Due to the steps taken to ensure high availability within a data center, registry disruptions are rare. Minor events are rapidly recovered from with no performance degradation. To ensure registry availability if an extraordinary event should occur which results in the extended loss of an entire operating environment, a mirror, hot-standby registry environment is operated. Multiple databases in a secondary data center, built according to the same design specifications, are replicas of the original database in the primary data center.

If it is determined that the primary data center will be unavailable for an extended period, disaster recovery plans are enacted. One of the replicated databases in the remote data center will be converted to become the new master database.

Application servers in this standby data center which have been configured in advance to point to the new master will be activated, and following some brief readiness tests, IP addresses which serve the registry from the primary data center will be migrated to the standby data center, making it active.

Replication to databases in remote data centers is monitored closely and typically lags by two to 10 seconds behind the master. In the event that disaster recovery efforts need to occur, the RPO is to within two minutes of the loss of the master database.

The disaster recovery plan is tested at least annually, and has an RTO of no more than four hours. In testing, execution of the plan is consistently completed within 30 minutes. More details can be found in our response to question #41.

#### Hot backup/secondary center

Primary registry functions are run out of all data centers, which is to say Afiliias does not have a discreet facility as primary and another discreet facility considered as a secondary. Afiliias TLDs are dispersed to avoid a single point of failure from a discreet location, thereby creating an architecture with multiple live environments, or "hot standby," available from every data center. For example, the .INFO primary is in location A and its secondary in location B, while the .MOBI primary is in location B and its secondary in location A. Thus, a complete "hot backup" of the registry is available in a "secondary" data center. Annual testing at Afiliias has shown transition to the "secondary" data center can be achieved within 30 minutes.

#### Relationship continuity

Nameshop is responsible for relationships with ICANN, registrars and any vendors (e.g., escrow provider) and will take all appropriate steps to maintaining those contractual relationships.

#### Data continuity

Afilias permanently maintains all raw transactional details in a data warehouse. The raw EPP transaction detail (XML data) is continually captured from the EPP servers, stored in a database, and backed up nightly. EPP commands that write to the database (creates, deletes, updates, etc.) are maintained in the warehouse database on a permanent basis and are available to the registry operator for online historical queries, auditing, and troubleshooting of registrar issues.

#### Human resource continuity

Plans to address human resource continuity include geographic diversity:

- Afilias has technical staff located in Toronto, Canada; Horsham, Pennsylvania, USA; Dublin, Ireland; and New Delhi, India.
- Afilias has fully operational customer service groups located in Toronto and New Delhi.
- Afilias has fully operational NOCs located in Toronto and Horsham. Each center is fully capable of autonomous operation in the event the other facility is offline.
- All technical staff have the ability to work remotely via high-speed virtual private network (VPN) connections in situations where they are unable to physically work in offices due to events such as disease, flooding, etc.

Nameshop will manage this TLD with the available staff resources of Afilias and hiring the required staff resources where necessary with human resources policies and procedures with respect to personnel management.

#### Business continuity

In the event of a catastrophic event which results in the simultaneous loss of both the primary and secondary production data centers, restoration of registry data and configuration will be recovered from nightly backups sent off-site in escrow to the escrow agent.

Nameshop will manage this TLD with as an integrated part of our company and consistent with corporate policies and planning for business continuity.

#### Customer ticketing and contact data continuity

Afilias' CRM provider, Salesforce.com®, understands that the confidentiality, integrity, and availability of Afilias customers' information are vital to business operations. Salesforce.com® uses a multi-layered approach to protect that key information, constantly monitoring and improving their application, systems, and processes to meet the growing demands and challenges of security.

#### Secure data centers

The service is collocated in dedicated spaces at top-tier data centers. These facilities provide carrier-level support, including:

##### Access control and physical security

- 24-hour manned security, including foot patrols and perimeter inspections
- Biometric scanning for access
- Dedicated concrete-walled Data Center rooms
- Computing equipment in access-controlled steel cages
- Video surveillance throughout facility and perimeter
- Building engineered for local seismic, storm, and flood risks

- Tracking of asset removal

#### Environmental controls

- Humidity and temperature control
- Redundant (N+1) cooling system

#### Power

- Underground utility power feed
- Redundant (N+1) CPS/UPS systems
- Redundant power distribution units (PDUs)
- Redundant (N+1) diesel generators with on-site diesel fuel storage

#### Network

- Concrete vaults for fiber entry
- Redundant internal networks
- Network neutral; connects to all major carriers and located near major Internet hubs
- High bandwidth capacity

#### Fire detection and suppression

- VESDA (very early smoke detection apparatus)
- Dual-alarmed, dual-interlock, multi-zone, pre-action dry pipe water-based fire suppression

#### Secure transmission and sessions

- Connection to the Salesforce environment is via SSL 3.0/TLS 1.0 ensuring that users have a secure connection from their browsers to the service
- Individual user sessions are identified and re-verified with each transaction, using a unique token created at login

#### Network protection

- Perimeter firewalls and edge routers block unused protocols
- Internal firewalls segregate traffic between the application and database tiers
- Intrusion detection sensors throughout the internal network report events to a security event management system for logging, alerts, and reports
- A third-party service provider continuously scans the network externally and alerts changes in baseline configuration

#### Disaster Recovery

- Afiliias' CRM provider performs real-time replication to disk at each data center, and near real-time data replication between the production data center and the disaster recovery center
- Data are transmitted across encrypted links.
- Disaster recovery tests verify the service providers projected recovery times and the integrity of our customer data

#### Backups

- All data are backed up to tape at each data center, on a rotating schedule of incremental and full backups.
- The backups are cloned over secure links to a secure tape archive.
- Tapes are not transported offsite and are securely destroyed when retired.

#### Internal and third-party testing and assessments

Salesforce.com® tests all code for security vulnerabilities before release, and regularly scans the network and systems for vulnerabilities. Third-party assessments are also conducted regularly:

- Application vulnerability threat assessments
- Network vulnerability threat assessments
- Selected penetration testing and code review
- Security control framework review and testing

#### Security monitoring

The Information Security department monitors notification from various sources and alerts from internal systems to identify and manage threats.

#### Proactive defenses to maintain registry continuity

Each of these measures mitigates the risk of failure and ensures registry continuity by Afiliias:

- Diversity. Operating from a geographical diverse network, with multiple providers at each location, and multiple hardware and software selections throughout the entire infrastructure.
- Efficiency. Afiliias operates a state-of-the-art, EPP-based SRS that is reliable, efficient and secure. The entire registry infrastructure is based on open standards and interoperability.
- Availability. A fast, secure, reliable DNS system to enable domains to resolve in near real-time, worldwide - 100% of the time. Afiliias has been managing stringent SLAs from inception for all registry systems.
- Redundancy. Afiliias introduces redundancy and diversity into its hardware, software, systems, communications and utilities to ensure no single point of failure exists anywhere in the infrastructure.
- Scalability. A proven architecture design and team that has scaled to over 20 million domains, 207 million contacts, 6 million hosts, and query volume exceeding 20 million daily queries.
- Monitoring and incident resolution. Afiliias has extensive 24x7 monitoring, defined incident management, escalation and communication procedures. Details on each are found throughout this application.
- Restoration commitment. In the event of an issue, Afiliias will use commercially reasonable efforts to restore the critical functions of the registry as quickly as possible. Restoration work will commence within 24 hours after the termination of an extraordinary event beyond the control of the registry operator, with full system functionality restored within a maximum of 48 hours following such event.
- Maintain a business continuity plan. See below for more information.
- Testing. Afiliias audits its procedures regularly and agrees to conduct Registry Services continuity testing at least once per year.
- Accessibility. Afiliias will make public on its website and supply to ICANN accurate contact details including a valid e-mail and mailing address as well as a primary contact for handling inquiries related to malicious conduct in the TLD, and will provide ICANN with prompt notice of any changes to such contact details.

For more information on Afiliias' provisions for registry failure, please see our response to question #41.

#### Mitigating financial risk

Afiliias' activities expose it to a variety of financial risks: currency risk, credit risk and liquidity risk.

Afiliias' overall risk management program focuses on the unpredictability of financial markets and seeks to minimize potential adverse effects on the company's financial performance.

Risk management is carried out under policies approved by the board of

directors. Afiliias' treasury identifies and evaluates financial risks in close co-operation with the company's operating units. The board provides principles for overall risk management, as well as policies covering specific areas, such as foreign exchange risk, interest rate risk, and credit risk, use of derivative financial instruments and non - derivative financial instruments, and investment of excess liquidity.

#### Market risk

- Foreign exchange risk: Most of Afiliias' purchases and sales are denominated in U.S. dollars thereby reducing the company's exposure to foreign exchange risks. The company does have some exposure to foreign exchange risks as it relates to payroll, office rent and general and administrative purchases made in Euros, Canadian dollars, and to a lesser extent Indian Rupees. However, given the size of Afiliias' operations conducted in foreign currencies, the costs of managing exposure to foreign exchange risks exceed any potential benefits. The directors will revisit the appropriateness of this policy should the company's non-U.S. dollar payroll and purchases change in size or nature.
- Cash flow and fair value interest rate risk: Afiliias has no significant interest-bearing assets. Therefore, the company's income and operating cash flows are substantially independent of changes in market interest rates.

#### Credit risk

- To mitigate credit risk, Afiliias' policy requires registrars to post cash funds or an irrevocable letter of credit in order to establish a line of credit against which the registration fees are charged at the time domain names are registered. The company has had minimal bad debt write-offs since its inception.
- Financial instruments that subject Afiliias to concentrations of credit risk consist principally of cash on deposit. The company maintains cash balances with financial institutions which at times exceed the insured amounts. Afiliias monitors the credit quality of these financial institutions.

#### Liquidity risk

Afiliias has sufficient funds available for operations and planned capital expenditures. Accordingly, Afiliias does not have any outstanding short-term debt financing, nor does it use derivative financial instruments.

#### Capital risk management

Afiliias' objectives when managing capital are to safeguard its ability to continue as a going concern in order to maintain an optimal capital structure to reduce the cost of capital.

Applicant has limited capital risk associate with managing this TLD. All risks are identified and planned according to responses to questions #48, #49, and #50.

#### Resources

Since its founding, Afiliias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afiliias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afiliias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afiliias project management methodology

allows efficient and effective use of staff in a focused way. 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 staff in a focused way.

Afilias has 40 operational staff involved in compliance with registry continuity obligations as described herein. As noted, Afilias is highly focused on not just registry continuity, but the success - high availability, quality domain services - of all its TLDs. All resources are available on an as-needed basis. The continuity plan is maintained by the Technology Department and receives direct input from both the Security and Resolution Services teams within Afilias and reviewed on a regular basis. Please see our response to question #31 for the organization overview.

With such resources from Afilias it may not require additional resources for contingency management; these functions are a part of the on-going management of this TLD, competently handled by Afilias. However, Nameshop, in the process of building up its Registry operations, would gradually build a team with the required competence to efficiently coordinate with Afilias, make periodic financial allocations to a reserve for funding continuity, over and above the conditions stipulated by ICANN; This Nameshop will do as the Registry operations grow beyond the initial projections submitted at this application stage.

---

#### **40. Registry Transition: provide a plan that could be followed in the event that it becomes necessary to transition the proposed gTLD to a new operator, including a transition process.**

Nameshop as the Registry Operator and Afilias, the registry backend service provider, are prepared to cooperate with a successor registry operator as directed by ICANN with respect to the assignment of Registry-Registrar Agreements between the registry operator and entities that are accredited as registrars for the gTLD registry; including executing appropriate assignment documents and delivering such agreements to the successor registry operator.

The descriptions below are based on actual experience transitioning .ORG and other gTLDs, both to Afilias' systems (the registry backend service provider) from legacy providers, and from Afilias' systems to another provider. Afilias operates standards-compliant systems and has the experience needed to ensure safe, stable transitions when necessary.

##### Experience with gTLD migrations

In January 2003, Afilias, in coordination with the Public Interest Registry (PIR assumed responsibility for operating .ORG and maintaining the authoritative database of all .ORG domain names. The transition of .ORG from the previous operator (VeriSign) is the largest real-time registry transition in Internet history. More than 2.6 million domains were transferred in less than 24 hours, without affecting any .ORG registrants or websites. The migration was further challenged by a complete registry protocol change from Registry Registrar Protocol (RRP) to Extensible Provisioning Protocol (EPP) - a completely new interface for many .ORG registrars - and registration data storage change from a "thin" model to a "thick" model, involving over 135 registrars both located in the U.S. and in International



locations. Not only were the technical challenges met with unparalleled success but also billing continuity was met for registrations including credits for representing deletes within the applicable grace periods involved as part of the transition of financial records. Customer deposits for funding were also transitioned from VeriSign to PIR during the transition period.

Afilias also had experience with conducting another migration in 2004. They created a continuity and migration plan for the National Internet eXchange of India (NIXI) and Government of India, and successfully migrated the .IN registry from its legacy registry operator with no interruption in DNS service and minimal interruption in other registry services. During the migration, Afilias also corrected many problems with the registry's data and brought existing and new registrars onto EPP. At various times Afilias has migrated many ccTLDs onto its systems from other providers, including: .AG (Antigua and Barbuda), .BZ (Belize), .GI (Gibraltar), .HN (Honduras), .MN (Mongolia), .SC (The Seychelles), and .LC (St. Lucia). All of these transitions included the onboarding and migration of registrars, the transition of registry databases from legacy operators to Afilias systems, IANA record updates, and transitioning DNS service in an uninterrupted fashion.

Migrating a registry from one provider to another entails great risk. Any potential registry service provider should provide a complete migration/transition plan that includes detailed plans with the following elements:

- Demonstrated ability to migrate a gTLD, regardless of its size;
  - How a migration from the old system to the new system can be accomplished with a registry outage of less than eight (8) hours, with no interruption to DNS (resolution) services;
  - A plan for DNS migration and continuity, including a rollover of all DNSSEC keys;
  - A detailed project plan for the migration itself;
  - Plans to migrate registrars to the new system with minimal disruption;
  - Continuity of daily registry operations while the transition is in progress; and,
- Fallback and contingency plans.

Registry transition with a named successor

The following procedure would be followed in the event that ICANN should require the handover of the registry to a named successor. Afilias will ensure such a transfer will occur in a timely fashion.

The complete list of steps and participants are defined below.

Transition planning steps, participants and monitoring

The steps of the transition of permanent operation will cover all of the critical functions of the registry. The transition is presented in the following phases:

Phase 1: Kick-off and communication

Phase 2: DNS

Phase 3: SRS/registry data

Phase 4: WHOIS

Phase 5: Data security & Escrow

Phase 6: Customer migration

Phase 7: IDNs

Phase 8: DNSSEC

## Phase 9: Custom Features and Policies

The technical transition will involve a multi-step procedure, outlined in detail below. The activities in Phases 2-8, though separately categorized, are not sequentially conducted, i.e., the timing of these tasks may overlap. During this period, both Afilias and the new registry operator can monitor services and, where noted, specific steps have been identified for confirming accuracy of data and security.

### Phase 1: Kick-off and communication

The transition will kick-off with an initial Transition Process Meeting between Nameshop, Afilias and the new registry operator. Representatives from each company will be present in the areas of DNS, WHOIS, database administration (for field types and values), customer support, technical support, and policy/compliance. In this phase, the team members meet their functional counterparts and define the specific schedules and technical facets, using the details herein as the initial project plan. The teams mutually detail the timeline with a goal to provide seamless continuity of service to ICANN and registrars in all areas possible.

The teams will also define internal and external communication plans to ensure relevant details are publicly available, and ICANN is fully apprised of all activities. Additionally, primary points of contact will be assigned for ICANN and registrars; these individuals and their respective contact information will be made available to all relevant parties.

Registrars will have detailed communication on the transition and the Operational Test & Evaluation (OT&E) environment being provided by the new registry operator. The communication plan will include two to three outreach meetings to registrars to ensure they have relevant information about the schedule and opportunities for Q&A.

The estimated duration of Phase 1 is 14 to 21 days.

### Phase 2: DNS

The DNS is the most critical component of the registry system. This plan ensures that the transition from Afilias' nameservers to the new registry operator nameservers will be smooth and seamless to the Internet community.

The procedures are as follows:

Afilias establishes a secure methodology with the new registry operator for transporting sensitive data. This may be as simple as PGP-encrypted email, Secure Copy Protocol (SCP), or other similar mechanisms. Afilias securely sends a zone file to the new registry operator who tests the file integrity and syntax. The new registry operator provisions the domain's zone on an appropriate set of primary nameservers. The new registry operator loads the zone file onto the primary nameservers and tests the distribution of the zone throughout the remainder of their infrastructure. At this point, the zone is not publicly accessible from the new registry operator's nameservers. The next portion of the transition depends on the technical capabilities of the new registry operator. Afilias offers two different mechanisms for transporting the zone between the two organizations during the cut-over:

If the new registry operator supports AXFR/IXFR:

- i. Afilias generates a unique set of TSIG keys. These keys are securely sent to the new registry operator with the additional configuration information necessary to ensure the new registry operator's primary nameservers can execute an AXFR/IXFR zone transfer from Afilias. The new registry operator

securely sends Afiliás the configuration information necessary to ensure that Afiliás can automatically notify the new registry operator's primary nameservers when a zone update is available. Each party makes applicable changes to their firewalls and other security components to ensure both sets of nameservers can communicate as needed. Afiliás adds the new registry operator's primary nameservers to its configuration to receive AXFR/IXFR zone transfers. Note that the new registry operator's nameservers will NOT yet be publicly accessible. Afiliás verifies that both AXFR and IXFR transfers are occurring on a regular basis.

ii. If the new registry operator does NOT support AXFR/IXFR: Afiliás sets up an SCP server for the new registry operator to periodically pickup zone files (along with an integrity check, e.g., an MD5 checksum). Appropriate firewall and other security component rules are changed to allow the new registry operator access. Afiliás generates keys on the systems that will access this SCP server, and delivers them to the new registry operator in a secure manner. The new registry operator will also send a list of IP addresses that will be accessing this SCP server. Afiliás submits a new zone file to the SCP server no less than once every 30 minutes. The new registry operator sets up internal systems to retrieve the zone file, check the file integrity, and load it onto the new registry operator's primary nameservers. Note that the new registry operator's nameservers will NOT yet be publicly accessible.

iii. The following applies regardless of AXFR/IXFR support: Afiliás' Network Operations Center and the new registry operator set up monitoring systems to check that zone files are correctly being updated and loaded at all times. One week prior to the registry cut-over, Afiliás adds the new registry operator's nameservers to the domain's zone file. This is done in advance to reduce the number of changing systems during this period of flux. If the new registry operator supports AXFR/IXFR: During the registry cut-over, Afiliás and the new registry operator switch roles. Afiliás changes its nameserver configuration to receive zone file transfers from the new registry operator and the new registry operator changes their nameserver configuration to send zone transfers to Afiliás.

iv. Afiliás begins transferring the zone and notifies the new registry operator when they are correctly receiving a zone file.

If successor registry operator does NOT support AXFR/IXFR: During the registry cut-over, Afiliás and the new registry operator switch roles. The new registry operator submits a zone file to the SCP server, using the same file name pattern as before (along with an integrity check, e.g., an MD5 checksum). Afiliás must pick up the file regularly check the file integrity and ensure that it is successfully loaded onto the nameservers each time.

Afiliás and the new registry operator monitor SOA resource record serial numbers for "drift" - if the Afiliás nameservers fall behind, Afiliás Technical Support immediately contacts the new registry operator to diagnose the problem and correct it.

i. Just after the registry cut-over, the new registry operator crafts an IANA TLD change request that adds its servers into the domain's delegation in the root zone. Note that this still contains Afiliás' servers to ensure stability of the zone (since caching resolvers will continue to have the Afiliás servers in their cache). When the IANA TLD change request completes the new registry operator's nameservers will be publicly accessible.

ii. One month after the cut-over, the new registry operator crafts another IANA TLD change request. This request removes Afiliás' nameservers from the domain's delegation in the root zone.

iii. One week after confirmation that this has been completed, the new registry operator removes Afiliás' nameservers from the domain's zone file.

iv. One week after this step, Afiliás removes the domain's zone from their nameservers.

v. The new registry operator stops the distribution of the zone file to Afiliias and both parties remove the firewall and other security component rules that permitted each other access to the zone file.  
The estimated duration of Phase 2 is 90 days.

#### Phase 3: SRS/registry data

To transition the registry data, the new registry operator must map the registry data onto its systems and perform Quality Assurance testing before restoring full functionality to registrars. The procedure is as follows: Set up an initial meeting between the new registry operator's and Afiliias' database teams. This meeting will determine what information will be available, as well as the data formats, and the processes to be used to exchange data securely (such as the SCP server described in the DNS transition). There will be five core registry data components that will need to be captured during this process: domain data objects, contact data objects, host data objects, object statuses, and restricted domain names. Restricted domain names are domain names that are restricted/reserved by ICANN and/or the registry operator, and can also comprised of IDN variants (please see Phase 7 for more details on IDN variants). Afiliias supports the new registry operator's efforts to begin the process for mapping all relevant data into its registry systems. As the data is mapped onto the new registry operator's systems, Afiliias provides data dumps to the new registry operator so they may test the conversion process and ensure that the mapping is correct. Corresponding zone files are also sent to ensure that data correctly maps to what is expected in the zone. Afiliias can provide a data request document which details what data is expected, and in which format. Clarification meetings (via phone or in person) may be required from time to time to resolve problems incurred during the mapping process. This works toward a finalized data request document. If any data is required that is currently out-of-band for the new registry operators EPP servers, the new registry operator determines whether to build an EPP extension or to continue to run an out-of-band service. At the cut-over onset, Afiliias disallows registrar access to the registry. They then begin to generate the data dump as specified in the data request document. Once this data has been generated, Afiliias securely sends the data to the new registry operator and informs them when the transfer has been completed. The new registry operator then loads this data into the registry, and produces a zone file for comparison. Once the data has been verified, the new registry operator pushes the zone out to its nameservers (see the DNS transition for more details). Registrar access to the new registry operator's registry is allowed. All available registrar and registry operator reports will be compressed and securely transferred to the new registry operator. During this phase, Afiliias will also work with the new registry operator to determine the feasibility of importing trouble tickets and or customer problem resolution mechanisms into its systems. If the systems can be mapped, Afiliias will provide periodic data dumps of unresolved tickets to the new registry operator ensure any known issues are tracked. If there is no practical way to import this data, Afiliias will provide the new registry operator with a current list of unresolved issues so they may be entered manually in the new registry operator's system.

The estimated duration of Phase 3 is four to six weeks.

#### Phase 4: WHOIS

Because of the nature of EPP and WHOIS systems, moving the WHOIS should be straightforward. During the testing and preparation for the SRS/registry data transition, the new registry operator's WHOIS service should also be tested. Once the registry has been loaded, the WHOIS service should be automatically

populated with data. All that will be required will be an IANA change request to show the WHOIS server at its new location. This will be done with the initial IANA change request in the DNS transition. The duration of this phase depends on the number of records and the speed of the new registry operator's system.

#### Phase 5: Data security and escrow

Data security and escrow are inherent parts of the SRS and registry systems and will be addressed with each discrete function. The registry operator, as contracted party with the escrow provider, will be responsible for updates and transfers of the data escrow and relevant contract.

#### Phase 6: Customer migration

Making sure customers have a smooth transition is one of the key factors of determining success of a transition. The steps for customer migration include:

- i. The new registry operator contacts the registrars to alert them of the upcoming transition and schedule. Registrar contact information will be provided as a Microsoft® Excel extract from the Afilias CRM database. The new registry operator begins building the changes needed to the Registrar Toolkit (RTK) - the code, libraries, and documentation that help the registrars communicate with the registry. These will include any EPP extensions that are applicable. When the RTK is ready, the new registry operator installs this code for download onto the registrar area of their website. Once the new registry operator's registry has the correct functionality installed (including any enhancements for EPP or other out-of-band extensions), the new registry operator launches their OT&E service.

The new registry operator's tech support then begins scheduling registrars for OT&E testing. This test is required for registrars to show that their systems are capable of transacting with the new registry operator's EPP servers. One week before the registry cut-over, the new registry operator issues registrar credentials into the production registry system. Note that registrars are not able to access the system yet, as they are still blocked on the server side. This allows registrars with automated systems to have the credentials in place when the system goes live. Once the registry is ready, the new registry operator removes the access blocks, and allows registrars access into the system.

The estimated duration of Phase 6 is four-six weeks.

#### Phase 7: IDNs

In addition to the steps described above for transition of registry data, IDNs presents additional critical artifacts: language policies, registry policies and associated registry data relating to IDNs.

Language Policies. This is the most critical portion of the transition as both Afilias and the new registry operator will need to ensure that prior to the transition of registry data, the new registry operator's implementation of IDNs matches to the same policies that Afilias adheres to. These policies include prohibited characters and strings, character inclusion, linguistic policies if applicable, and variant table and mapping policies where relevant. Registry Policies. Registry policies such as relevant EPP extensions catering to IDNs and WHOIS display policies for IDN queries will be forwarded to the new registry operator for review. Ideally, the new registry operator may decide to utilize and implement Afilias' policies; this will ensure a much smoother transition for both registrars and registrants.

If this is not the case, the new registry operator will need to communicate their policies to existing registrars and offer ample time for them to modify their clients to comply with the new policies. IDN Data. In addition to common data associated with an ASCII domain object, there are three additional sets of data for IDNs: language script tags that are associated to each IDN, any associated variants that are reserved due to the registration of the IDN, and any associated variants that are active or resolvable through DNS. Transition of this data will follow the same steps described in Phase 3 above for SRS/Registry Data.

The estimated duration of Phase 7 is eight to 12 weeks.

#### Phase 8: DNSSEC

Afilias will work with the new registry operator to facilitate a rollover of DNSSEC keys. Facilitating a rollover across company boundaries is a complex operation, and involves the risk of all or part of the zone being rendered invalid for a period of time. The exact procedure of the DNSSEC transition is dependent on the processes and procedures practiced by the new registry operator, but conceptually the following steps are required. (Note that since Afilias uses both a KSK and a ZSK in its DNSSEC configuration, the steps will be described as if both keys are present.)

Prior to the DNS cut-over, the new registry operator will generate a Key Signing Key (KSK). This will be added in the DNSKEY Resource Record Set (RRset) running on the Afilias nameservers. Afilias will have the new registry operator sign a set of Zone Signing Keys (ZSKs) using their KSK. The zone will be signed with both the Afilias-signed ZSKs as well as the new registry operator's ZSKs for a period of time. Afilias will submit an IANA TLD change request to add the new registry operator's DS record(s) to the domain's delegation in the root zone. At cut-over, the process in step 2 will be reversed except that the Afilias keys will have the revoke bit set. After a period post cut-over, the new registry operator will submit an IANA TLD change request to remove the Afilias inserted DS record(s) from the domain's delegation in the root zone. An appropriate amount of time after the IANA change request completes the new registry operator can safely remove the Afilias inserted DNSSEC Resource records from the zone. The estimated duration of Phase 8 is eight to 12 weeks.

#### Phase 9: Custom Features and Policies

In addition to the steps described above for transition of registry data, custom features present additional critical artifacts: feature description and use cases, EPP extensions if applicable, and associated registry data relating to the feature.

Afilias will first prepare a high level walkthrough of the custom features available for the gTLD to the new registry operator. This walkthrough will focus on feature descriptions, high level workflows and data descriptions. Once the initial walkthrough is completed, Afilias will provide detailed specifications of the features in question. These documents will include detailed use cases, work flows and EPP extension samples and XSDs where applicable. After a sufficient period of evaluation for the new registry operator, Afilias will schedule a follow up meeting to clarify any questions the new registry operator may have. Afilias will also discuss with the new registry operator the transfer of registry data, including data formats, transfer method and frequency. Transition of this data will follow the same steps described in Phase 3 above for SRS/Registry Data. Once the new registry operator has implemented the custom feature(s), they will be able to properly integrate the data with their system and thoroughly test their system. During

this period, Afiliias will be available to answer any questions to ensure efficient adoption from the new registry operator.

The estimated duration of Phase 9 is six to 12 weeks per custom feature/policy.

Transition process with a request for proposals

This will not fundamentally change the transition process itself. Once ICANN has selected a winning RFP respondent, Nameshop and Afiliias will begin the transition process as described above. If there is no respondent that meets the ICANN standards, and it is determined that the gTLD should ultimately be closed, then Nameshop and Afiliias will work with ICANN on the processes needed to appropriately shut down the TLD. As of this writing, ICANN has not yet set processes or requirements for the sunset phase of a TLD.

Transition Process for an Emergency Back-end Registry Operator (EBERO)

It is difficult to specify the actual processes to be involved with an emergency back-end registry operator, since this entity has not yet been determined, and the capabilities of that provider are not known. The following is a rough outline of how the transition could be expedited to an emergency back-end registry operator.

The time required to migrate to the EBERO will depend on the amount of cooperation involved before a disaster occurs.

Preparation required before a disaster:

i. Afiliias and EBERO determine method for zone transfers

By pre-negotiating and testing a zone transfer method (including transfer primary and secondaries and transaction signature keys), the EBERO will have the ability to quickly setup and run the DNS for the zone. This is critical to reconstitute the DNS function within the ICANN required parameters.

ii. Afiliias and EBERO determine method for secure data transfer

Similar to the zone transfer, this mechanism would be used for the underlying registry data (assuming it will not be unavailable due to the disaster). Pre-negotiation of the transfer mechanism will reduce the time required to bring the EBERO registry online.

iii. EBERO generates DNSSEC KSK and ZSK records, and sends to Afiliias for inclusion in the zone

By having the EBERO-created KSK and ZSK in the zone, the time required to migrate the zone in a fashion that keeps the zone valid throughout the process is reduced. Should a disaster occur, the EBERO can immediately begin signing the zone. If viable, Afiliias will then also sign the zone with the current keys, and set the revoke bit on the Afiliias keys.

At ICANN's determination of a required cutover, the aforementioned transition can occur, but in a much more compressed timeframe. Cutover of the DNS - the most critical function to the Internet Community, is now facilitated much quicker, because the zone file transfer has already been pre-negotiated and simply needs to be "turned on". DNSSEC transition is also much quicker, because the KSK and ZSK of the EBERO are already in the zone and properly signed by the original ZSK. This means that the EBERO can immediately start signing the zone (as indicated in Step 2 of the DNSSEC transition above).

Other transitions

Other transition activities include:

- Registry Operator Agreement with ICANN;
- Policy and the handling of reserved and premium names -- which ones are they, how are they reserved, etc.;
- Arrangements (if any) for transitioning and continuity of community-related policies and information. (For example, community membership functionality, any associated databases of membership information, etc.);
- Transition of financial records -- not just registrar account balances but also turnover of letters of credit, turnover of registrar deposit funds held by the losing registry at its bank, etc.;
- Transition of registrar and registry operator reports;
- Transition of registrar contact database;
- Turnover of Registry-Registrar Agreements and other contracts; assignment of contracts to the successor registry;
- Arrangements for names involved in: security and anti-abuse operations (e.g. Conficker), legal issues (such as domains suspended due to court orders, and disputes (domains involved in URS cases, domains involved in ICANN's transfer dispute process, domains involved in lawsuits, etc.), and;
- Turnover of materials from the losing operator's Web site, including any registrar relations area (documentation, policy postings, etc.).

Transition resourcing plans

Since its founding, Afiliias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afiliias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afiliias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afiliias project management methodology allows efficient and effective use of staff in a focused way. Afiliias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afiliias project management methodology allows efficient and effective use of staff in a focused way. Afiliias will allocate appropriate resources from every requisite department to ensure a smooth transition.

It is anticipated that over 40 individuals from across Afiliias' technical functions will be involved.

Nameshop will dedicate appropriate resources to support a transition as required.

---

**41. Failover Testing: provide a description of the failover testing plan, including mandatory annual testing of the plan. Examples may include a description of plans to test failover of data centers or operations to alternate sites, from a hot to a cold facility, or registry data escrow testing. Describe resourcing plans (number and description of personnel roles allocated to this area).**



Answers for this question (#41) are provided by Afilias, the back-end provider of registry services for this TLD.

Part of Afilias' decade of experience operating several large TLDs includes creating and testing detailed plans for registry failover. Afilias has incorporated this into its registry operations and will do the same for this TLD. Specifically, Afilias:

- Has highly detailed plans that anticipate types of registry failures, and defines the efforts to respond, and;
- Tests various components of this plan very regularly and the entire plan at least once annually.

In Afilias' experience, and based on empirical evidence, a registry is more likely to experience emergencies than complete failures. Accordingly, Afilias has implemented an Emergency Response Program (ERP) and a Global Emergency Response System (GERS) to deal with each type incident.

Failover types, intervals, test plans, and teams

Afilias' Emergency Response Program (ERP) provides for the coordination and implementation of activities to ensure that adequate and timely response measures are taken. Emergency management is a dynamic process, requiring planning, training, drills, testing equipment, and coordinating activities with stakeholders. The ERP works on a defined schedule and has an allocated budget that includes consideration for research, seminars, consulting services, and other expenses that may be necessary.

The Emergency Response Program has three primary areas of focus:

Incident detection and analysis

In the event of an emerging incident, geographically distributed monitoring tools are employed to determine the scope and of incident impact. The ERP details the procedures for problems ranging from partial failure of a subsystem to the total failure of all data centers.

In the first few moments of an incident, evaluation and escalation procedures are employed from within multiple NOCs. The NOC serves as a centralized management center for emergency operations.

During the detection phase of an incident, NOC teams follow the guidelines established in the ERP, ensuring that the appropriate first-responders are contacted and provided with information necessary to complete an incident impact assessment and begin incident response.

The ERP defines a protocol for escalation to various technical groups, account managers and management depending on the severity and nature of the incident.

Incident response coordination

A vital aspect of the ERP is a focus on ensuring that the appropriate resources are brought to bear to resolve an incident as rapidly and as safely as possible.

Each incident is assigned an Incident Coordinator, usually a member of management with the authority to make decisions. The IC is responsible for front-line management of the incident: tactical planning and execution, determining whether outside assistance is needed, and for relaying requests for internal resources or outside assistance through the NOC.

#### Incident management and communications

The ERP defines incident communication policy and ensures there is a clear chain of command available to coordinate and authorize incident response.

During an incident resulting in service disruption, a senior manager will be assigned to act as Incident Director. Working in concert with the Incident Coordinator, the Incident Director has the authority to determine the short and long terms effects of an emergency; order the partial or complete shutdown of the registry; interface with registrars, outside organizations and the media; and issue updates to registrars to aid registrants and other stakeholders.

#### Emergency registry handover

Should there be a disaster in which the entire registry database and operation has to be handed over, the Afiliias' DNS Emergency Contingency Plan contains detailed procedures that ensure such a transfer will occur quickly.

Afiliias maintains the core registry database files in an ANSI-SQL compliant RDBMS, enabling complete portability of the data from Afiliias operating systems or escrow.

To ensure smooth operation of the registry under such an eventuality, copies of Afiliias' software and systems, systems configurations, operations manuals, data and all other related material are stored at each of the EOCs. The plan for the operation of the registry, including the operations manual, listing of automated (cron) jobs, quality assurance manuals, and similar documents required for the stable operation of the registry is stored at each of the EOCs. As a contingency, the DNS ECP also plans for a data reconciliation procedure that will be procured from registrars which allows for a separate and independent path of reconciliation of data.

Finally, the DNS ECP contains a defined succession plan with members backed up in different geographic locations (i.e., key personnel are backed up in Europe, North America and Asia) in case of a complete failure.

#### Testing the ERP

Disaster Recovery (DR) drills are conducted periodically (no less than once a year) for the registry, usually including a complete failover from one data center to another and reconfiguration of all the related services. The drills are conducted according to the documented Disaster Recovery Procedures (DRPs) and, if required, improvements are implemented.

Afiliias has Disaster Recovery Site Failover plans for all data centers, offices, and its products and services (including Global Registry Services, DNS, and Corporate Services), as well as plans against other disasters.

The test plans are updated both during the testing period and during application upgrades, system upgrades, and infrastructure upgrades.

#### Disaster Recovery Site Failover Plan

The information presented below is a generic description of Afiliias' Disaster Recovery Site Failover Plan. In order to ensure that all necessary operational elements are in place to execute the Disaster Recovery plan, a number of routine tasks are carried out as part of standard operating procedures on a regular basis:

- Backups of all registry data and registry software components are made and validated on a daily basis. At least one backup copy of all critical system

components is available at each production datacentre to ensure that backups can be restored to aid in registry recovery if required. Additionally, encrypted database and registry software backups are stored off-site to guard against irrecoverable loss of data or vital registry components in the event of a catastrophic loss of multiple datacenters.

- Database consistency and availability is ensured through replication of databases to multiple subscribed database instances in a target failover datacenter. Failover systems in alternate datacenters are monitored to ensure that subscribed databases are kept in sync with the origin database and that all disaster-recovery database targets are fully operational.
- Application availability is achieved by operation of "warm" failover systems in alternate datacenters. Consistency with production configuration is ensured through the use of configuration management tools to deploy production configuration updates simultaneously to production and failover application servers. Failover servers are monitored for availability and to ensure there is no drift between failover and production configuration.
- Server and network equipment in the disaster recovery datacenter is monitored on an ongoing basis to ensure that all standby systems are fully operational if required in the event of a disaster. Capacity needs are evaluated regularly to ensure that sufficient hardware resources are available to provide service from disaster-recovery datacenters.
- Service monitoring is established on failover systems and changes made to monitoring on production systems and services are replicated in the disaster recovery environment to ensure that all monitoring in production is ready for rapid deployment in disaster recovery datacenters.
- Connectivity to the disaster recovery datacenter is monitored consistently to ensure that sufficient capacity and availability exists to activate the datacenter at a moment's notice if required. In addition to primary connectivity, secondary connectivity is available via modem and leased lines to key networking equipment.
- Standardized, pre-approved communication templates are maintained to aid in rapid outreach to registrars, staff and external agencies as required in the event of a disaster.

## Registry failover procedure description

### Initiation

If the on-call manager declares a "Disaster" situation, NOC is required to:

1. Notify on-calls for all teams involved in Disaster Recovery. A list of teams is provided in each specific Disaster Recovery procedure. Before contacting each on-call, be sure to have the following information to pass on:

- Primary ticket number
  - Conference bridge home number and entry code
  - Instant messaging conference address. Most will ask that you send an invite via your instant messaging client.
2. Send an email message to all staff formally announcing the beginning of the Disaster Recovery procedure.
  3. If a notice to registrars has not already been sent as part of the procedures for whatever scenario caused the disaster, begin this process now.

### Phase 1

Registry with all required services by SLAs should be running in production mode as a result of this phase. (Detailed steps are provided in the Afiliias internal wiki.)

1. Choose one of the following actions. If the Primary site is:
  - Accessible. Shut down Primary site gracefully.
  - Not accessible. Block access to Primary site.

2. Change information in DNS.
3. Perform preparation tasks to start registry:
  - 3.1 Production Control - Start EPP, web, WHOIS applications and pass to QA (testing the registry through the common entry opened to single test registrar).
  - 3.2 Production Control - Start oxrs-ping and DNS Distributor (while QA is testing the core functionality).
  - 3.3 NOC - Enable monitoring.
4. Perform oxrs-ping and performance checks.
5. Make decision to start registry in production (Management).
6. Start registry in production.

#### Phase 2

All registrar-related and public-related services should be working as a result of this phase.

1. Enable other application services (event handler, DNS distributor) if stopped during Phase 1 due to performance issues.
2. Enable firewall and rate-limiting rules (if not applied before).
3. Adjust monitoring.
4. Move report tasks.
5. Prepare new database replicas.
6. Reconcile transactions lost during failover.
7. Perform WHOIS cache, rate-limiters, tuneup, etc. (various team-specific tasks).
8. Prepare failback task list.

All operational phase 2 tasks are typically completed within 20 minutes from the end of stage 1 tasks. Preparations for the return of registry service to the primary site, or an alternate DR site will vary from incident to incident.

Since the output of a standard RDBMS backup is used for escrow, the testing is to restore the database from the backup output. The deposit is received from the escrow provider and restored as the primary registry database. Standard functional tests are performed to ensure accuracy and completeness. Verification is done by the escrow agent every time they receive the deposit and if any errors are discovered it is escalated to us and we re-submit the deposit. We also test the Escrow deposits twice a year during internal audits.

Most failures impacting registry operations within a site are recovered automatically with no or limited registry impact. Based on experience in testing, Afiliias anticipates the ability to recover a registry during a complete site failure is about 30 minutes.

The failover tests are conducted under the guidance of a manager who coordinates the failover activities. The time taken for every step of the failover plan is recorded as it occurs by the coordinating manager. Additionally, any notes regarding deviations from the plan, or difficulties that arose during implementation are recorded. The results are used to confirm that the plan is sound. High-level estimates are measured against the actual results recorded during the failover test. A change request may be submitted to adjust the failover plan in response to issues that may have arisen during the test. The results are shared with all members of all technical teams that may be participants in a failover under emergency circumstances. Additionally, summary is provided to senior management and to the registry operator upon request.

#### Failover plan updates

The failover plans are updated as part of the change management process (see our response to question #33). If a change to configuration items in the operating environment due to a software or hardware release will materially impact the execution of the failover plan, a child request for adjustments to the failover plan will be submitted to capture any necessary revisions. The failover plan is governed by the same stringent change management process as the operating environment itself.

#### Testing experience

Over the past several years, Afiliias' failover plan has been tested numerous times for multiple registries and in multiple datacenters.

Due to the success of these tests, the basic framework of the failover plan has remained unchanged since its initial development. However, each test of the plan provides learning opportunities, and aspects of the plan have been altered in response to information gathered during tests.

On some occasions, minor issues have arisen which caused small delays in restoration of normal registry operations. Under most circumstances, full registry functionality is restored in under 45 minutes.

The failover plan was conducted to its fastest completion in 37 minutes, with registry operations restored after only 31 minutes - the additional time was spent validating registry functionality prior to re-launch.

The slowest failover execution took 1 hour and 24 minutes. On this occasion unexpected difficulties were encountered converting the target replica to become the origin database. Lessons learned from this test resulted in an increase of monitoring on subscribed databases to ensure that the database inconsistency issue which delayed the process would not go undetected in the future.

The failover process has been conducted successfully by fully assembled test teams as well as a "skeleton crew" to ensure that all elements are in place to ensure success under a variety of circumstances.

Repeated testing of the procedure has demonstrated its efficacy in restoring registry operations in the event of a catastrophic registry failure.

#### Resourcing plans

Since its founding, Afiliias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afiliias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afiliias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afiliias project management methodology allows efficient and effective use of staff in a focused way. Afiliias operates in a matrix structure, which allows its staff to be allocated to various TLDs or projects as needs occur. Within our organization, appropriate functional skills are always "on-call" to meet needs. With a team of specialists and generalists, Afiliias uses a disciplines project management methodology to ensure efficient and effective use of staff to address

customer needs. Company managers are knowledgeable of the current status of and priorities associated with their areas of responsibility which permits them to make informed decisions.

While the majority of technical resources are in Toronto, there are members of development, operations and quality assurance in five different countries on three separate continents. Afiliias is fully equipped to provide: 1) work-at-home arrangements for all staff, as needed, and as is regularly done to provide 24X7 coverage with on-call staff and managers, and 2) geographical redundancy. We also have senior technical management in four countries to provide direction and decision-making authority as needed.

The registry failover-testing plan is carried out by experienced, existing members from all technical departments on an "as needed" basis. This TLD will be integrated into the planning described above upon launch.

The failover team for integrating and on-going maintenance includes 41 Afiliias team members, including the NOC staff, Data Services team, and various technical analysts.

---

**42. Monitoring and Fault Escalation Processes: provide a description of the proposed (or actual) arrangements for monitoring critical registry systems (including SRS, database systems, DNS servers, Whois service, network connectivity, routers and firewalls). This description should explain how these systems are monitored and the mechanisms that will be used for fault escalation and reporting, and should provide details of the proposed support arrangements for these registry systems. Describe resourcing plans (number and description of personnel roles allocated to this area).**

Answers for this question (#42) are provided by Afiliias, the back-end provider of registry services for this TLD.

As a provider of stable and secure registry service for the past decade, Afiliias recognizes the high degree of importance on monitoring and responding to potential threats and prioritizes the support activities accordingly. The technical organization has an extensive set of monitoring tools and information protocols. Afiliias will provide this existing capability for this TLD, specifically:

- Effective monitoring tools that track all critical registry system components, support systems, facilities, and communications networks;
- Detailed protocols for incident reporting which track the entire incident lifecycle, from identification through resolution, with communication plans for both internal and external information sharing, and;
- Tested plan of action for registry failover that prioritizes critical registry functions and limits any downtime that is managed and updated by existing, trained staff.

**System monitoring**

Each registry system component is monitored for security, performance and stability both from within the data center and from a remote site. Three separate monitoring systems provide independent checks for potential problems. This allows a validated early warning system, in order to allow

ample preparation in case of a detected fault. 24x7 on-site and remote network and system monitoring ensures system up-time and performance at all times.

If any anomalies occur, technical support staff is on duty monitoring systems 24x7 and is alerted immediately. Second-level technical staff is available on-call 24x7 to immediately address any potential failure of a system component.

Afilias actively monitors the SRS and the related network at its redundant Network Operations Center (NOC). All NOC sites are staffed 24x7. The NOC team receives real-time reports of key system performance metrics and the availability of all registry services. At any time, a minimum of four qualified registry operations engineers are available on site, or by phone, to respond to emergencies.

Afilias monitors the system for security breaches both from within the data center and outside, using both system-based and network-based testing tools. Afilias also performs network vulnerability assessments on a regular basis. Operations staff also monitors systems for security-related performance anomalies.

Afilias' monitoring systems provide:

- Continuous monitoring of all network and server infrastructure components;
- Network availability monitoring;
- Network performance management using Nagios and OpenNMS;
- Application performance monitoring, and;
- Alert management.

An illustrative list of monitoring tools/techniques used by Afilias are described below:

- Internal checks: enabled on each individual server and network device that constantly monitor for any failure, which is instantly reported to the Network Operations staff.
- External checks: enabled from a third party site, to provide external monitoring of Web, Mail, DNS, WHOIS, API, EPP or any other service accessible from the Internet.
- Nagios Monitoring: <http://www.nagios.org/>. This host and service monitor is designed to identify network and system problems in the DNS, applications performance, monitoring, and alert management. The monitoring daemon runs intermittent checks on specified hosts and services using external "plug-ins" which return status information to Nagios. When a problem is encountered, the daemon sends out notifications to the NOC via e-mail, instant messenger and SMS. Current status information, historical logs and reports can all be accessed via a web browser.
- Nagios Monitoring for Disaster Recovery: Nagios has been configured for Disaster Recovery and failover to alternate data centers. During disaster recovery, monitoring is pre-configured, and it can be brought up in the disaster recovery data center while fail-over is in progress.
- Cacti Monitoring: Please see: <http://www.cacti.net/>. This is an open source, web-based graphing tool designed as a frontend to RRDTool's data storage and graphing functionality. Cacti is configured to poll services at predetermined intervals and graph the resulting data. Cacti allows for easily graphed statistics on a minute by minute, hourly, daily and weekly basis for both registry and DNS performance.
- OpenNMS: Please see: <http://www.opennms.org/>. This is an enterprise grade network management platform developed under the open source model. OpenNMS is

a distributed, scalable platform for all aspects of the Afiliias Fault, Configuration, Accounting, Performance, and Security (Afiliias FCAPS) network management model. OpenNMS features service polling to determine service availability, data collection, storage and reporting on network information, and event and notification management for receiving events, both internal and external.

- Application performance monitoring: Afiliias uses a variety of tools for application performance monitoring. These tools constantly check registry performance for various commands (Create, Delete, Update, Info, Check, etc.) and alert the Network Operations staff if at any time the performance thresholds are exceeded. Whenever possible, thresholds are set to warn of imminent problems before they occur.
- Alert and Warning system: Afiliias subscribes to early alert and warning systems and monitors global issues on DDoS attacks, viruses, worms and SPAM proactively.

Specific critical functions are monitored extensively. For example:

- Database monitoring. For databases, Afiliias uses Nagios monitoring. Specifically, DB Ping queries which look for a response; failure is no response and/or timeout. Issues are flagged if transactions are running longer than 50ms.
- DNS servers monitoring. Internal checks are enabled on each individual server and network device that constantly monitors the device for any failure, which is instantly reported to the Network Operations staff.
- Web Monitoring: Internal and external checks are enabled on each individual web server that constantly monitors the web server for any HTTP/HTTPS error, which is instantly reported to the Network Operations staff.
- WHOIS systems monitoring. WHOIS monitoring is performed from external locations and internally within the data centers where the application is hosted. Errors and system failures are reported instantly to the Network Operations staff.
- Routers. Router monitoring is currently performed 24x7 via the OpenNMS tool. Alerts are reported instantly to the Network Operations staff.
- Firewalls monitoring. Firewall monitoring is performed 24x7. Alerts are reported instantly to the Network Operations staff. Changes to a firewall configuration are deployed by Network Engineering staff and explicitly checked by Network Operations staff.

#### Incident management process

To effectively manage the data from these monitoring tools, Afiliias has implemented a detailed Incident handling process shown in Figure 42-a.

Detailed plans for each summarized step in Figure 42-a and Afiliias' communication plans are available upon request. They define the team members involved, goals, incident report development and data requirements, communication plans for internal and external contact, escalation, recommendations and resolution. In short, these multi-page protocols track an anomaly or potential issue from identification through problem resolution, e.g., change modification. These plans are available upon request.

#### Incident Report

1. Afiliias will produce an Incident Report for Customer facing tickets, or (Bal) Critical tickets.
2. The Afiliias produced Incident Report will be delivered within 3 business days of the resolution of the ticket.
3. Incident Reports will contain:
  - Timeline of events



- Details of the process and incident
- Root cause
- Suggested action items
- Action owners
- Sign off by Account Manager

#### Incident Report process flow

Step 1: Collecting the Information and Timeline for an IR

- During an incident, as per the above Incident & DR Handling flowchart/procedure:
1. The receiver of the Escalation alert will become the Incident Owner and own the incident tracking ticket for the duration of the incident.
  2. The Afiliias Technical team will add a summary of their repair activities chronologically and the resolution.
  3. The Afiliias Technical team will follow up with the customer to provide updates to the tracking ticket periodically (every 60 min.).

Step 2: Preparing a draft IR - NOC

- The Afiliias Technical team will transform the information out of the tracking ticket into an IR draft, converting local times to UTC, and attach it to a new IR tracing ticket as a Rich Text Format (RTF) document.
- The Afiliias Technical team will assign the IR ticket to the Afiliias on-call manager.

NOTES:

1. The Afiliias Technical team will create an Incident Report Tracking Ticket in the Incident Reports □ RT Queue with a subject in the following format: Incident Report YYYY-MM-DD: Brief description of issue. (Use the date of the incident, not the date the report is being created.) If multiple products are impacted, then a single tracking ticket will be used.
2. The Afiliias Technical team will link any incident-related tickets to the Incident Report ticket for reference.

Step 3: Reviewing and revising the draft report - On-call manager

- On the next business day following the incident, the on-call manager will conduct an incident review/summary meeting with internal stakeholders. It is mandatory for all the involved team members to participate in the meeting. Team members prepare their comments/recommendations for the meeting, add actions and owners.
- At the meeting: The team will review the draft, make corrections as required, discuss and add recommendations. Staff should indicate if additional information is forthcoming from external sources (e.g. hardware vendor incident analysis, etc.).
- After the meeting: The on-call manager will assign the RT ticket to the MAT and the relevant Account Manager(s) will receive a revised draft.

Step 4: Completing the IR - Account Manager(s) and On Call Director(s)

- The Account Manager(s) will make any necessary changes and send the Incident Report to the On Call Director for final approval.
- The On-Call Director for Managed DNS will be either the department head of Customer Service or the department head of Corporate Services.
- After the approval of the Incident Report, the Account Manager will then attach the revised version to the Incident Report Tracking Ticket, and submit it to the Customer within 3 business days.

Step 5: Implementing the recommendations

- The Afiliias Maintenance Approval Team (MAT) will review the report at their next immediate meeting.

- MAT will make final corrections to the recommendations and add additional comments (if any)

Commitment to provide a 24x7 fault response team

Afilias' redundant NOCs are located at its facility in Toronto, Ontario and at its facility in Horsham, USA. The 24x7 NOC function is the foundation of the Afilias fault response trigger mechanism; because NOC is staffed round the clock, and because they have the full array of tools to review the comprehensive registry system for all critical and non-critical functions, NOC is usually the origin of most fault responses.

Afilias NOC engineers are highly trained analysts with specialized skills in monitoring and performing Tier1 analysis of errors, faults and catastrophes on the registry system. A well-defined escalation policy allows NOC members to trigger a larger scale response to faults whose solution is beyond the capability of the NOC team.

Afilias manages a 24x7 on-call operation, where multiple team members with specialist skills in each critical registry function are available to respond to a fault response escalation. This 24x7 escalation response team includes members of senior technical management, who are also on-call and who operate as a pair to ensure redundancy and backup.

The 24x7 on-call fault response team, in addition to the 24x7 NOC team and the 24x7 Customer Support team are all located in geographically disperse areas, to avoid over-dependence or failure due to a geographic locale fault.

All 24x7 fault response team members are issued with state-of-the-art communications and computing equipment, in order to ensure optimal availability and accessibility. In addition, 24x7 fault response team members' Internet connectivity to their homes is paid for by Afilias; further, all 24x7 fault response team members are provided network cards which allow for Internet access via mobile networks, in the contingency that regular Internet access is disrupted. The 24x7 NOC includes an array of satellite hub equipment, dedicated line cards, satellite gateways, NMS servers, protocol processors and ample spare equipment.

In summary, Afilias is both capable of and commits to a fully staffed, properly trained and well managed 24x7 fault response team.

Meeting fault tolerance guidelines

The Afilias NOC has a dedicated Engineering Team and a 24x7 Tech Support team comprised of highly-skilled, RedHat-certified professionals who monitor and optimize the network on a continuous basis from two, separate mirrored locations. All employees and contractors sign agreements stating that they will be available to work on a 24x7 basis. Additionally, Afilias offers registry customers (registry operators) the capability to remotely monitor network operation and performance.

Continuous, around-the-clock monitoring of the network to ensure optimal performance with regards to fault tolerance is always maintained and SLA commitments have always been met. The Afilias monitoring teams' primary responsibilities, tasks and attributes include, but are not limited to:

- Design and implement network infrastructure based on business requirements and best practices in a cost effective manner. Afilias' professionally

trained Engineers respond to all issues related to production network services with a sense of urgency in a 24x7 operational environment. In addition, the NOC team independently works with Operations, Data Services, Support operations and Technical Support to provide network support while evaluating existing network solutions and optimize where possible.

- Perform network monitoring and capacity planning, ensuring network performance and fault tolerance meet SLAs. The Afiliias monitoring team evaluates, tests and recommends new technology platforms that will increase network performance and reliability.
- All 24x7 NOC staff has extensive experience managing large and complex networks and implementations in either a large enterprise or ISP environment with experience in vendor product evaluation (hardware, software, service provider). The Afiliias team boasts Network Operators with excellent written and verbal communications skills, with strong network problem isolation and troubleshooting skills. All must have working knowledge of DNS, strong knowledge of the TCP/IP protocol stack, and strong experience in Cisco IOS. Working knowledge in dynamic routing protocols such as OSPF and BGP, coupled with working knowledge of T1, T3, Sonet, Frame-relay, MPLS and Ethernet, are also required. Hands-on knowledge of load balancers, traffic management devices, and traffic generators is also necessary.
- Strong knowledge in statistical gathering and analysis via scripting languages.

Afiliias 24x7 comprehensive ownership of the entire fault handling and escalation process is supported by a robust fault tolerance escalation and incident handling process. Afiliias fault monitoring experience in managing mission-critical operations efficiently has been successfully replicated in both NOCs.

In addition to continuous improvements to fault monitoring tools, processes and operational reporting, Afiliias has effectively shortened the turnaround time to resolve faults by:

- Close fault monitoring by the Fault Response team (part of the NOC) from detection until fault resolution;
- Immediate response to faults reported by the remote monitoring system before being reported by end users;
- Defined fault terminology to minimize delay due to mis-interpretation by different registry operators' end users;
- Performing immediate first line fault restoration via remote control system;
- Introducing automation to improve staff efficiency (e.g., automated paging and messaging);
- "Live" information for contractors or customers taking over shift or faults, and;
- Managing and coordinating with various parties affected by the incident.

#### Facilities security

All production facilities have 24x7 onsite security staff to prevent physical security breaches. CCTV cameras are recording all activities in and around the facility. The security personnel monitor these and any anomalies detected are investigated and reported. Only authorized users have physical access to the production facilities. Only those personnel with government-issued picture IDs and listed on authorized access lists are permitted entry. An authorized staff member must accompany all visitors. Within the data centers, Afiliias' own cabinets and cages are securely bolted to the floors. Visitors to these data centers cannot access Afiliias' caged areas.

Physical security is maintained at each Afiliias office. CCTV cameras are also installed at the office locations. These record any activity and are also

monitored by the NOC staff. Any issues are quickly identified and escalated. All visitors to the offices must register to gain entrance to any Afiliias facility and be accompanied by an authorized staff member. Employees are given access badges that only allow them into areas they are authorized for. For example, only Operations and NOC staff are allowed access into the server room. Security alarm systems are in place and alert authorities upon activation.

#### Fault tolerance building security

Afiliias vigilantly controls physical access to its operating facilities. Physical security mechanisms include security trained guards 24x7, closed circuit TV surveillance video cameras, and intrusion detection systems. The NOC monitors access to all locations on a 24x7 basis.

At Afiliias SRS data center locations, employees must present badges to gain entrance, and must wear their badges at all times while in the facility. All visitors must register to gain entrance to any Afiliias facility. Visitors must display visitor badges at all times while they are in the facility, and must be escorted by an Afiliias employee. Visitor registration records are maintained for a period of one year.

Afiliias on-site security personnel are on duty 24x7 to monitor closed-circuit television cameras placed strategically throughout the facilities. Security personnel are stationed at each building-access point throughout normal working hours; at other times, employees must use authorized electronic key cards to gain access to the buildings. Further, any room that houses sensitive data or equipment is equipped with a self-closing door that can be opened only upon activation of a hand geometry reader.

Senior facility managers establish the rights of employees to access individual rooms, and ensure that each reader is programmed to pass only authorized individuals. The electronic readers compile and maintain an access record. The system is tested monthly as per fault tolerance guideline procedures.

Afiliias' ability to provide real-time fault reporting both to the registry operators and customer engineers fundamentally differentiates Afiliias' approach. Afiliias' fault reporting system is specifically tailored to the fault reporting environment. It provides many value-added services to registry operators in terms of:

- Monitors and tracks all inbound fault calls.
- Afiliias makes fault-recording data available to registry customer and Afiliias management staff.
- Provides a common, customized fault database to record all faults.
- Provides an extensive, yet flexible and customized reporting of the faults.

In addition, Afiliias staff members consolidate a monthly report of the most commonly seen incidents, analyze fault trends, and recommend pre-emptive actions. All these value-added services help registry operators to understand the common faults better and make right decisions in pre-emptive actions and planning.

#### Resourcing plans

Since its founding, Afiliias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afiliias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past

decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. 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 staff in a focused way. 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 staff in a focused way.

The proven monitoring and fault escalation management at Afilias is supported by 51 team members who are responsible for both the implementation and ongoing monitoring and fault escalation of this TLD. This includes 14 dedicated NOC analysts split between two locations in Toronto, Ontario, and Horsham, Pennsylvania that provide 24x7 fault monitoring, reporting, and issue resolution. As described above, this team is solely dedicated to monitoring systems, escalating problems (as required), and notifying key personnel of issues.

Fault monitoring resource continuity

Plans to address human resource continuity include geographic diversity:

- Afilias has technical staff located in Toronto Canada; Horsham, Pennsylvania USA; Dublin, Ireland; and New Delhi, India.
- Afilias has fully operational Customer Service groups located in Toronto and New Delhi.
- Afilias has fully operational Network Operation Centers located in Toronto and Horsham.

Each center is fully capable of autonomous operation in the event that the other facilities should go offline. All technical and NOC staff have the ability to work remotely via high-speed virtual private network (VPN) connections in situations where they are unable to physically work in the offices due to unexpected events such as an outbreak of disease, flooding, etc.

---

**43. DNSSEC: Describe the policies and procedures the proposed registry will follow, for example, for signing the zone file, for verifying and accepting DS records from child domains, and for generating, exchanging, and storing keying material. Describe how the DNSSEC implementation will comply with relevant RFCs, including but not limited to: RFCs 4033, 4034, 4035, 5910, 4509, 4641, and 5155 (the latter will only be required if Hashed Authenticated Denial of Existence will be offered). Describe resourcing plans (number and description of personnel roles allocated to this area).**

Answers for this question (#43) are provided by Afilias, the back-end provider of registry services for this TLD.

Afilias has been at the forefront of DNSSEC deployment. Securing certain domain name information through signing can play a vital role in Internet security. DNSSEC can protect both website managers/owners as well as consumers or users. Afilias has been committed to enhancing domain security through DNSSEC, as illustrated by:

- Supporting the first major gTLD to launch DNSSEC: .ORG;
- Identifying the defect in RFC 4310 (DNSSEC provisioning via EPP) and taking a lead role in developing the revised standard, RFC 5910, and;
- Continued support of the DNSSEC-deployment community efforts at ICANN and in the technical community.

On June 2nd, 2009, Afilias performed the technical implementation of DNSSEC in .ORG, which became the first major gTLD - and the largest zone at the time - to be signed using DNSSEC. Since then, Afilias has signed all of the TLDs for which it provides services, unless specifically requested not to do so by the registry operator.

Afilias is also an active participating member of the DNSSEC Coalition. The registry system deployed will be fully DNSSEC-aware, including adding DS record information via EPP, as well as displaying DS record information via WHOIS output.

Continuing pioneering registry work, Afilias has deployed NSEC3 for its signed TLDs. When DNSSEC systems are deployed using the older NSEC standard, it is possible to download the entire TLD zone, by "walking the tree". However, using the NSEC3 standard, this becomes much more difficult. NSEC3 ensures that TLD zones will be kept as private and secure as possible.

Afilias' coupling of NSEC3 with Opt-Out makes manipulation of the signed zone more efficient. Only Resource Record sets for which the TLD nameserver is authoritative are signed, reducing the zone size significantly. This allows for faster signing and updates to the zone.

Afilias' architecture uses multiple state-of-the-art, High Security Modules in secure facilities to sign zones. By implementing the signer with dedicated, hardened systems, Afilias automatically signs zones quickly and efficiently. These systems ensure that keys are safe and secure, because they never leave the High Security Module.

Afilias trains registry personnel and registrars on how to implement and deploy DNSSEC for second level domains, and how to interact with the registry to pass Delegation Signer (DS) records up to Afilias. Afilias takes care of all key generation, key rollover, and signing for a TLD, making the deployment of DNSSEC in a TLD an ordinary and straightforward service.

#### DNSSEC Policy Statement

The DNSSEC Policy Statement includes two facets:

##### 1. DS record publication

Afilias will allow registrars to transmit Delegation Signer (DS) records into the registry over EPP, in compliance with RFC 5910. Because DS records may exist in the parent zone before the corresponding DNSKEY exists in the child zone, Afilias cannot immediately check that a DS record offered by the registrar "completes the trust chain" to the child zone. These DS records will be published in the same manner as described for other resource records.

##### 2. Zone signing

Afilias re-signs zones on roughly a two-week basis (which varies to discourage potential attacks). All zone signing is done using keys stored in High Security Modules (HSMs). New DS records are signed as soon as they are introduced into the system. RRSIGs typically have a 20-day expiry, leaving as much as six days to diagnose a problem with a particular signing without adversely affecting the validity of the zone.

For a complete draft of this statement, see attachment "43-DNSSEC Policy Statement". This document will be available on the TLD website.

#### Standards compliance

Afilias' registry deployments currently support the following DNSSEC-related RFCs:

- RFC 2536: DSA KEYS and SIGs in the Domain Name System (DNS).
- RFC 2539: Storage of Diffie-Hellman Keys in the Domain Name System (DNS).
- RFC 3110: RSA/SHA-1 SIGs and RSA KEYS in the Domain Name System (DNS).
- RFC 4033: DNS Security Introduction and Requirements.
- RFC 4034: Resource Records for the DNS Security Extensions.
- RFC 4035: Protocol Modifications for the DNS Security Extensions.
- RFC 4398: Storing Certificates in the Domain Name System (DNS).
- RFC 4470: Minimally Covering NSEC Records and DNSSEC On-line Signing.
- RFC 4509: Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs).
- RFC 4986: Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover.
- RFC 5011: Automated Updates of DNS Security (DNSSEC) Trust Anchors.
- RFC 5074: DNSSEC Lookaside Validation (DLV). Afilias is compliant, although this RFC is not germane to running authoritative name servers.
- RFC 5155: DNS Security (DNSSEC) Hashed Authenticated Denial of Existence.
- RFC 5702: Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC.
- RFC 5910: Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP).
- RFC 6014: Cryptographic Algorithm Identifier Allocation for DNSSEC. Afilias is compliant, although this RFC is not germane to running authoritative name servers.

RFC 4641 is currently under document update at the IETF. As this is a guide for operational practices, there is no sense of formal "compliance" with this work-in-progress. However, Afilias currently follows the guidelines of RFC 4641 and will continue to follow the guidelines in RFC 4641-bis as it becomes available.

RFC 5933 describes the use of GOST algorithms for use in DNSKEY and RRSIG resource records. Afilias does not support GOST, as this algorithm is considered to be insecure with the cryptographic community.

#### Key management procedures

Afilias operates zones directly under the root (TLDs), as well as second level zones directly under the TLDs it supports (e.g., co.in.). For each zone, Afilias maintains sets of Zone Signing Keys (ZSKs) which are used to sign the zone, and Key Signing Keys (KSKs) which are used to sign ZSKs.

#### Key management system

Afilias uses a combination of secured hardware and software specifically designed for DNSSEC. Each system includes a High Security Module (HSM), which is FIPS 140-2 level 2 compliant. Afilias deploys multiple systems in each registry data center, with one designated as the primary system. In the event of a primary failure, up to three additional signing systems take over responsibility for zone signing. The four systems are set up in a "bow-tie" configuration, ensuring that each system has two "hot stand-by" systems immediately available if needed. The configuration for a given zone is set up in a "bow-tie" configuration as depicted in Figure 43-a.

#### Key generation

New KSKs are generated either on demand (because of a real or perceived compromise), or on an interval of roughly three years (as a matter of security the exact number of days fluctuates). KSKs are generated with both the Zone Key (bit 7) and the Sep Entry Point (bit 15) flags set. New ZSKs are generated on a roughly monthly basis (again, as a matter of security) and have the Zone Key (bit 7) flag set. Both KSKs and ZSKs are currently signed using the RSASHA1-NSEC3-SHA1 algorithm.

#### Key dissemination

The systems employed by Afiliias transfer key information by further encrypting the keys and sending the encrypted information via internal secured networks to the other signers. Only the signing systems have the ability to decrypt these transferred messages. There is no other mechanism to extract the private key information from the HSMs. This is also depicted in Figure 43-a.

#### Key introduction and revocation

As new ZSKs are generated, they are introduced into the zone (i.e., the DNSKEY record is published and signed in the zone) one month before being used to sign the zone. This allows time for validating resolvers to recognize this DNSKEY as valid for signing a given zone. Once the introduction period is over, this key is used to sign the zone. Once a ZSK has been used for a month, the revoke (bit 8) flag is set for this key, and is used one final time to sign the zone, along with the previously introduced new ZSK. Only the new key will be used for subsequent zone signing. The revoked key will continue to exist in the zone for roughly another month before it is removed from the zone.

New KSKs are introduced and destroyed in a similar fashion.

#### Key publication

Because all of these zones fall either directly under the root, or indirectly (via a complete "chain of trust" through an Afiliias-operated TLD), public key signing key (KSK) information is disseminated to the public by generation of a Delegation Signer (DS) DNS record, which is then submitted to the IANA for inclusion in the root zone. When new KSKs are generated, the accompanying DS record is submitted to IANA well in advance of the start of its usage.

#### Signature generation, expiry and zone signing

Currently, the Afiliias registry system accepts Delegation Signer (DS) records from registrars. When a DS record is received from a registrar (via EPP) for a domain name in a signed zone, that record is immediately signed, and the corresponding RRSIG record has an expiry of 20 days. This ensures that no matter when a record is received, the original signature is valid for at least one zone resigning, with time left in the event that there is an issue with the zone resigning.

The zone is signed roughly once every two weeks. Again, this allows for time to solve problems with signing a zone before individual signatures expire.

#### Domain name transfers

When a domain name is transferred between DNS operators, best security practices recommend a key rollover. Afiliias has no insight into the DNSSEC practices of DNS operators. A registrant is responsible for coordinating the transfer between the DNS operators and, specifically, ensuring that the DS



record for the new public key information is submitted through their registrar to the registry. This is essential to ensure uninterrupted DNS service.

Separately, when a registrant is transferring a domain from one registrar to another, the Afiliias registry system requires that the gaining registrar also be certified to offer DNSSEC services. A registration transfer request will fail if the gaining registrar is not certified to offer DNSSEC services and the domain is currently signed at the losing registrar. While a domain is signed it can only be transferred between registrars certified to offer DNSSEC services. This is necessary to ensure that a registrant (or their DNS operator) can continue to execute their key management responsibilities.

#### Resources

Since its founding, Afiliias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afiliias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afiliias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afiliias project management methodology allows efficient and effective use of staff in a focused way. Afiliias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afiliias project management methodology allows efficient and effective use of staff in a focused way.

Across Afiliias, there are 56 team members knowledgeable and contributing to the support of DNSSEC. Specifically, the Afiliias Content Propagation and Resolution Team (CPR), comprised of 10 DNS technologists, are responsible for DNSSEC resolution. The Production Control team, with 14 members, is jointly responsible with CPR for signing integrity. This existing team will be responsible for both implementation and ongoing maintenance of DNSSEC. Code developers and QA personnel create and test SRS code updates. Tech Support personnel train registrars and assist them with testing and implementation.

---

**44.(OPTIONAL) IDNs: state whether the proposed registry will support the registration of IDN labels in the TLD, and if so, how. For example, explain which characters will be supported, and provide the associated IDN Tables with variant characters identified, along with a corresponding registration policy. This includes public interfaces to the databases such as Whois and EPP. Describe resourcing plans (including number and description of personnel roles allocated to this area). Describe how the IDN implementation will comply with RFCs 5890, 5891, 5892, and 5893, as well as the ICANN IDN Guidelines at <http://www.icann.org/en/topics/idn/implementation-guidelines.htm>.**

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS, WHICH ICANN INFORMS US (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE, ACCORDING TO SPECIFIC GUIDANCE FROM ICANN UNDER CASE ID 11027.

---

## Demonstration of Financial Capability

---

**45. Financial Statements: provide audited or independently certified financial statements (balance sheet, income statement, statement of shareholders equity/partner capital, and cash flow statement) for the most recently completed fiscal year for the applicant, and unaudited financial statements for the most recently ended interim financial period for the applicant. For newly-formed applicants, provide the latest available financial statements. Financial statements are used in the analysis of projections and costs.**

Nameshop is a new Proprietary firm, its first operational financial statements will be audited for statutory requirements by 30 September 2012.

For the purpose of evaluation, Balance Sheets, Income Statements showing Owner's Equity for the accounting years ended March 31, 2011 and March 31, 2012 are attached as self-certified statements.

---

**46. Projections Template: provide financial projections for costs and funding using Template 1 (attached) for the most likely scenario. The template is intended to provide commonality among TLD applications and thereby facilitate the evaluation process. Include explanations for any significant variances between years (or expected in years beyond the timeframe of the template) in any category of costing or funding. Describe the basis / assumptions for the numbers provided, and the rationale for the basis / assumptions. This may include studies, reference data, or other steps taken to develop the responses and validate any assumptions made.**

The financial projections are based on conservative estimate of limited operations during the first 3 years, but expected to grow more than proportionately after the first 3 years. At this stage Nameshop would financially scale up its operations and would commit additional escrow deposits to support continuity of operations if called for. The registration fee is taken at US \$ 25 per registration with an annual increase of 10%, however with increase in the number of registrations, the Registration Fee could also be brought down to about \$ 10 at current price levels. The projections provide a rough indication without any rigidity of decision on the fee structure. Nameshop has chosen a competent and experienced Registry Service provider with an arrangement that minimizes inhouse Technical and Operational staff requirements; Nameshop as a Registry would focus on marketing functions. Estimates provided for the first 3 years are commensurate with the initial volume of operations for the first 3 years. With most of the Registry Services functions handled by Afiliast, the

capital expenditures will be kept at a minimal level during the first 3 years. Nameshop will utilize its present office infrastructure at Erode, India, which is a family owned property with the required office equipment and manage its administrative functions by hiring a compact staff of efficient marketing professionals from the region. However after financially scaling up its operations, nameshop would scale up its marketing infrastructure as also enhance its support infrastructure to complement the services provided by Afiliias.

The conservative projections presented are not to be taken as a sign of short sightedness or lack of understanding of the potential for the TLD string applied for. The string applied for is expected to become far more relevant after a little later than immediately, so the Applicant has prepared this projections with a good understanding and a willingness to be patient. The Applicant has chosen to raise a conservative level of funds at this stage, and expects the business of this Registry to be more attractive to investors post-application stage, and would raise additional funds by private placement.

The founder expects some family funds to be available for investment which could be used to supplement available funds in the event of contingencies.

---

**47(a). Costs and capital expenditures: describe and explain the expected costs and capital expenditures of setting up and operating the proposed Registry. As described in the Applicant Guidebook, the information provided will be considered in light of the entire application and the evaluation criteria. Therefore, this answer should agree with the information provided in the template to: 1) maintain registry operations, 2) provide registry services described above, and 3) satisfy the technical requirements described in the Demonstration of Technical & Operational Capability section. Costs should include both fixed and variable costs.**

The investment strategy is conservative. Nameshop as applicant with a reasonably good access to a few potential investors, has opted to wait till the application process is complete before seeking substantial investments. The capital costs are kept at a minimal level with a strategy to purposefully avoid unnecessary pre-application infrastructure or publicity. The applicant company has its own office infrastructure for Nameshop as a domain reseller business which is operated together with InternetStudio, a web hosting business. This infrastructure is more than adequate at the applications stage. For the first 3 years of operation at conservative volumes, Nameshop will utilize the same office infrastructure at Erode, India, which is a family owned property with the required office equipment and manage its administrative functions by hiring a compact staff of efficient marketing professionals from the region. However after financially scaling up its operations, nameshop would scale up its marketing infrastructure as also enhance its support infrastructure.

Nameshop has chosen a competent and experienced Registry Service provider with an arrangement that minimizes inhouse Technical and Operational staff requirements; Nameshop as a Registry would focus on marketing functions. Estimates provided for the first 3 years are commensurate with the initial volume of operations for the first 3 years. With most of the Registry

Services functions handled by Afiliias, the capital expenditures will be kept at a minimal level during the first 3 years.

Phases of funding:

The financial projections are based on conservative estimate of limited operations during the first 3 years, but expected to grow more than proportionately after the first 3 years. At this stage Nameshop would financially scale up its operations and would commit additional escrow deposits to support continuity of operations if called for. The conservative projections presented are not to taken as a sign of short sightedness or lack of understanding of the potential for the TLD string applied for. The string applied for is expected to become far more relevant after a little later than immediately, so the Applicant has prepared this projections with a good understanding and a willingness to be patient. The Applicant has chosen to raise a conservative level of funds at this stage, and expects the business of this Registry to be more attractive to investors post-application stage, and would raise additional funds by private placement.

Projected operating cash outflows for Marketing, Customer Support and Technical functions are based on the fact that the Registry Services functions are largely managed by the Registry Service provider with a very limited need for oversight or intervention on these functions; Marketing & customer support functions would be focused on relationship management of the Registrars associated for the initial volume for the first 3 years. For the first 3 years the Founder of Nameshop would oversee the overall operations and compensation for the founder is not taken into account at this phase of initial operations.

---

**47(b). Describe anticipated ranges in projected costs. Describe factors that affect those ranges.**

As referenced throughout this application, we have contracted with Afiliias for back-end registry services, who has over a decade of experience managing TLDs. This knowledge was leveraged to produce a technical plan that was consistent with the needs of our business model. Our contract with Afiliias is such that any change in the level of registrations only affects the variable costs per domain paid to Afiliias; there is no escalator clause that would result in this fee being greater than the agreed upon schedule. This fee structure has a minimum cost per financial transaction and this represents the entire fee paid to Afiliias for handling all of the technical operations of the Registry including 4 of the 5 critical registry functions (excludes escrow).

---

**48(a). Funding and Revenue: Funding can be derived from several sources (e.g., existing capital or proceeds/revenue from operation of the proposed registry). For each source (as applicable), describe: I) How existing funds will provide resources for both: a) start-up of operations, and b) ongoing operations, II) a description of the revenue model including projections for transaction volumes**

**(if the applicant does not intend to rely on registration revenue in order to cover the costs of the registry's operation, it must clarify how the funding for the operation will be developed and maintained in a stable and sustainable manner), III) outside sources of funding (the applicant must, where applicable, provide evidence of the commitment by the party committing the funds). Secured vs. unsecured funding should be clearly identified, including associated sources for each type.**

Nameshop is conservative in raising funds at the application stage, no more than what is required to meet the application fee, guarantee requirement, and other necessary costs but is inclined to bring in additional capital by private placement post application. Apart from the reasons of being conservative, this decision is also from out of caution that the string applied for needs to be kept confidential to minimize the chances of contention. With this caution, Nameshop has so far refrained from reaching out to potential investors and would take up that exercise after ICANN makes the applied for strings public.

i) and ii) The calculations presented in the financial projections DO NOT take into account this plan to raised funds by private placement. At the present level of initial funding, Start up operations are sufficiently funded for the start up phase, ongoing operations would leave a surplus from Year I at conservative level of expenses, and in a scenario of difficulties in achieving the projected number of registrations there is a sufficient contingency plan to bring in additional capital from family sources as also raise debts if necessary from private sources.

iii) sources of funding include funds from the founder, family funds which are supplemented by a Domain Industry establishment which partially provides the initial funding at the application stage. Post application, potential investors would include Domain businesses, venture capitalists and a larger circle of family and friends. Nameshop would also make use of some additional family funds to be made available to the founder in the near future.

iv) There would be significant change in the scale of operations post funding.

v) As explained earlier, Nameshop has deferred discussions with potential investors due to a cautious unwillingness to disclose the string applied for at the application stage, but has broadly discussed with some investors who are inclined to consider investments after more information is disclosed.

---

**48(b). Describe anticipated ranges in projected funding and revenue. Describe factors that affect those ranges.**

As referenced throughout this application, we have contracted with Afilius for back-end registry services, who has over a decade of experience managing TLDs. This knowledge was leveraged to produce a technical plan that was consistent with the needs of our business model. Our contract with Afilius is such that any change in the level of registrations only affects the variable costs per domain paid to Afilius; there is no escalator clause that would

result in this fee being greater than the agreed upon schedule. This fee structure has a minimum cost per financial transaction and this represents the entire fee paid to Afiliias for handling all of the technical operations of the Registry including 4 of the 5 critical registry functions (excludes escrow).

---

**49(a). Contingency Planning: describe your contingency planning: identify any projected barriers to implementation of the business approach described in the application and how they affect cost, funding or timeline in your planning. Identify any particular regulation, law or policy that might impact the Registry Services offering. For each contingency, include impact to projected revenue and costs for the 3-year period presented in Template 1.**

If not a barrier, some difficulties are foreseen in competing for special attention from the Top Registrars in a scenario where there will be more than thousand new TLDs competing for front page listing. However the applicant believes that the applied for string satisfies a definite need of the Registrants, so with subsequent phases of financial scaling up, the company plans to undertake targeted advertising through social networks to create awareness among users about the usefulness of the applied for string.

For any shortfalls in cash flow for the first three years, the contingency plan is to bring in additional funds from family as also raise short term debts from friends and relatives.

---

**49(b). Describe your contingency planning where funding sources are so significantly reduced that material deviations from the implementation model are required. In particular, how will on-going technical requirements be met? Complete a financial projections template (Template 2) for the worst case scenario.**

Worst Case projections are based on the scenario of insufficient results for the given level of initial efforts in building up the initial volume. Nameshop is committed to sustain operations even in the event of set backs by bridging the cash flow gap with short term debts from known sources.

As explained earlier, the investments in his firm at this application stage is at a conservative level, more funds are to be raised post-application, and for contingencies, the founder would introduce funds from family that would be made available. The founder is also in a position to raise long term debts from friends and relatives. The chances of reduced funding for the projected level of operations is minimal.

Even in this worst case scenario, a sum of US \$ 50,000 is sufficient as debt for a 3-5 year term to sustain operations and the applicant is in a position to raise debts, bring in his own capital without taking into consideration the funds possible from other operations such as Web Design and Web Hosting undertaken in the Business Name InternetStudio.

---

**49(c). Describe your contingency planning where activity volumes so significantly exceed the high projections that material deviation from the implementation model are required. In particular, how will on-going technical requirements be met?**

The applicant has considered such positive scenarios and with a view to be prepared for volumes of several million registrations, opted to work with Afiliias even as a Start Up. The overall Registry Service functions are fully entrusted to Afiliias, who as a Registry Service Provider has a scalable infrastructure to handle technical requirements for us even in a scenario where the volumes exceed that of the existing TLDs with top registrations volumes.

The applicant is in a position to consult with experts from the Domain Industry and from the ICANN Community to ensure that the business of this TLD is not only technically serviced well with significant increases in activity volumes, but also ensure that the activities are commercially ethical and confirm to Internet Community values as the space expands.

The applicant's business plan is to build up this TLD space as a global TLD, with alternate business models that require some discussions with the Registry Service Provider and potential associates. These discussions are to be taken up post-application and the applicant wishes to present the details at a later date.

---

**50(a). Continuity: Provide a cost estimate for funding critical registry operations on an annual basis. The critical functions of a registry which must be supported even if an applicant's business and/or funding fails are:**

- i) DNS resolution for registered domain names;**
- ii) Operation of the Shared Registration System;**
- iii) Provision of Whois service;**
- iv) Registry data escrow deposits; and**
- v) Maintenance of a properly signed zone in accordance with DNSSEC requirements.**

**List the estimated annual cost for each of these functions (specify currency used).**

50a: Cost of critical registry functions

The projected cash outflows for the five critical registry functions are approximately \$6000. This amount represents the cost per year of maintaining essential registry functions while remaining in full compliance with all ICANN-mandated RFCs.

This estimate of the cost for a minimal registry services subcontractor has been evaluated by Afilias, a global registry services provider. Over the past decade, Afilias has launched and transitioned generic, restricted, established, and ccTLDs and currently provides critical registry services and other registry support for 20 million domains. This experience affords Afilias unique insight into both the minimum requirements for operating a small TLD and full requirements for managing a large, open TLD.

This estimate is an approximate cash outflow for minimum, critical registry functions only and does not include the full range of resources, services, expertise, and advanced capabilities that will be provided by Afilias in supporting this TLD. The estimate above is commensurate with the technical, operational, and financial approach described in this application. The cost of the COI is tied to the amount sufficient for ICANN to protect the registrants of this TLD through a third-party Emergency Back End Registry Operator (EBERO) delivering necessary registry functions for a limited time in the unlikely events of a failure of the Applicant or insufficient funding. Afilias has arrived at upper and lower ranges of reasonable costs for a third party providing critical infrastructure and essential activities associated with an EBERO registry.

To determine the costs for an EBERO provider, Afilias has analyzed data that includes observed costs. The data has been analyzed using standard industry practices based on accrual accounting appropriate to this exercise. Adjustments were made for non-recurring items and capital expenditures, which could not realistically be excluded when operating a registry over an extended period of time. The estimate also does not include the cost of transitioning the registry. Where possible, the component costs of individual registry functions have been tracked. However, due to the interrelated nature of critical registry services, this is not always possible. For example, DNSSEC is an incremental cost of basic DNS resolution. Also, WHOIS costs have significant overlap with the SRS. Ranges of volume in daily DNS, DNSSEC, and WHOIS queries as well as EPP transactions were captured in the historical operating data.

Essential costs that cannot be attributed to a specific function have been allocated across the various functions using either a straight-line method, weighted by function, weighted by query, or some other weighting relevant to the particular line item cost. Resources required to meet SLA, web-based, and port-43 performance metrics have been included. Data escrow, as an external function, has been estimated by the fees paid for this service as well as internal costs to the registry service providing the data.

Afilias has also estimated these costs, where possible, for individual TLDs to provide a scalable model for critical registry functions based on the number of domains registered. Afilias' several TLDs represent a broad range of sizes in domain registrations and query rates. This cross-section of the estimates provides a model that has been used to calculate the COI for this TLD and accounts for the incremental costs associated with various levels of query responses. Based on estimates presented in this proposal and their associated query rates, we expect the costs for a third-party EBERO provider, operating for a limited period of time, to be distributed across the critical



functions according to the chart below:

Most Likely  
Critical Registry Function Costs

	Yr 1	Yr 2	Yr 3		
DUMs	2,500	3,000	3,300		
Operation of SRS		\$2,145	\$2,145	\$2,145	
Data Escrow (Internal)		\$351	\$351	\$351	
Provision of Whois		\$273	\$273	\$273	
DNS Resolution for Registered Domain Names		\$858	\$858	\$858	
Maintenance of Zone in Accordance with DNSSEC		\$273	\$273	\$273	
Total Critical Registry Functions (EBERO)			\$3,900	\$3,900	\$3,900
Data Escrow	\$500	\$500	\$500		
Total Critical Registry Function Costs		\$4,400	\$4,400	\$4,400	

---

**50(b). Applicants must provide evidence as to how the funds required for performing these critical registry functions will be available and guaranteed to fund registry operations for a minimum of three years following the termination of the Registry Agreement**

The applicant has calculated that US \$ 18000 is required for continuity of operations and would deposit this amount in an escrow account as specified.

---



# New gTLD Financial Assistance Form

Public Component for  
Financial Assistance  
Application (Criteria 1)

**Version 2012-01-11**





Application ID:

---

### **Public Component ( Criteria 1 ) - Questions**

Candidates will receive points as indicated below for demonstrating each of the following public interest criteria. Candidates should indicate on their application for funding support which criteria they believe their application meets. Candidates do not need to meet all criteria to meet the threshold or qualify for financial assistance, but priority will be given to those who are scored the highest.

**Nine points is the maximum, and a minimum of five points is required.**

Please refer to the New gTLD Financial Assistance Handbook for instructions on how to complete this form.

**Enter your Application ID below:**

Application ID: 1-1873-71868

### Community based project

The New gTLD Applicant Guidebook specifies that each applicant must declare if its application is a community-based project. Applicants for financial support that also have indicated that a project is community-based will be evaluated by the Support Application Review Panel (SARP) teams against the four Community Priority evaluation criteria found in [Module 4 of the New gTLD Applicant Guidebook](#): community establishment, nexus between proposed string and community, registration policies, and community endorsement. Rather than following the strict scoring methodology in the New gTLD Applicant Guidebook, the SARP will perform a high-level review to determine whether the applicant generally meets those criteria. Applicants that generally meet the criteria in the four tests will be given 1 point. Applicants that do not meet this threshold will receive 0 points.

**1**

It is important to note that while the SARP and the ICANN New gTLD Evaluation Panels are using similar criteria in certain cases, the SARP's objective is to identify those applicants most worthy of financial support to help reduce barriers to entry for the ICANN application process, not to evaluate an applicant's New gTLD Application. Some applicants that receive funding support may not ultimately be successful with their New gTLD Applications. Given that the SARP's priority is to identify those candidates that meet public interest priorities and not to address a contention set, the SARP will be given instructions to be more liberal in its interpretation of the Community Based priority criteria. In this regard, SARP findings related to community-based projects may be somewhat inconsistent with the Guidebook described Community Priority Evaluation that the financial aid applicant may later face.

**Question:** How does your application serve your community?

This question is meant broadly to address how the applicant is proving service to its relevant group of users. It is possible, but it is not required that the application is designated as a community TLD as defined in the New gTLD Applicant Guidebook.

Maximum Points: 1

The string applied for, .IDN (an ascii gTLD) bridges IDN users across language communities. This ascii TLD is offered to the Internationalized Domain Name Registrants as a supplementary, optional domain name as an an ascii TLD representation of the Internationalized Domain Name registered by the Registrant.

Registrants of Internationalized Domain Names are visible within their language community, but across communities, it requires a way of communicating the internationalized domain name to other language communities.

The applied for string, .IDN bridges this gap. As an additional TLD registered by the Internationalized Domain Name user, this ascii TLD could be communicated as an ascii representation of the Internationalied Domain Name that is set up to point to the Internationalized Domain Name.

With these benefits the applied for string offers an invaluable service to the community of IDN registrants.

<b>2</b>	<b>Public interest benefit including support for distinct cultural, linguistic or ethnic communities</b>
	<p>The Applicant Support Program targets those applications that provide benefit to the public interest. These are applications that support distinct cultural, linguistic or ethnic communities, as well as communities with a defined social need. Applications that demonstrate a benefit to the public interest, enhance the public good, or promote the general welfare will be given priority. Applicants who meet the community-based application threshold might also receive points under this criterion. However, some applicants not designating their applications as community-based applications might still offer benefit for a distinct cultural, linguistic or ethnic community. For example, this might include groups with geographically dispersed diasporas or linguistic minorities. Applicants who demonstrate how their project will benefit such communities and serve the public interest will receive 1 point.</p>

Applicants may provide documentation already prepared to support their answer to Question 18 (Mission/Purpose) in the ICANN New gTLD Application, but may also provide supplemental documentation as appropriate.

**Question:** How does the proposed gTLD demonstrate benefit to the public interest, enhance the public good or promote the general welfare of the expected beneficiary community? Describe the public interest benefit of your gTLD. Answers should address (among others) the following points:

- What is the mission/purpose of your proposed gTLD?
- Will the proposed gTLD support distinct cultural, linguistic or ethnic communities (e.g., groups with geographically dispersed Diasporas or linguistic minorities protected by certain treaties) or communities meeting a defined social need?

Maximum Points: 1

The purpose of the proposed gTLD is to offer a bridge for the Internationalized Domain Name Registrant to connect to users beyond their own language communities. This gTLD would be of help in furthering the Internet Community's efforts to preserve the Internet as a unified, Global space.

The proposed gTLD .IDN supports multiple cultural, linguistic and ethnic communities across the world by helping communities connect to the rest of the world across the barrier of language.

**Service in an under-served language, the presence of which on the Internet has been limited**

Candidates applying for a string that is providing build-out of a language or script whose web presence is limited will be given priority for funding support. This may include smaller script communities whose scripts are very limited on the web and communities that regularly use more than one script but might otherwise face challenges with the build out of two scripts. Applicants that provide data or other documentation demonstrating the lack of presence of their language on the Internet and how their project will support that language presence will receive 1 point.

**3 Question:** Does the proposed gTLD offer service in an under-served language, the presence of which on the Internet has been limited?

If Yes, how? You should include answers to (a), (b) and (c) below:

- a) Identify the language
- b) Provide data or evidence of the limited presence of this language on the Internet.
- c) Describe how the proposed project will support or improve that language presence, including whether and in what ways outreach and communications will help to achieve your projected benefits.

Maximum Points: 1

The proposed gTLD, .IDN is intended to serve users of various different languages, irrespective of whether the presence of the language is wide or global. Even if the language or script is completely unfamiliar to the global user, the global user will find it easier to decipher the internationalized domain name in a script completely unfamiliar to him or her.



<b>Operation in a developing economy</b>	
<b>4</b>	<p>Applicants from developed countries may apply, but priority will be given to those from developing economies. Evaluation will be based on the expected service to public interest and the beneficiary community of the project and not the location of the back-end operations. Applications from and benefitting Least Developed Countries (LDCs), Landlocked Developing Countries (LLDCs), and Small Island Developing States (SIDS) based on the listing of the United Nations Department of Economic and Social Affairs (UNDESA) will receive 2 points. Please see <a href="http://www.unohrls.org/">http://www.unohrls.org/</a> for the list of countries in these categories. Applications from and benefitting indigenous peoples as described in Article 1 of Convention No. 169 of the International Labour Organization and the UN Declaration on the Rights of Indigenous Peoples will receive 2 points. Applications from and benefitting those from the UNDESA list of Developing Countries, who are not LDCs, LLDCs or SIDS, will receive 1 point. Applicants from all other (developed) countries and who are not Indigenous Peoples will receive 0 points.</p> <p><b>Question:</b> What is the geographic location of the applicant, and what is the geographic location of the primary expected beneficiary community? How does the gTLD benefit the geographic community indicated?</p> <p>Maximum Points: 2</p>
	<p>The geographic location of the applicant, Nameshop is India, the geographic location, country of birth and country of residence of the Founder and Proprietor of Nameshop is India.</p> <p>The proposed gTLD, .IDN serves language communities across the world, but well over 3 billion users of these beneficiaries reside in developing countries.</p> <p>The applied for string is from an applicant from a developing country, for the benefit of users largely from developing countries.</p>



Application ID:

---

<b>5</b>	<p style="text-align: center;"><b>Advocated by non-profit, civil society and/or non-governmental organizations in a manner consistent with the organizations' social service mission(s) (0-1 points)</b></p> <p>An applicant may demonstrate benefit to the public interest through support for their project from local or partner organizations such as non-profit, civil society, and/or non-governmental organizations. Applicants may meet this requirement by providing letters of support from such organizations that indicate how the proposed project would further the organization's social service mission or benefit the public interest; or evidence of gTLD project partners or donors/funding sponsors whose mission is aligned with the public interest.</p> <p><b>Question:</b> Has your project received endorsement from non-profit, civil society and/or nongovernmental organizations in a manner consistent with the organizations' social service mission(s)?</p> <p>If yes, provide a listing of the organizations along with an overview of the type of endorsement. Letters of support from identified organizations should validate assertions. Documentary evidence of funding support or partnership arrangements should be provided.</p> <p>Maximum Points: 1</p>
<p>The string applied for has been kept confidential at the application stage, and has not been publicly revealed so far. Post application, after ICANN announces the strings applied for, the applicant would reach out for endorsements by a few non-profit and civil society organizations as also from language communities.</p>	



Application ID:

---

**Operation by a not-for-profit organization****6**

Priority will be given to entities that are not formed as conventional for-profit businesses – i.e., non-governmental organizations, non-profit entities, civil society organizations, foundations, trusts, mission-based organizations, etc. Non-profit organizations and similarly organized entities are eligible for 2 points; other organizations such as public-private partnerships, and hybrid entities (e.g. those that are profit/non-profit) are eligible for 1 point.

**Questions:** Is the applicant formed as a not-for-profit organization?

Is the applicant formed as a public-private partnership or other hybrid entity?

Maximum Points: 2

No, the applicant is not formed as a not-for-profit entity, but the applicant is inclined to set aside a certain portion of the income from operations to help further the efforts of the Internet Community to preserve the Internet as a free and open, unified global space.



Application ID:

---

**Operation by a local entrepreneur or not-for profit organization in a developing economy providing demonstrable social benefit****7**

While the Applicant Support Program is not intended to be used as a substitute for addressing conventional business risk, there is value in providing some support to entrepreneurs or non-profit organizations from developing countries whose project provides a demonstrable social benefit but who are unable to execute their project without funding support. The applicant can demonstrate that its project will provide social benefit including, but not limited to: (1) providing investment in the skill base of the target community; (2) fostering gender balance and the presence of minorities in the target community; (3) providing a positive contribution to the national or regional economy of its operation. Applicants will receive 1 point if able to document such social benefits.

**Question:** Is the applicant a local entrepreneur or not-for profit organization in a developing economy providing demonstrable social benefit? Provide a description and any supporting documentation to demonstrate how the project will provide social benefit.

Maximum Points: 1

Nameshop will operate from India, and would engage Technical and Marketing staff from India. As this TLD space expands, there could be significant direct and employment opportunities created and Nameshop could be of some value to the Nation's economy. The applicant is also inclined to further gender balance in the employment opportunities to be generated.



Application ID:

---





# New gTLD Financial Assistance Form

Confidential Component  
for Financial Assistance  
Application (Criteria 2 &  
3)

**Version 2012-01-11**

Application ID:

---

### **Financial Need Criteria**

A maximum of 5 points is possible on the Financial Need criteria. Applicants will be required to submit materials to detail various constraints that affect their ability to acquire and implement a gTLD without assistance.

### **Financial Capabilities Criteria**

A maximum of 2 points is possible on the Financial Capabilities criteria. Applicants are asked to submit materials to demonstrate basic financial capabilities to operate an ongoing concern of the size and complexity of a proposed registry, as well as past experience doing so.

Please refer to the New gTLD Financial Assistance Handbook for instructions on how to complete this form.

### **Enter your Application ID below:**

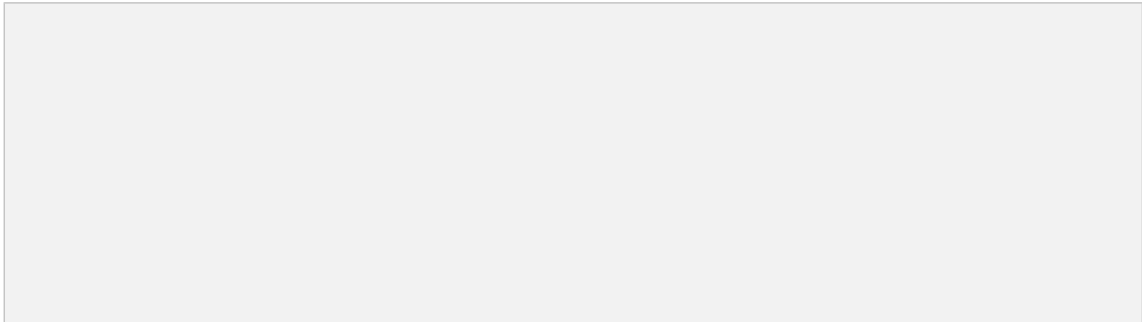
Application ID: 1-1873-71868

## Financial Need (Criteria 2)

	<b>Operational environment</b>
<b>1</b>	<p>A complete answer demonstrates why the applicant may have limited access to funding and specific environmental factors that have caused constraints to raising initial capital to pay for fees. The applicant may provide letters from other funding organizations that have considered requests for support on this or other efforts. A response will merit a 2 if its assertions are substantiated with documentation specific to the gTLD project application and its lack of ability to raise funds for the evaluation fee or other initial expenses. A response will merit a 1 if the applicant generally describes a challenging operational environment, but does not have documentation specific to the financial aspects of its project. A response that does not provide adequate justification for why its operational environment poses a challenge to raising the financial capital to support its application or project is given 0 points.</p> <p><b>Question:</b> Provide a description of any constraints that affect your ability to successfully apply for and operate a gTLD without financial assistance.</p> <p>Maximum Points: 2</p>
<p>Nameshop is based in India, where the banking and financial community is more inclined to fund ventures with traditional business models, and calculated risks, even in the the technology sector. The new gTLD business opportunities are relatively unfamiliar to the average Indian investor or banker.</p> <p>The applicant requires funding support as a businessman venturing into business after a ten year interruption in his career in business.</p>	

Application ID:

---



<b>Organizational size</b>	
<b>2</b>	<p>Small and medium-sized organizations often face specific challenges in obtaining sufficient human and financial resources to carry out their business or organizational mission. Moreover, these organizations may face disproportionate costs in meeting the administrative burden required by completing the New gTLD Program Application. To help address this barrier, the Applicant Support Program will give priority to small and medium sized organizations when evaluating applications. Small and medium sized organizations, not associated with a larger parent entity, will be given 1 point.</p> <p><b>Question:</b> Is the applicant a small or medium-sized organization, not associated with a larger parent organization? Maximum Points: 1</p>
<p>Yes. Nameshop is a Start Up, a Proprietary form of business, with a very limited capital, not associated with or part of a medium or large business entity.</p>	

### Project budget and funding resources

**3**

In order to complete the New gTLD Program Application, the applicant must provide financial projections that demonstrate a sustainable business (even if break-even is not achieved through the first three years of operation). Applicants to the Applicant Support Program should provide a narrative to correspond with their Financial Projections and their description of funding and revenue sources to identify where ICANN financial support would assist in ensuring sustainable operations or mitigating any projected risks. Applicants should provide tabular information on operational expenses and other relevant data that is also provided in their New gTLD Application. Applicants may also include letters from donors who may be promising project funding if the New gTLD Application is successful, but which may point to a lack in the initial start up funding to pay the USD 185,000 application fee. Applicants who clearly identify why financial support would help to improve their financial projections or mitigate any potential risks will be given 1 point. Applicants whose financial projections exhibit funding needs (or whose projections demonstrate inadequate start-up capital and three years of sustainable operations) will be given 0 points.

**Question:** Describe why funding support from ICANN would assist in ensuring sustainable operations of your project or mitigating any risks. The answer should correspond with your Financial Projections and description of funding and revenue sources.

Maximum Points: 1

Funding support in the form of reduced fees makes the business of new gTLDs accessible and affordable. Without funding support, this opportunity is out of reach for Nameshop as a small Start Up. The funding support would help the company get started and the Applicant is confident that the required funding could be raised at growth stage in the national and international environment.

Application ID:

---

<b>Outreach for financial support</b>	
<b>4</b>	<p>Applicants that have taken the extra steps to seek additional funding or create partnerships that could lead to additional support such as through matching grants or guaranteed loans or payments will be considered for an additional point. The applicant may provide letters from other organizations that have considered requests for support on this or other efforts. A response will merit one point if its assertions are substantiated with documentation specific to this project, otherwise no points will be awarded.</p> <p><b>Question:</b> Have you sought financial support from other donors or partners through, e.g., grants, guaranteed loans, matching funds? These applications are additional evidence of need.</p> <p>If Yes, then provide a listing of any such organization and copies of responses received to funding requests.</p> <p>Maximum Points: 1</p>

Application ID:

---

No. Nameshop has not sought any other funds as grants or matching funds. However the firm has sought initial investments by a private offer.



## Financial Capabilities (Criteria 3)

<b>Basic financial capability to operate an ongoing concern of the proposed registry</b>	
<b>5</b>	<p>While an applicant's project should demonstrate some level of need as described above, the applicant must also demonstrate basic financial capability to operate an ongoing concern of the size and complexity of a proposed registry through demonstrating managerial capabilities and financial resources. Applicants should provide a summary of their qualifications consistent with answers to Questions 45-47 in the New gTLD Program Application section on basic financial capability. Applicants should provide emphasis on demonstrating their ability to manage an organization and finances relative to the size of their project. Those meeting the requirements are given 1 point. Those who fail these requirements are given 0 points.</p> <p><b>Question:</b> How is your organization set up financially to successfully operate a registry if financial support from ICANN and potentially others? The response should be consistent with information in the New gTLD Program Application.</p> <p>Maximum Points: 1</p>
<p>The applicant is in a position to bring in a certain level of funds as also in a position to raise funds from family sources and private investors. With a strategy to operate conservatively before scaling up with more investments from a few more investors, the applicant has a clear and effective plan to sustain operations and grow.</p>	

**Previously executed projects****6**

Applicants with proven results in managing organizations and projects of this complexity in the past will be given priority. Applicants who provide documentation citing previously managed and operated programs will be given 1 point.

**Question:** Describe how you have executed against the budget of projects of comparable size, and complexity to your gTLD project? If yes, then provide a listing and short summary of such projects.  
Maximum Points: 1

Yes, I have founded and managed a Textile Company during the years 1997 - 2001 with operations that recorded average growth in excess of 50% over a 4 year period, with revenues to the tune of US \$ 1.5 million in year 2000 prices. I am a Business Management graduate, comfortable as an entrepreneur, and am competent enough to manage this gTLD project successfully.

**Nameshop**

389/1, PERUNDURAI ROAD, ERODE - 638 001.

Currency: INR

## INCOME AND EXPENDITURE ACCOUNT FOR THE YEAR ENDED 31.03.2011

To Bank Charges	2,450	Income	20,000
To Bank Postage	2,250		
To Net Profit	15,300		
Total	<u>20,000</u>		<u>20,000</u>

BALANCE SHEET AS ON 31.03.2011

## LIABILITIES


Capital	1,00,000
Add :	
Net Income from Income and Expenditure A/c	15,300

Total	<u>1,15,300</u>
-------	-----------------

## ASSETS

Printer	10,250
Web Hosting Account set up / other advances	48,880
Other Advances	28,798
Cash at Bank	2,448
Cash on Hand	24,924

Total	<u>1,15,300</u>
-------	-----------------

For Name Shop  
  
Proprietor



**Nameshop**

389/1, PERUNDURAI ROAD, ERODE - 638 001.

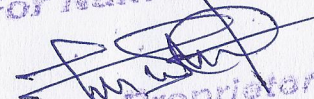
Currency: INR

**INCOME AND EXPENDITURE ACCOUNT FOR THE YEAR ENDED 31.03.2012**

To Bank Charges	3,834	By Web Design Service Charges	66,000
To Bank Postage	750		
To Bank Salary	27,099		
To Net Income	34,317		
Total	<u>66,000</u>		<u>66,000</u>

**BALANCE SHEET AS ON 31.03.2012**

<b>LIABILITIES</b>		<b>ASSETS</b>	
Capital	9,35,972	Printer	10,250
<b>Add :</b>		Web Hosting Set up and related advances	48,880
Net Income and Expenditure A/c	34,317	Other Advances	28,798
		Application fee to ICANN New G.T.L.D	2,57,400
		Sundry Debtors	66,000
		Cash at Bank	2,917
		Cash on Hand	5,56,044
Total	<u>9,70,289</u>		<u>9,70,289</u>

For Name Shop  
  
Proprietor



The Internet Corporation for Assigned Names and Numbers

11 March 2013

Mr. Sivasubramanian Muthusamy  
Nameshop  
389/1 Perundurai Road  
Erode  
Tamilnadu 638011  
India

Re: Support Applicant Review Panel's Determination for Application ID 1-1873-71868

Dear Mr. Sivasubramanian Muthusamy:

Thank you for your participation in the New gTLD Applicant Support Program.

The Support Applicant Review Panel (SARP) has completed its financial assistance review. This letter serves as your official notification from ICANN regarding the Panel's determination for application ID 1-1873-71868.

After careful consideration and extensive review performed against the criteria outlined in the New gTLD Financial Assistance Handbook, the SARP determined that your application did not meet the following minimum requirements to qualify for financial assistance:

**Criteria 1: Public Interest Benefit**

- Community-based project
- Public interest benefit
- Service in under-served language
- Advocated by non-profit, civil society, or NGO (outside support)
- Operation by not-for-profit
- Operation by local entrepreneur

**Criteria 2: Financial Need**

- Operational environment
- Project budget and funding sources
- Outreach for financial support





Criteria 3: Financial Capabilities

- Basic financial capability
- Previously executed projects

Due to this determination, your application is ineligible for further review under the New gTLD Program and the evaluation fee amount of USD 47,000 will be refunded as stated in the Financial Assistance Handbook.

If you have any questions regarding this communication, please contact the Customer Service Center at [newgtld@icann.org](mailto:newgtld@icann.org).

Sincerely,

A handwritten signature in black ink, appearing to read "Christine Willett", is written over a light blue horizontal line.

Christine Willett  
Vice President, gTLD Operations  
Internet Corporation for Assigned Names and Numbers

Welcome to the New gTLD Customer Service Portal!

[Home](#)[Contact Us](#)[Logout](#)

**Users: Appeal against this decision on Applicant support request.**

[Back](#)

**Subject:** Appeal against this decision on Applicant support request.

**Note:** Hello, Thank you for informing me of the results of the Applicant Support program. The information I have is that the application did not meet the criteria, but did not specify which of the criteria was unmet by the the application. I wish to submit a request for this information as also an appeal for reconsideration. Please also note that I have also submitted a review request for a decision on the string change request on this application. In view of these requests, please do not initiate, from your end, any process to close this application. Thank you Sivasubramanian M Proprietor Nameshop

**Attachment:**

© 2004-2011 [SugarCRM Inc.](#) All Rights Reserved.

POWERED BY  
**SUGARCRM.**



## New gTLD Application Change Request Form

Application ID:	<b>1-1873-71868</b>
Applying Entity:	Nameshop
Applied-for TLD:	IDN
Primary Contact Name:	Sivasubramanian M
Primary Contact Email:	<a href="mailto:isolatednet@gmail.com">isolatednet@gmail.com</a>
Primary Contact Phone No:	+919952403099
Reason for the change request:	<p>Nameshop has applied for the string .IDN as an ASCII string. During the ICANN meeting in Prague, it was pointed out that this string could be viewed as confusable at the country level due to the fact that this is alpha3 country code.</p> <p>The applied for string, .IDN is in the generic, global TLD space, and not a geoTLD, and not intended for country level operations. This is an ASCII TLD for the benefit of idn.idn registrants worldwide. Though not filed as a Community TLD, it is a TLD with a larger Community purpose, as the idea and purpose of .IDN is to offer a bridge for the Internationalized Domain Name Registrants to connect to users beyond their own language communities.</p> <p>The proposed gTLD, .IDN supports multiple cultural, linguistic and ethnic communities across the world by helping communities connect to the rest of the world across the barriers of language. This gTLD is intended to serve users of different languages, irrespective of whether the presence of the language is wide or global. Even if the language or script is completely unfamiliar to the global user, with a .IDN ASCII string mapped to the idn.idn name, the global user will find it easier to decipher the internationalized domain name in a script completely unfamiliar to him or her.</p> <p>While Internationalized Domain Names enable users to connect within their language communities locally, the proposed gTLD would connect users from different communities to connect globally. This gTLD would be of help</p>



in furthering the Internet Community's efforts to preserve the Internet as a unified, Global space.

The Applicant Guide book, under section 'Policy Requirements for Generic Top Level Domains' III 3.1 states that "Applied-for gTLD strings in ASCII must be composed of three or more visually distinct characters. Two- character ASCII strings are not permitted, to avoid conflicting with current and future country codes based on the ISO 3166-1 standard." In this section, III.3.1. on what is not permitted, there is no mention of alpha 3 country codes, while this section unambiguously reserves two character ISO standard country codes.

Under the section on 'Geographic Names Review', 2.2.1.4 the guide book states that strings that are country or territory names will not be approved. Here, what is stated as "will not be approved" includes 2.2.1.4.1.i alpha-3 code listed in the ISO 3166-1 standard.

As an applicant applying for a generic ASCII string, that is not a Geographic String or Country Code for country level operations, the title "Geographic Names Review" appeared to be that of a section offering guidelines pertinent only to the applications for geographic names (strings), so the caution on alpha3 ISO codes was completely missed.

Nameshop as the applicant for .IDN has no intention of positioning this TLD in any manner as a country level TLD to cause any confusion whatsoever. I hope ICANN would take into account the fact that the string + idea + business model makes the application. Viewed together, .IDN is global, with a larger purpose and the idea as conceived to be implemented by a fair business model would indeed add enormous value to ICANN's new gTLD program in the area of IDN implementation.

The above has been represented to the new gTLD team with a copy to the Acting CEO on July 18, with the request to ICANN:

1. To consider .IDN for delegation, if the above details would satisfy the ccNSO and the GAC.

2. If there are difficulties, to allow the applicant to change the string to another string of three or more ASCII characters that is not reserved, not a country or territory name, uncontentious but represents the purpose of this TLD.

The applicant has also noticed objections in the comment process to ICANN allowing the applied for string on the grounds that it is an alpha3 country code for Indonesia. In deference of these objections, despite the belief that the request (1) stated above is in order on the grounds stated earlier, the applicant now wishes to opt for request (2) stated above, that of changing the string applied for to " another string of three or more ASCII characters that is not reserved, not a country or territory name, uncontentious but represents the purpose of this TLD"

Nameshop wishes to change the answer to question 13 a as "INTERNET" which suits the mission of connecting Internationalized Domain Name users to the Global Internet space.

The proposed change does not affect countries or geographic regions. The changed string confirms to the purpose of the application by nameshop, that of enabling IDN registrants to connect to the global Internet users from all other language communities.

----- begin Changes to the CONFIDENTIAL portion -----

The following note may please be recorded in the CONFIDENTIAL portion of the application, as the applicant does not wish to make a public announcement of this nature during the application phase:

**1. Management of .INTERNET**

The applicant intends to approach and invite three or more Internet Leaders of known commitment to Internet to be active and participative members of the Management Board to set directions for the management of the proposed TLD. This is to ensure that this string is managed responsibly, as benevolently as possible. They would seated together with other Management Board members with a focused Business perspective.

**2. Contribution to the growth and evolution of Internet and other good causes.**

Nameshop voluntarily wishes to set aside, year after year, one quarter of the Post Tax profits (or pre-tax profits if the Tax Laws allow a full tax exemption of contribution to such a cause) arising from registration of every .INTERNET domain name over and above a minimal base volume of registrations. This contribution is to be allocated and utilized largely to the decisions of the Board Members as proposed in (1) above. Name shop would be willing to execute written, legally binding commitments to ICANN to this effect. The funds so set aside are intended to be utilized for the good of the Internet, where possible, in areas where sufficient probono funds are not available. However the fund's management may have the flexibility to allocate and utilize funds for inadequately funded humanitarian causes- without any geographic discrimination - if sufficient funds for Internet causes are otherwise available.

The present constitution of the company as a Proprietary firm based in India allows room for formalizing these intentions with a new company structure, possibly by including a foundation created for this purpose as a shareholder or partner admitted to the benefits of business, free of liabilities.

---- end of Changes to CONFIDENTIAL portion ----

---

## Request for Changes to Application number: 1-1873-71868 by Nameshop

---

### Applied-for gTLD string

---

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

*The answer(s) exactly as entered in TAS:* IDN

***Changes that you would like to make to these answers in tracked changed***

~~IDN~~ INTERNET

---

There are no substantive changes to any other answer to the applications. Change to the answer to Question 13 does not substantially alter the responses to the answers to other questions by way of commitments made and arguments presented.

However, the references to the applied for string as “IDN” changes to “INTERNET” wherever “IDN” is mentioned as the applied for string in some sections of the application, for instance as in the answer to Question 18 shown below:

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

The purpose of the proposed gTLD is to offer a bridge for the Internationalized Domain Name Registrant to connect to users beyond their own language communities. This gTLD would be of help in furthering the Internet Community's efforts to preserve the Internet as a unified, Global space.

The proposed gTLD ~~.IDN~~.INTERNET supports multiple cultural, linguistic and ethnic communities across the world by helping communities connect to the rest of the world across the barrier of language.

---

**18(b). How proposed gTLD will benefit registrants, Internet users, and others.**

i) The proposed gTLD ~~.IDN~~.INTERNET supports multiple cultural, linguistic and ethnic communities across the world by helping communities connect to the rest of the world across the barrier of language.

ii) The proposed gTLD, ~~.IDN~~.INTERNET is intended to serve users of various different languages, irrespective of whether the presence of the language is wide or global. Even if the language or script is completely unfamiliar to the global user, the global user will find it easier to decipher the internationalized domain name in a script completely unfamiliar to him or her.

iii) While Internationalized Domain Names enable users to connect within their language communities, the proposed gTLD would connect users from different communities to connect across communities.

iv) The applicant intends to follow ICANN policies by the book, and is inclined to take advice from Community Members to build up this TLD space as one with high ethical standards.

v) Nameshop would follow the recommendation of the Community whois working groups and ICANN whois policy and privacy policies to protect the privacy and confidential information of the users.

The proposed registry would engage communication experts from various regions in its effort to reach the benefits of this TLD to users across language communities.

---

# nameshop

*gTLD String: .IDN with a change request for .INTERNET*

*Applicant Entity Name: Nameshop*

*Application ID#: 1-1873-71868*

## SPECIFICATION 11

### PUBLIC INTEREST COMMITMENTS

*1. Nameshop, the Registry Operator will use only ICANN accredited registrars that are party to the Registrar Accreditation Agreement approved by the ICANN Board of Directors during 2013 (or any subsequent form of Registrar Accreditation Agreement approved by the ICANN Board of Directors) in registering domain names. A list of such registrars shall be maintained by ICANN on ICANN's website.*

*2. Nameshop, as Registry Operator will operate the registry for the TLD in compliance with all commitments, statements of intent and business plans stated in the following sections of Registry Operator's application to ICANN for the TLD, which commitments, statements of intent and business plans are hereby incorporated by reference into this Agreement. Registry Operator's obligations pursuant to this paragraph shall be enforceable by ICANN and through the Public Interest Commitment Dispute Resolution Process established by ICANN, as it may be amended by ICANN from time to time, the "PICDRP"). Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Registry Agreement) following a determination by any PICDRP panel and to be bound by any such determination.*

The string .INTERNET, changed from the originally applied for string .IDN, though not filed as a Community TLD, is a TLD with a larger Community purpose, as the idea and purpose of the proposed TLD is to offer a bridge for the Internationalized Domain Name Registrants to open up their Web spaces for users beyond their own language communities. The string was applied for with the idea of a business plan to offer this domain extension to the registrants of various IDN domain names as an additional ASCII domain name that would point to their IDN space, which is otherwise a space with a domain name in a local script, not intelligible, hence out of reach for those outside their language space. The .INTERNET string is so applied for, with the larger purpose of building global Trust over IDN domains and making web spaces with IDNs accessible across their local scripts thereby contributing to the Internet Community's efforts to keep the Internet as One Internet as a global space. Nameshop hereby commits to operate .INTERNET in a manner that this purpose is central to the operation of this TLD.

Nameshop also wishes to reaffirm it's commitments to implement this string responsibly, with Community Advice where possible.

*3. Nameshop, as the Registry Operator agrees to perform following specific public interest commitments, which commitments shall be enforceable by ICANN and through the PICDRP. Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and*

*adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Registry Agreement) following a determination by any PICDRP panel and to be bound by any such determination.*

## 1. Management of .INTERNET

The applicant intends to approach and invite three or more Internet Leaders of known commitment to Internet to be active and participative members of the Management Board to set directions for the management of the proposed TLD (**by an arrangement that is free of any legal commitments on their part**). This is to ensure that this string is managed responsibly, as benevolently as possible. They would seated together with other Management Board members with a focused Business perspective.

## 2. Contribution to the growth and evolution of Internet and other good causes.

Nameshop voluntarily wishes to set aside, year after year, one quarter of the Post Tax profits (or pre-tax profits if the Tax Laws allow a full tax exemption of contribution to such a cause) arising from registration of every .INTERNET domain name over and above a minimal base volume of registrations. This contribution is to be allocated and utilized largely to the decisions of the Board Members as proposed in (1) above. Name shop would be willing to execute written, legally binding commitments to ICANN to this effect. The funds so set aside are intended to be utilized for the good of the Internet, where possible, in areas where sufficient probono funds are not available. However the fund's management may have the flexibility to allocate and utilize funds for inadequately funded humanitarian causes- without any geographic discrimination - if sufficient funds for Internet causes are otherwise available.

3 The present constitution of the company as a Proprietary firm based in India allows room for formalizing these intentions with a new company structure, possibly by including a foundation created for this purpose as a shareholder or partner admitted to the benefits of business, free of liabilities. Nameshop hereby commits to formalize this commitment by a legally binding agreement with the Public Interest oversight mechanism of ICANN, if one is so created and designated by any name, or confirm to any other process formulated by ICANN for oversight of Public Interest Commitments.

4. Nameshop also commits to modify this commitment suitably to address any possible gaps in the language of this expression.

5. Namehsop would also build in clauses for continuity of these commitments after any minor or major change in the company structure of Nameshop, after any minor or major change in the shareholders of Nameshop by designating the 25% commitment to Global Public Interest as specified above, as an unchangeable commitment, as permanent as legally possible.

6. Further, the present Proprietor of Nameshop commits to utilize, over and above the 25% of the total already committed, at least one half of his share of income from the operations of .INTERNET on investments / business pursuits in the Internet space, with a similar clause to set aside at least one quarter of the income to the same foundation.

Sivasubramanian M  
Proprietor  
March 05, 2013



The Internet Corporation for Assigned Names and Numbers

Sivasubramanian M  
Nameshop

1 November 2012

**Re: Conflict between “IDN” and the ISO 3166-1 standard**

Dear Sivasubramanian M,

Thank you for your communication regarding the New gTLD Applicant Guidebook, and the applicability of the prohibitions contained within for country codes.

In order to create a process whereby ICANN is not in the position of deciding which countries and other geographic codes are afforded special protections, the Applicant Guidebook's provisions rely on a number of internationally recognized standards that define which terms are considered geographic names. The precise definitions are described in section 2.2.1.4 of the Applicant Guidebook, available at <http://newgtlds.icann.org/en/applicants/agb>.

Your request that the string “.IDN” not be considered a geographic name conflicts with the reservation of that three-letter string in ISO 3166-1 as a code representing “Indonesia” as you have also noted in your communication.

Broadly, the reservations in the new gTLD program regarding country names and country codes reflect the principle that meaningful representations of countries could be potentially used to represent country-code top-level domains, and there is ongoing work within the ICANN Country Codes Name Supporting Organization (ccNSO) regarding potential new definitions of what constitutes a ccTLD. So as not to introduce a potential conflict with future ccTLDs, names and codes that may be eligible to be delegated as ccTLDs are not permitted to be applied for as gTLDs in this round. It is not possible to waive these restrictions during this round of new gTLD applications.

We would also like to acknowledge receipt of your request to change the applied-for TLD. ICANN takes all change requests seriously and will review your request carefully against the criteria published at <http://newgtlds.icann.org/en/applicants/customer-service/change-requests>. We will notify you once a determination has been made.

Thank you for your communication and your interest in the New gTLD Program.

Yours sincerely,

Kurt J. Pritz  
Chief Strategy Officer  
ICANN





The Internet Corporation for Assigned Names and Numbers

Nameshop  
Mr. Sivasubramanian Muthusamy  
Whitefield  
389/1 Perundurai Road  
Erode Tamilnadu 638011  
IN

Re: CSC Case Number 37809

This letter is to inform you that the request to change the applied for string from "IDN" to "INTERNET" for application ID: 1-1873-71868 has been rejected.

This change request was carefully evaluated based on the criteria described at <http://newgtlds.icann.org/en/applicants/customer-service/change-requests>.

As a reminder, evaluation fees may be refunded pursuant to Section 1.5.1 of the Applicant Guidebook.

Thank you for your cooperation and patience regarding this change request. Please let us know if you have any additional questions regarding the application.

Sincerely,

Christine Willett  
VP, gTLD Operations

Welcome to the New gTLD Customer Service Portal!

[Home](#)[Contact Us](#)[Logout](#)

## Users: appeal against the decision on the Change Request

[Back](#)

**Subject:** appeal against the decision on the Change Request

**Note:** Hello, Thank you for conveying the change request decision today. I wish to appeal against this decision. I am in the process of drafting a response to appeal against this decision and will submit this later this week. In the meantime please convey to the evaluation team that nameshop wishes to request a review. Also, I have not received any clarifying questions so far. If any question were posted, kindly point me to the case number. Thank you. Sivasubramanian M.

**Attachment:**

© 2004-2011 SugarCRM Inc. All Rights Reserved.

POWERED BY  
**SUGARCRM.**



Sivasubramanian M &lt;isolatedn@gmail.com&gt;

---

## Appeal against the ruling of new gTLD on the nameshop change request

---

Sivasubramanian M &lt;isolatedn@gmail.com&gt;

Wed, Feb 27, 2013 at 3:43 PM

To: fadi.chehade@icann.org, akram.atallah@icann.org, steve.crocker@icann.org

Cc: Desiree Miloshevic &lt;dmiloshevic@afiliias.info&gt;, Afiliias LaPlante' &lt;rlaplante@afiliias.info&gt;, Ram Mohan &lt;rmohan@afiliias.info&gt;

Dear Fadi Chehade,

Nameshop (<http://nameshop.in> NOT [nameshop.com](http://nameshop.com) which is misleading ) , with the 'company' structure of a Proprietary firm in India, has applied for the string .IDN. Though not filed as a Community TLD, it is a TLD with a larger Community purpose, as the idea and purpose of the proposed TLD is to offer a bridge for the Internationalized Domain Name Registrants to open up their Web spaces for users beyond their own language communities. The string was applied for with the idea of a business plan to offer this domain extension to the registrants of various IDN domain names as an additional ASCII domain name that would point to their IDN space, which is otherwise a space with a domain name in a local script, not intelligible, hence out of reach for those outside their language space. The .IDN string is so applied for, with the larger purpose of building global Trust over IDN domains and making web spaces with IDNs accessible across their local scripts thereby contributing to the Internet Community's efforts to keep the Internet as One Internet as a global space.

Post application Nameshop noticed that IDN was the alpha3 country code for Indonesia and that three letter alpha country codes are reserved. (The Applicant Guide book, under section 'Policy Requirements for Generic Top Level Domains' III 3.1 on what is not permitted, there is NO mention of alpha 3 country codes. It is only under the section on 'Geographic Names Review', 2.2.1.4 the guide book states that alpha-3 codes 'will not be approved'. But this section under the title 'Geographic Names Review' did NOT seem pertinent to the Nameshop Application which is NOT for a Geographic String, so the error occurred.)

Nameshop brought the situation to the attention of new gTLD, ccNSO and GAC and assured that as the applicant for .IDN has no intention of positioning this TLD in any manner as a country level TLD to cause any confusion whatsoever. With this and other explanations, the applicant requested ICANN

1. to consider .IDN for delegation, if the above details would satisfy the ccNSO and the GAC.
2. If there are difficulties, to allow [nameshop] to change the string to another string of three or more ASCII characters that is not reserved, not a country or territory name, uncontentious but represents the purpose of this TLD.

Despite the belief that the request (1) stated above is in order on the grounds stated earlier, the applicant presented the option for request (2) stated above, and a Change Request was filed to change the answer to question 13 (a) as "INTERNET" which suits the mission of connecting Internationalized Domain Name users to the Global Internet space and of contribution to the community's efforts to keep the Internet as One Internet. The changed string is not reserved, not a country or territory name, uncontentious, represents the purpose of this TLD. The Change Request was in conformity with the criteria specified for allowing changes:

### *1. Explanation – Is a reasonable explanation provided?*

The Change Request explained the grounds, and has explained that the requested change is fair.

### *2. Evidence that original submission was in error – Are there indications to support an assertion that the change merely corrects an error?*

. IDN is an alpha3 country code, but the Applicant Guide Book mentioned that alpha3 codes will not be approved only under a section titled 'Geographic Names Review' which appeared to be a section that was not pertinent to this string which is not a geographical name. So this error occurred. The applied for change is in order as it corrects the error in the choice of the string.

*3. Other third parties affected – Does the change affect other third parties materially?*

No other parties are affected, because .INTERNET is NOT a string applied for by any other applicant, the string is uncontested and it is not a Geographic name, so the requested change does not affect any other third party materially.

*4. Precedents – Is the change similar to others that have already been approved? Could the change lead others to request similar changes that could affect third parties or result in undesirable effects on the program?*

Nameshop is possibly the only applicant who in need of such an alpha3 code to be changed. Any other applicant who originally applied for alpha3 codes did not choose to apply for a change. As Nameshop is the only applicant making a request to change the alpha3 code to an alternate generic string that is not reserved. So there no other applicant in a similar situation under compulsion to change the string, so there would not be any undesirable effects on the program by allowing this alpha3 code to be changed to .INTERNET.

*5. Fairness to applicants – Would allowing the change be construed as fair to the general community? Would disallowing the change be construed as unfair?*

The requested change is fair to the general community because Nameshop seeks to replace a string that would otherwise affect a country's privileges with a generic string that represents the purpose of the TLD application. The requested change is fair as it enables the implementation of an ASCII TLD that would bridge IDN communities with other communities and contribute to the community's efforts to preserve the Internet as One Internet.

On the contrary, disallowing the change would indeed be construed as unfair, as it amounts to a breach of process of the change request process as also amounts to subjective judgement by the evaluation team, prejudicial to the overall ICANN process.

*6. Materiality – Would the change affect the evaluation score or require re-evaluation of some or all of the application? Would the change affect string contention or community priority consideration?*

The requested change does not materially affect the evaluation score or require a reevaluation of any other application. The changed string is uncontested and does not in any way affect community priority consideration.

*7. Timing – Does the timing interfere with the evaluation process in some way? ICANN reserves the right to require a re-evaluation of the application in the event of a material change. This could involve additional fees or evaluation in a subsequent application round. (AGB §1.2.7)*

This request for change was filed during September 2012, and it is still not late to allow this change and proceed in accordance with the priority drawn for this application - priority no 150.

This change request submitted on Sep 30, 2012 (attached)

On follow up new gTLD first sent a reply (attached) on Nov 2 to say that .IDN is not allowed, but the change request was under consideration. There was some administrative change in the new gTLD administration after this point of time. Later on February 19, a file (attached) was posted in the CRM which 'rejected' the change request without any reasons assigned.

I wish to appeal against this decision, for which reasons are not assigned, on the following grounds:

The Change Request is conformity with the criteria specified as shown above. New gTLD has rejected the Request without due consideration of:

- a) the merits of the overall purpose of this application
- b) the gaps in the Applicant Guide Book that are to be attributed to the error of choice of an alpha 3 string
- c) the merits of the Change Request as a fair solution, and
- d) the conformity of the Change Request to the criteria specified for change.

Nameshop also wishes to draw your attention to the facts that this is an application under an applicant support request, an application from a Developing country and an application of value to the IDN program.

Please reconsider this decision and allow this application to proceed in accordance with the priority of this application (No 150), also considering the fact that this string would serve its purpose better if delegated together with the early IDN strings.

Nameshop also wishes to reaffirm it's commitments to implement this string responsibly, with community advice where possible, as also commit to utilize a significant portion of profits on larger causes as specified in the change request, to which effect Nameshop would be executing Public Interest Commitments separately.

Thank you.

Sivasubramanian M  
Nameshop  
<http://nameshop.in>

----- Forwarded message -----

From: Sivasubramanian M <[isolatedn@gmail.com](mailto:isolatedn@gmail.com)>

Date: Wed, Jul 18, 2012 at 11:48 PM

Subject: Fwd: Application for dotIDN as an ASCII gTLD by Nameshop from India

To: [Cherine.Chalaby@icann.org](mailto:Cherine.Chalaby@icann.org)

Cc: [mike.silber@icann.org](mailto:mike.silber@icann.org), Bertrand de La Chapelle <[bdelachapelle@gmail.com](mailto:bdelachapelle@gmail.com)>, Sebastien Bachollet <[sebastien.bachollet@icann.org](mailto:sebastien.bachollet@icann.org)>, Afiliias LaPlante' <[rlaplante@afiliias.info](mailto:rlaplante@afiliias.info)>, Desiree Miloshevic <[dmiloshevic@afiliias.info](mailto:dmiloshevic@afiliias.info)>

Dear Cherine Chalaby,

My firm, Nameshop, is one of the twelve new gTLD applicants from India as also one of the three applicants under the Applicant Support Program for Developing Countries.

I am writing to request your attention to the following request sent to Kurt Pritz and the new gTLD team on the application for .IDN. The request is reproduced here for ease of reading as also copied below as sent.

Nameshop has applied for the string .IDN as an ASCII string. I understand that it was pointed out that this string, as also a few other strings proposed by a large applicant, may be seen as strings that could be viewed as confusable at the country level due to the fact that these are alpha3 country codes.

The applied for string, .IDN is in the generic, global TLD space, and not a geoTLD, and not intended for country level operations. This is an ASCII TLD for the benefit of idn.idn registrants worldwide. Though not filed as a Community TLD, it is a TLD with a larger Community purpose, as the idea and purpose of .IDN is to offer a bridge for the Internationalized Domain Name Registrants to connect to users beyond their own language communities. The proposed gTLD, .IDN supports multiple cultural, linguistic and ethnic communities across the world by helping communities connect to the rest of the world across the barriers of language. This gTLD is intended to serve users of different languages, irrespective of whether the presence of the language is wide or global. Even if the language or script is completely unfamiliar to the global user, with a .IDN ASCII string mapped to the idn.idn name, the global user will find it easier to decipher the internationalized domain name in a script completely unfamiliar to him or her. While Internationalized Domain Names enable users to connect within their language communities locally, the proposed gTLD would connect users from different communities to connect globally. This gTLD would be of help in furthering the Internet Community's efforts to preserve the Internet as a unified, Global space.

The Applicant Guide book, under section 'Policy Requirements for Generic Top Level Domains' III 3.1 states that "Applied-for gTLD strings in ASCII must be composed of three or more visually distinct characters. Two- character ASCII strings are not permitted, to avoid conflicting with current and future country codes based on the ISO 3166-1 standard." In this section, III.3.1. on what is not permitted, there is no mention of alpha 3 country codes, while this section unambiguously reserves two character ISO standard country codes.

Under the section on 'Geographic Names Review', 2.2.1.4 the guide book states that strings that are country or territory names will not be approved. Here, what is stated as "will not be approved" includes 2.2.1.4.1.i alpha-3 code



listed in the ISO 3166-1 standard.

As an applicant applying for a generic ASCII string, that is not a Geographic String or Country Code for country level operations, the title "Geographic Names Review" appeared to be that of a section offering guidelines pertinent only to the applications for geographic names (strings), so the caution on alpha3 ISO codes was completely missed.

I wish to assure that Nameshop as the applicant for .IDN has no intention of positioning this TLD in any manner as a country level TLD to cause any confusion whatsoever. I hope ICANN would take into account the fact that the string + idea + business model makes the application. Viewed together, .IDN is global, with a larger purpose and the idea as conceived to be implemented by a fair business model would indeed add enormous value to ICANN's new gTLD program in the area of IDN implementation.

My request to ICANN is:

1. To consider .IDN for delegation, if the above details would satisfy the ccNSO and the GAC.
2. If there are difficulties, to allow me to change the string to another string of three or more ASCII characters that is not reserved, not a country or territory name, uncontentious but represents the purpose of this TLD.

Thank You.

Sivasubramanian M  
Nameshop, India.

----- Forwarded message -----

From: "Sivasubramanian M" <[isolatedn@gmail.com](mailto:isolatedn@gmail.com)>

Date: Jul 18, 2012 11:04 PM

Subject: Application for dotIDN as an ASCII gTLD by Nameshop from India

To: "Kurt Pritz" <[kurt.pritz@icann.org](mailto:kurt.pritz@icann.org)>

Cc: <[akram.atallah@icann.org](mailto:akram.atallah@icann.org)>, <[karla.valente@icann.org](mailto:karla.valente@icann.org)>, "Afilias LaPlante" <[rlaplante@afilias.info](mailto:rlaplante@afilias.info)>, "Desiree Miloshevic" <[dmiloshevic@afilias.info](mailto:dmiloshevic@afilias.info)>

Dear Kurt Pritz,

Nameshop has applied for the string .IDN as an ASCII string. I understand that it was pointed out that this string, as also a few other strings proposed by a large applicant, may be seen as strings that could be viewed as confusable at the country level due to the fact that these are alpha3 country codes.

The applied for string, .IDN is in the generic, global TLD space, and not a geoTLD, and not intended for country level operations. This is an ASCII TLD for the benefit of idn.idn registrants worldwide. Though not filed as a Community TLD, it is a TLD with a larger Community purpose, as the idea and purpose of .IDN is to offer a bridge for the Internationalized Domain Name Registrants to connect to users beyond their own language communities. The proposed gTLD, .IDN supports multiple cultural, linguistic and ethnic communities across the world by helping communities connect to the rest of the world across the barriers of language. This gTLD is intended to serve users of different languages, irrespective of whether the presence of the language is wide or global. Even if the language or script is completely unfamiliar to the global user, with a .IDN ASCII string mapped to the idn.idn name, the global user will find it easier to decipher the internationalized domain name in a script completely unfamiliar to him or her. While Internationalized Domain Names enable users to connect within their language communities locally, the proposed gTLD would connect users from different communities to connect globally. This gTLD would be of help in furthering the Internet Community's efforts to preserve the Internet as a unified, Global space.

The Applicant Guide book, under section 'Policy Requirements for Generic Top Level Domains' III 3.1 states that "Applied-for gTLD strings in ASCII must be composed of three or more visually distinct characters. Two-character ASCII strings are not permitted, to avoid conflicting with current and future country codes based on the ISO 3166-1 standard." In this section, III.3.1. on what is not permitted, there is no mention of alpha 3 country codes, while this section unambiguously reserves two character ISO standard country codes.

Under the section on 'Geographic Names Review', 2.2.1.4 the guide book states that strings that are country or territory names will not be approved. Here, what is stated as "will not be approved" includes 2.2.1.4.1.i alpha-3 code listed in the ISO 3166-1 standard.

As an applicant applying for a generic ASCII string, that is not a Geographic String or Country Code for country level operations, the title "Geographic Names Review" appeared to be that of a section offering guidelines pertinent only to the applications for geographic names (strings), so the caution on alpha3 ISO codes was completely missed.

I wish to assure that Nameshop as the applicant for .IDN has no intention of positioning this TLD in any manner as a country level TLD to cause any confusion whatsoever. I hope ICANN would take into account the fact that the string + idea + business model makes the application. Viewed together, .IDN is global, with a larger purpose and the idea as conceived to be implemented by a fair business model would indeed add enormous value to ICANN's new gTLD program in the area of IDN implementation.

My request to ICANN is:

1. To consider .IDN for delegation, if the above details would satisfy the ccNSO and the GAC.
2. If there are difficulties, to allow me to change the string to another string of three or more ASCII characters that is not reserved, not a country or territory name, uncontentious but represents the purpose of this TLD.

Thank You.

Sivasubramanian M  
Nameshop, India.

Sent from Turiya MID  
<http://turiya.mobi>

---

### 3 attachments



**Request for Changes to the nameshop gTLD application filed on 30 Sep 2012.pdf**  
323K



**Response\_Sivasubramanian\_Final received on Nov 2 2012 on dot IDN.pdf**  
132K



**ChangeRequestDecision\_37809 on the request to change the string to internet received on Feb 19 2013.pdf**  
177K