Appendix E

Updated Amazon Applications for .MUSIC, .SONG and .TUNES with Material Changes

New gTLD Application Submitted to ICANN by: Amazon EU S.à r.l.

Application Downloaded On: 30 Apr 2014

String: MUSIC

Application ID: 1-1316-18029

Applicant Information

1. Full legal name

Amazon EU S.à r.l.

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Con ac nforma ion Redac ed

4. Fax number

Contact nformation Redacted

5. If applicable, website or URL

http://www.amazon.com/

Primary Contact

6(a). Name

Lorna Gradden

6(b). Title

Operations Director

6(c). Address

6(d). Phone Number

Contact nformation Redacted

6(e). Fax Number

Contact nformation Redacted

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Dana Northcott

7(b). Title

Associate General Counsel, IP

7(c). Address

7(d). Phone Number

Contact nformation Redacted

7(e). Fax Number

Con ac nforma ion Redac ed

7(f). Email Address

Contact Informat on Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Contact Information Redacted

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

Luxembourg

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

Attachments are not displayed on this form.

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

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

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

Amazon EU S.à r.l. is not a joint venture.

Applicant Background

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

Name	Position

Allan Lyall	Manager
Eric Laurent Broussard	Manager
Eva Charlotte Gehlin	Manager
Gregory William Greeley	Manager
John Timothy Leslie	Manager

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

Name	Position
Allan Lyall	Manager
Eric Laurent Broussard	Manager
Eva Charlotte Gehlin	Manager
Gregory William Greeley	Manager
John Timothy Leslie	Manager

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

Name	Position
Amazon Europe Holding Technologies S.C.S.	Not Applicable

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

Applied-for gTLD string

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

MUSIC

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

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

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

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

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

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

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

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

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

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

15C. List any variants to the applied-for gTLD string according to the relevant IDN tables.

---

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

Neustar, Amazon EU S.à r.l.'s provider of back end registry services, confirms that it does not anticipate any problems in the operation or rendering of this ASCII string. The string conforms to accepted standards and poses no threat to the operational security and stability of the Internet.

---

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

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

Founded in 1994, Amazon opened on the World Wide Web in July 1995 and today offers Earth's Biggest Selection. Amazon seeks to be Earth's most customer-centric company, where customers can find and discover anything they might want to buy online, and endeavors to offer its customers the lowest possible prices. Amazon and other sellers offer millions of unique new, refurbished and used items in categories such as Books; Movies, Music & Games; Digital Downloads; Electronics & Computers; Home & Garden; Toys, Kids & Baby; Grocery; Apparel, Shoes & Jewelry; Health & Beauty; Sports & Outdoors; and Tools, Auto & Industrial. Amazon Web Services provides Amazon's developer customers with access to in-the-cloud infrastructure services based on Amazon's own back-end technology platform, which developers can use to enable virtually any type of business. The new latest generation Kindle is the lightest, most compact Kindle ever and features the same 6-inch, most advanced electronic ink display that reads like real paper even in bright sunlight. Kindle Touch is a new addition to the Kindle family with an easy-to-use touch screen that makes it easier than ever to turn pages, search, shop, and take notes – still with all the benefits of the most advanced electronic ink display. Kindle Touch 3G is the top of the line e-reader and offers the same new design and features of Kindle Touch, with the unparalleled added convenience of free 3G. Kindle Fire is the Kindle for movies, TV shows, music, books, magazines, apps, games and web browsing with all the content, free storage in the Amazon Cloud, Whispersync, Amazon Silk (Amazon's new revolutionary cloud-accelerated web browser), vibrant color touch screen, and powerful dual-core processor.

The mission of the <.TLD> registry is:

To provide a unique and dedicated platform while simultaneously protecting the integrity of Amazon's brand and reputation.

A <.TLD> registry will:

- Offer a stable and secure foundation for online communication and interaction.
- Provide a platform for innovation.

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

The <.TLD> registry will benefit registrants and internet users by offering a stable and secure foundation for online communication and interaction.

What is the goal of your proposed gTLD in terms of areas of specialty, service levels or reputation?

Amazon intends for its new <.TLD> gTLD to provide a unique and dedicated platform for stable and secure online communication and interaction. The <.TLD> registry will be run in line with current industry standards of good registry practice.

What do you anticipate your proposed gTLD will add to the current space in terms of competition, differentiation or innovation?

Amazon values the opportunity to be one of the first companies to own a gTLD.

A <.TLD> registry will:

- Offer a stable and secure foundation for online communication and interaction.
- Provide a platform for innovation.

What goals does your proposed gTLD have in terms of user experience?

Amazon intends for its new <.TLD> gTLD to provide a unique and dedicated platform for stable and secure online communication and interaction.

Provide a complete description of the applicant's intended registration policies in support of the goals above.

Amazon's Intellectual Property group will be responsible for the development, maintenance and enforcement of a Domain Management Policy. The Domain Management Policy will define (i) the rules associated with eligibility and domain name allocation, (ii) the license terms governing the use of a <.TLD> domain name, and (iii) the dispute resolution policies for the <.TLD> gTLD. Amazon will update the Domain Management Policy as needed to reflect the registry's business goals and, where appropriate, ICANN consensus policies.

Registration of a domain name in the <.TLD> registry will be undertaken in four steps: (i) Eligibility Confirmation, (ii) Naming Convention Check, (iii) Acceptable Use Review, and (iv) Registration.

For example, on the rules of eligibility, each applied for character string must conform to the <.TLD> rules of eligibility. Each <.TLD> name must:

- be at least 1 character and no more than 63 characters long
- not contain a hyphen on the 3rd and 4th position (tagged domains)
- contain only letters (a-z), numbers (0-9) and hyphens or a combination of these
- start and end with an alphanumeric character, not a hyphen
- not match any character strings reserved by ICANN
- not match any protected country names or geographical terms

Additionally:

- Internationalized domain names (IDN) may be supported in the <.TLD> registry at the second level.
- The <.TLD> registry will respect third party intellectual property rights.
- All <.TLD> domains will carry accurate and up-to-date registration records.

Amazon's Intellectual Property group reserves the right to revoke a license to use a <.TLD> domain name, at any time, if any use of a <.TLD> domain name violates the Domain Management Policy.

Will your proposed gTLD impose any measures for protecting the privacy of confidential information of registrants or users?

Yes. Amazon will implement appropriate privacy policies respecting requirements of local jurisdictions. For example, Amazon is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union.

Describe whether and in what ways outreach and communications will help to achieve your projected benefits?

Amazon will assess the need to undertake public outreach or mass communication about its new gTLD registry in line with the goals for the TLD.

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

Amazon intends to initially provision a relatively small number of domains in the <.TLD> registry to support the goals of the TLD. These initiatives should not impose social costs of any type on consumers.

How will multiple applications for a particular domain be resolved, for example, by auction or on a first come first served basis?

Applications from eligible requestors for domains in the <.TLD> registry will be considered by Amazon's Intellectual Property group on a first come first served basis and allocated in line with the goals of the TLD.

Explain any cost benefits for registrants you intend to implement (e.g. advantageous pricing, introductory discounts, bulk registration discounts).
Domains in the <.TLD> registry will be provisioned to support the goals of the TLD. Accordingly, "cost benefits" may be explored depending on the goals of the TLD. Amazon shares the goals of enhancing customer trust and choice.

The Registry Agreement requires that registrars be offered the option to obtain initial domain name registrations for periods of one to ten years at the discretion of the registrar, but no greater than 10 years. Additionally the Registry Agreement requires advance written notice of price increases. Do you intend to make contractual commitments to registrants regarding the magnitude of price escalation?

The Domain Management Policy will include the costs and benefits of a unique and dedicated platform for stable and secure online communication and interaction.

---

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

No

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

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

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

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

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

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

21A. Is the application for a geographic name?

No

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

Amazon EU S.à r.l., with support of its ultimate parent company, Amazon.com, Inc. (collectively referred to in this response throughout as "Amazon"), is committed to managing the <.TLD> registry in full compliance with all applicable laws, consensus policies, ICANN guidelines, RFCs and the Specifications of the Registry Agreement. In the management of domain names in the <.TLD> registry, based on GAC advice and Specification 5, Amazon intends to block from initial registration all required domain names.

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

security or stability concerns.
The following registry services are customary services offered by a registry operator:

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

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

23.1 Introduction

Amazon EU S.à r.l. has elected to partner with Neustar, Inc. to provide back-end services for the .MUSIC registry. In making this decision, Amazon EU S.à r.l. recognized that Neustar already possesses a production-proven registry system that can be quickly deployed and smoothly operated over its robust, flexible, and scalable world-class infrastructure. The existing registry services will be leveraged for the .MUSIC registry. The following section describes the registry services to be provided.
23.2 Standard Technical and Business Components
Neustar will provide the highest level of service while delivering a secure, stable and comprehensive registry platform. Amazon EU S.à r.l. will use Neustar's Registry Services platform to deploy the .MUSIC registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to .MUSIC.

- Registry-Registrar Shared Registration Service (SRS)
- Extensible Provisioning Protocol (EPP)
- Domain Name System (DNS)
- WHOIS
- DNSSEC
- Data Escrow
- Dissemination of Zone Files using Dynamic Updates
- Access to Bulk Zone Files
- Dynamic WHOIS Updates
- IPv6 Support
- Rights Protection Mechanisms
- Internationalized Domain Names (IDN).

The following is a description of each of the services.
SRS
Neustar's secure and stable SRS is a production-proven, standards-based, highly reliable, and high-performance domain name registration and management system. The SRS includes an EPP interface for receiving data from registrars for the purpose of provisioning and managing domain names and name servers. The response to Question 24 provides specific SRS information.
EPP
The .MUSIC registry will use the Extensible Provisioning Protocol (EPP) for the provisioning of domain names. The EPP implementation will be fully compliant with all RFCs. Registrars are provided with access via an EPP API and an EPP based Web GUI. With more than 10 gTLD, ccTLD, and private TLDs implementations, Neustar has extensive experience building EPP-based registries. Additional discussion on the EPP approach is presented in the response to Question 25.
DNS
Amazon EU S.à r.l. will leverage Neustar's world-class DNS network of geographically distributed nameserver sites to provide the highest level of DNS service. The service utilizes "Anycast" routing technology, and supports both IPv4 and IPv6. The DNS network is highly proven, and currently provides service to over 20 TLDs and thousands of enterprise companies. Additional information on the DNS solution is presented in the response to Questions 35.
WHOIS
Neustar's existing standard WHOIS solution will be used for .MUSIC. The service provides supports for near real-time dynamic updates. The design and construction is agnostic with regard to data display policy is flexible enough to accommodate any data model. In addition, a searchable WHOIS service that complies with all ICANN requirements will be provided. The following WHOIS options will be provided:
Standard WHOIS (Port 43)
Standard WHOIS (Web)
Searchable WHOIS (Web)
DNSSEC
An RFC compliant DNSSEC implementation will be provided using existing DNSSEC capabilities. Neustar is an experienced provider of DNSSEC services, and currently manages signed zones for three large top level domains: .biz, .us, and .co. Registrars are provided with the ability to submit and manage DS records using EPP, or through a web GUI. Additional information on DNSSEC, including the management of security extensions is found in the response to Question

43.
Data Escrow
Data escrow will be performed in compliance with all ICANN requirements in conjunction with an approved data escrow provider. The data escrow service will:

- Protect against data loss
- Follow industry best practices
- Ensure easy, accurate, and timely retrieval and restore capability in the event of a hardware failure
- Minimizes the impact of software or business failure.

Additional information on the Data Escrow service is provided in the response to Question 38.
Dissemination of Zone Files using Dynamic Updates
Dissemination of zone files will be provided through a dynamic, near real-time process. Updates will be performed within the specified performance levels. The proven technology ensures that updates pushed to all nodes within a few minutes of the changes being received by the SRS. Additional information on the DNS updates may be found in the response to Question 35.
Access to Bulk Zone Files
Amazon EU S.à r.l. will provide third party access to the bulk zone file in accordance with specification 4, Section 2 of the Registry Agreement. Credentialing and dissemination of the zone files will be facilitated through the Central Zone Data Access Provider.
Dynamic WHOIS Updates
Updates to records in the WHOIS database will be provided via dynamic, near real-time updates. Guaranteed delivery message oriented middleware is used to ensure each individual WHOIS server is refreshed with dynamic updates. This component ensures that all WHOIS servers are kept current as changes occur in the SRS, while also decoupling WHOIS from the SRS. Additional information on WHOIS updates is presented in response to Question 26.
IPv6 Support
The .MUSIC registry will provide IPv6 support in the following registry services: SRS, WHOIS, and DNS/DNSSEC. In addition, the registry supports the provisioning of IPv6 AAAA records. A detailed description on IPv6 is presented in the response to Question 36.
Required Rights Protection Mechanisms
Amazon EU S.à r.l. will provide all ICANN required Rights Mechanisms, including:

- Trademark Claims Service
- Trademark Post-Delegation Dispute Resolution Procedure (PDDRP)
- Registration Restriction Dispute Resolution Procedure (RRDRP)
- UDRP
- URS
- Sunrise service.

More information is presented in the response to Question 29.
Internationalized Domain Names (IDN)

IDN registrations are provided in full compliance with the IDNA protocol. Neustar possesses extensive experience offering IDN registrations in numerous TLDs, and its IDN implementation uses advanced technology to accommodate the unique bundling needs of certain languages. Character mappings are easily constructed to block out characters that may be deemed as confusing to users. A detailed description of the IDN implementation is presented in response to Question 44.
23.3 Unique Services
Amazon EU S.à r.l. will not be offering services that are unique to .MUSIC.
23.4 Security or Stability Concerns
All services offered are standard registry services that have no known security or stability concerns. Neustar has demonstrated a strong track record of security and stability within the industry.

---

24. Shared Registration System (SRS) Performance:
describe

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

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

24.1 Introduction

Amazon EU S.à r.l. has partnered with Neustar, Inc., an experienced TLD registry operator, for the operation of the .MUSIC Registry. Amazon EU S.à r.l. is confident that the plan in place for the operation of a robust and reliable Shared Registration System (SRS) as currently provided by Neustar will satisfy the criterion established by ICANN.

Neustar built its SRS from the ground up as an EPP based platform and has been operating it reliably and at scale since 2001. The software currently provides registry services to five TLDs (.BIZ, .US, TEL, .CO and .TRAVEL) and is used to provide gateway services to the .CN and .TW registries. Neustar's state of the art registry has a proven track record of being secure, stable, and robust. It manages more than 6 million domains, and has over 300 registrars connected today.

The following describes a detailed plan for a robust and reliable SRS that meets all ICANN requirements including compliance with Specifications 6 and 10.

24.2 The Plan for Operation of a Robust and Reliable SRS

High-level SRS System Description

The SRS to be used for .MUSIC will leverage a production-proven, standards-based, highly reliable and high-performance domain name registration and management system that fully meets or exceeds the requirements as identified in the new gTLD Application Guidebook.

The SRS is the central component of any registry implementation and its quality, reliability and capabilities are essential to the overall stability of the TLD. Neustar has a documented history of deploying SRS implementations with proven and verifiable performance, reliability and availability. The SRS adheres to all industry standards and protocols. By leveraging an existing SRS platform, Amazon EU S.à r.l. is mitigating the significant risks and costs associated with the development of a new system. Highlights of the SRS include:

State-of-the-art, production proven multi-layer design
Ability to rapidly and easily scale from low to high volume as a TLD grows
Fully redundant architecture at two sites
Support for IDN registrations in compliance with all standards
Use by over 300 Registrars
EPP connectivity over IPv6
Performance being measured using 100% of all production transactions (not sampling).

SRS Systems, Software, Hardware, and Interoperability

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

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

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

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

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

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

SRS Design

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

Protocol Layer
Business Policy Layer
Database.

Each of the layers is described below.

Protocol Layer

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

horizontally scalable as dictated by volume.
The EPP servers authenticate against a series of security controls before granting service, as follows:

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

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

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

Business Policy Layer

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

Similar to the EPP protocol farm, the SRS consists of a farm of application servers within this layer. This design ensures that there is sufficient capacity to process every transaction in a manner that meets or exceeds all service level requirements. Some registries couple the business logic layer directly in the protocol layer or within the database. This architecture limits the ability to scale the registry. Using a decoupled architecture enables the load to be distributed among farms of inexpensive servers that can be scaled up or down as demand changes. The SRS today processes over 30 million EPP transactions daily.

Database

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

Figure 24-1 depicts the overall SRS architecture including network components.

Number of Servers

As depicted in the SRS architecture diagram above Neustar operates a high availability architecture where at each level of the stack there are no single points of failures. Each of the network level devices run with dual pairs as do the databases. For the .MUSIC registry, the SRS will operate with 8 protocol servers and 6 policy engine servers. These expand horizontally as volume increases due to additional TLDs, increased load, and through organic growth. In addition to the SRS servers described above, there are multiple backend servers for services such as DNS and WHOIS. These are discussed in detail within those respective response sections.

Description of Interconnectivity with Other Registry Systems

The core SRS service interfaces with other external systems via Neustar's external systems layer. The services that the SRS interfaces with include:

WHOIS
DNS
Billing
Data Warehouse (Reporting and Data Escrow).

Other external interfaces may be deployed to meet the unique needs of a TLD. At this time there are no additional interfaces planned for .MUSIC.

The SRS includes an "external notifier" concept in its business policy engine as a message dispatcher. This design allows time-consuming backend processing to be decoupled from critical online registrar transactions. Using an external notifier solution, the registry can utilize "control levers" that allow it to tune or to disable processes to ensure optimal performance at all times. For example, during the early minutes of a TLD launch, when unusually high volumes of transactions are expected, the registry can elect to suspend processing of one or more back end systems in order to ensure that greater processing power is available to handle the increased load requirements. This proven architecture has been used with numerous TLD launches, some of which have involved the processing of over tens of millions of transactions in the opening hours. The following are the standard three external notifiers used the SRS:

WHOIS External Notifier

The WHOIS external notifier dispatches a work item for any EPP transaction that may potentially have an impact on WHOIS. It is important to note that, while the WHOIS external notifier feeds the WHOIS system, it intentionally does not have visibility into the actual contents of the WHOIS system. The WHOIS external notifier serves just as a tool to send a signal to the WHOIS system that a change is ready to occur. The WHOIS system possesses the intelligence and data visibility to know exactly what needs to change in WHOIS. See response to Question 26 for greater detail.

DNS External Notifier

The DNS external notifier dispatches a work item for any EPP transaction that may potentially have an impact on DNS. Like the WHOIS external notifier, the DNS external notifier does not have visibility into the actual contents of the DNS zones. The work items that are generated by the notifier indicate to the dynamic DNS update sub-system that a change occurred that may impact DNS. That DNS system has the ability to decide what actual changes must be propagated out to the DNS constellation. See response to Question 35 for greater detail.

Billing External Notifier

The billing external notifier is responsible for sending all billable transactions to the downstream financial systems for billing and collection. This external notifier contains the necessary logic to determine what types of transactions are billable. The financial systems use this information to apply appropriate debits and credits based on registrar.

Data Warehouse
The data warehouse is responsible for managing reporting services, including registrar reports, business intelligence dashboards, and the processing of data escrow files. The Reporting Database is used to create both internal and external reports, primarily to support registrar billing and contractual reporting requirement. The data warehouse databases are updated on a daily basis with full copies of the production SRS data.
Frequency of Synchronization between Servers
The external notifiers discussed above perform updates in near real-time, well within the prescribed service level requirements. As transactions from registrars update the core SRS, update notifications are pushed to the external systems such as DNS and WHOIS. These updates are typically live in the external system within 2-3 minutes.
Synchronization Scheme (e.g., hot standby, cold standby)
Neustar operates two hot databases within the data center that is operating in primary mode. These two databases are kept in sync via synchronous replication. Additionally, there are two databases in the secondary data center. These databases are updated real time through asynchronous replication. This model allows for high performance while also ensuring protection of data. See response to Question 33 for greater detail.
Compliance with Specification 6 Section 1.2
The SRS implementation for .MUSIC is fully compliant with Specification 6, including section 1.2. EPP Standards are described and embodied in a number of IETF RFCs, ICANN contracts and practices, and registry-registrar agreements. Extensible Provisioning Protocol or EPP is defined by a core set of RFCs that standardize the interface that make up the registry-registrar model. The SRS interface supports EPP 1.0 as defined in the following RFCs shown in Table 24-1.

Additional information on the EPP implementation and compliance with RFCs can be found in the response to Question 25.
Compliance with Specification 10
Specification 10 of the New TLD Agreement defines the performance specifications of the TLD, including service level requirements related to DNS, RDDS (WHOIS), and EPP. The requirements include both availability and transaction response time measurements. As an experienced registry operator, Neustar has a long and verifiable track record of providing registry services that consistently exceed the performance specifications stipulated in ICANN agreements. This same high level of service will be provided for the .MUSIC Registry. The following section describes Neustar's experience and its capabilities to meet the requirements in the new agreement.
To properly measure the technical performance and progress of TLDs, Neustar collects data on key essential operating metrics. These measurements are key indicators of the performance and health of the registry. Neustar's current .biz SLA commitments are among the most stringent in the industry today, and exceed the requirements for new TLDs. Table 24-2 compares the current SRS performance levels compared to the requirements for new TLDs, and clearly demonstrates the ability of the SRS to exceed those requirements.

Their ability to commit and meet such high performance standards is a direct result of their philosophy towards operational excellence. See response to Question 31 for a full description of their philosophy for building and managing for performance.
24.3 Resourcing Plans
The development, customization, and on-going support of the SRS are the responsibility of a combination of technical and operational teams, including:

- Development/Engineering
- Database Administration
- Systems Administration
- Network Engineering.

Additionally, if customization or modifications are required, the Product Management and Quality Assurance teams will be involved in the design and testing. Finally, the Network Operations and Information Security play an important role in ensuring the systems involved are operating securely and reliably.
The necessary resources will be pulled from the pool of operational resources described in detail in the response to Question 31. Neustar's SRS implementation is very mature, and has been in production for over 10 years. As such, very little new development related to the SRS will be required for the implementation of the .MUSIC registry. The following resources are available from those teams:
Development/Engineering – 19 employees
Database Administration- 10 employees
Systems Administration – 24 employees
Network Engineering – 5 employees
The resources are more than adequate to support the SRS needs of all the TLDs operated by Neustar, including the .MUSIC registry.

---

25. Extensible Provisioning Protocol (EPP): provide a detailed description of the interface with registrars, including how the applicant will comply with EPP in RFCs 3735 (if applicable), and 5730-5734.
If intending to provide proprietary EPP extensions, provide documentation consistent with RFC 3735, including the EPP templates and schemas that will be used.

Describe resourcing plans (number and description of personnel roles allocated to this area).
A complete answer is expected to be no more than 5 pages. If there are proprietary EPP extensions, a complete answer is also expected to be no more than 5 pages per EPP extension.

25.1 Introduction
Amazon EU S.à r.l.'s back-end registry operator, Neustar, has over 10 years of experience operating EPP based registries. They deployed one of the first EPP registries in 2001 with the launch of .biz. In 2004, they were the first gTLD to implement EPP 1.0. Over the last ten years Neustar has implemented numerous extensions to meet various unique TLD requirements. Neustar will leverage its extensive experience to ensure Amazon EU S.à r.l. is provided with an unparalleled EPP based registry. The following discussion explains the EPP interface which will be used for the .MUSIC registry. This interface exists within the protocol farm layer as described in Question 24 and is depicted in Figure 25-1.

25.2 EPP Interface
Registrars are provided with two different interfaces for interacting with the registry. Both are EPP based, and both contain all the functionality necessary to provision and manage domain names. The primary mechanism is an EPP interface to connect directly with the registry. This is the interface registrars will use for most of their interactions with the registry. However, an alternative web GUI (Registry Administration Tool) that can also be used to perform EPP transactions will be provided. The primary use of the Registry Administration Tool is for performing administrative or customer support tasks.
The main features of the EPP implementation are:
Standards Compliance: The EPP XML interface is compliant to the EPP RFCs. As future EPP RFCs are published or existing RFCs are updated, Neustar makes changes to the implementation keeping in mind of any backward compatibility issues.
Scalability: The system is deployed keeping in mind that it may be required to grow and shrink the footprint of the Registry system for a particular TLD.
Fault-tolerance: The EPP servers are deployed in two geographically separate data centers to provide for quick failover capability in case of a major outage in a particular data center. The EPP servers adhere to strict availability requirements defined in the SLAs.
Configurability: The EPP extensions are built in a way that they can be easily configured to turn on or off for a particular TLD.
Extensibility: The software is built ground up using object oriented design. This allows for easy extensibility of the software without risking the possibility of the change rippling through the whole application.
Auditable: The system stores detailed information about EPP transactions from provisioning to DNS and WHOIS publishing. In case of a dispute regarding a name registration, the Registry can provide comprehensive audit information on EPP transactions.
Security: The system provides IP address based access control, client credential-based authorization test, digital certificate exchange, and connection limiting to the protocol layer.
25.3 Compliance with RFCs and Specifications
The registry-registrar model is described and embodied in a number of IETF RFCs, ICANN contracts and practices, and registry-registrar agreements. As shown in Table 25-1, EPP is defined by the core set of RFCs that standardize the interface that registrars use to provision domains with the SRS. As a core component of the SRS architecture, the implementation is fully compliant with all EPP RFCs.

Neustar ensures compliance with all RFCs through a variety of processes and procedures. Members from the engineering and standards teams actively monitor and participate in the development of RFCs that impact the registry services, including those related to EPP. When new RFCs are introduced or existing ones are updated, the team performs a full compliance review of each system impacted by the change. Furthermore, all code releases include a full regression test that includes specific test cases to verify RFC compliance.

Neustar has a long history of providing exceptional service that exceeds all performance specifications. The SRS and EPP interface have been designed to exceed the EPP specifications defined in Specification 10 of the Registry Agreement and profiled in Table 25-2. Evidence of Neustar's ability to perform at these levels can be found in the .biz monthly progress reports found on the ICANN website.

EPP Toolkits
Toolkits, under open source licensing, are freely provided to registrars for interfacing with the SRS. Both Java and C++ toolkits will be provided, along with the accompanying documentation. The Registrar Tool Kit (RTK) is a software development kit (SDK) that supports the development of a registrar software system for registering domain names in the registry using EPP. The SDK consists of software and documentation as described below.
The software consists of working Java and C++ EPP common APIs and samples that implement the EPP core functions and EPP extensions used to communicate between the registry and registrar. The RTK illustrates how XML requests (registration events) can be assembled and forwarded to the registry for processing. The software provides the registrar with the basis for a reference implementation that conforms to the EPP registry-registrar protocol. The software component of the SDK also includes XML schema definition files for all Registry EPP objects and EPP object extensions. The RTK also includes a "dummy" server to aid in the testing of EPP clients.
The accompanying documentation describes the EPP software package hierarchy, the object data

model, and the defined objects and methods (including calling parameter lists and expected response behavior). New versions of the RTK are made available from time to time to provide support for additional features as they become available and support for other platforms and languages.

25.4 Proprietary EPP Extensions

The .MUSIC registry will not include proprietary EPP extensions. Neustar has implemented various EPP extensions for both internal and external use in other TLD registries. These extensions use the standard EPP extension framework described in RFC 5730. Table 25-3 provides a list of extensions developed for other TLDs. Should the .MUSIC registry require an EPP extension at some point in the future, the extension will be implemented in compliance with all RFC specifications including RFC 3735.

The full EPP schema to be used in the .MUSIC registry is attached in the document titled “EPP Schema.”

25.5 Resourcing Plans

The development and support of EPP is largely the responsibility of the Development/Engineering and Quality Assurance teams. As an experience registry operator with a fully developed EPP solution, on-going support is largely limited to periodic updates to the standard and the implementation of TLD specific extensions.

The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:

Development/Engineering – 19 employees

Quality Assurance - 7 employees.

These resources are more than adequate to support any EPP modification needs of the .MUSIC registry.

---

26. Whois: describe

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

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

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

Frequency of synchronization between servers.

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

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

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

26.1 Introduction

Amazon EU S.à r.l. recognizes the importance of an accurate, reliable, and up-to-date WHOIS database to governments, law enforcement, intellectual property holders and the public as a whole and is firmly committed to complying with all of the applicable WHOIS specifications for data objects, bulk access, and lookups as defined in Specifications 4 and 10 to the Registry Agreement. Amazon EU S.à r.l.’s back-end registry services provider, Neustar, has extensive experience providing ICANN and RFC-compliant WHOIS services for each of the TLDs that it operates both as a Registry Operator for gTLDs, ccTLDs and back-end registry services provider. As one of the first “thick” registry operators in the gTLD space, Neustar’s WHOIS service has been designed from the ground up to display as much information as required by a TLD and

respond to a very stringent availability and performance requirement.
Some of the key features of .MUSIC's solution include:

- Fully compliant with all relevant RFCs including 3912
- Production proven, highly flexible, and scalable with a track record of 100% availability over the past 10 years
- Exceeds current and proposed performance specifications
- Supports dynamic updates with the capability of doing bulk updates
- Geographically distributed sites to provide greater stability and performance
- In addition, .MUSIC's thick-WHOIS solution also provides for additional search capabilities and mechanisms to mitigate potential forms of abuse as discussed below. (e.g., IDN, registrant data).

26.2 Software Components
The WHOIS architecture comprises the following components:

- An in-memory database local to each WHOIS node: To provide for the performance needs, the WHOIS data is served from an in-memory database indexed by searchable keys.
- Redundant servers: To provide for redundancy, the WHOIS updates are propagated to a cluster of WHOIS servers that maintain an independent copy of the database.
- Attack resistant: To ensure that the WHOIS system cannot be abused using malicious queries or DOS attacks, the WHOIS server is only allowed to query the local database and rate limits on queries based on IPs and IP ranges can be readily applied.
- Accuracy auditor: To ensure the accuracy of the information served by the WHOIS servers, a daily audit is done between the SRS information and the WHOIS responses for the domain names which are updated during the last 24-hour period. Any discrepancies are resolved proactively.
- Modular design: The WHOIS system allows for filtering and translation of data elements between the SRS and the WHOIS database to allow for customizations.
- Scalable architecture: The WHOIS system is scalable and has a very small footprint. Depending on the query volume, the deployment size can grow and shrink quickly.
- Flexible: It is flexible enough to accommodate thin, thick, or modified thick models and can accommodate any future ICANN policy, such as different information display levels based on user categorization.
- SRS master database: The SRS database is the main persistent store of the Registry information. The Update Agent computes what WHOIS updates need to be pushed out. A publish-subscribe mechanism then takes these incremental updates and pushes to all the WHOIS slaves that answer queries.

26.3 Compliance with RFC and Specifications 4 and 10
Neustar has been running thick-WHOIS Services for over 10+ years in full compliance with RFC 3912 and with Specifications 4 and 10 of the Registry Agreement.RFC 3912 is a simple text based protocol over TCP that describes the interaction between the server and client on port 43. Neustar built a home-grown solution for this service. It processes millions of WHOIS queries per day.
Table 26-1 describes Neustar's compliance with Specifications 4 and 10.

Neustar ensures compliance with all RFCs through a variety of processes and procedures. Members from the engineering and standards teams actively monitor and participate in the development of RFCs that impact the registry services, including those related to WHOIS. When new RFCs are introduced or existing ones are updated, the team performs a full compliance review of each system impacted by the change. Furthermore, all code releases include a full regression test that includes specific test cases to verify RFC compliance.

26.4 High-level WHOIS System Description
26.4.1 WHOIS Service (port 43)
The WHOIS service is responsible for handling port 43 queries. Our WHOIS is optimized for speed using an in-memory database and master-slave architecture between the SRS and WHOIS slaves.
The WHOIS service also has built-in support for IDN. If the domain name being queried is an IDN, the returned results include the language of the domain name, the domain name's UTF-8 encoded representation along with the Unicode code page.
26.4.2 Web Page for WHOIS queries
In addition to the WHOIS Service on port 43, Neustar provides a web based WHOIS application (www.whois.MUSIC). It is an intuitive and easy to use application for the general public to use. WHOIS web application provides all of the features available in the port 43 WHOIS. This includes full and partial search on:

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

It also provides features not available on the port 43 service. These include:

1. Redemption Grace Period calculation: Based on the registry's policy, domains in pendingDelete can be restorable or scheduled for release depending on the date/time the domain went into pendingDelete. For these domains, the web based WHOIS displays "Restorable" or "Scheduled for Release" to clearly show this additional status to the user.
2. Extensive support for international domain names (IDN)
3. Ability to perform WHOIS lookups on the actual Unicode IDN
4. Display of the actual Unicode IDN in addition to the ACE-encoded name
5. A Unicode to Punycode and Punycode to Unicode translator
6. An extensive FAQ
7. A list of upcoming domain deletions

26.5 IT and Infrastructure Resources
As described above the WHOIS architecture uses a workflow that decouples the update process from the SRS. This ensures SRS performance is not adversely affected by the load requirements of dynamic updates. It is also decoupled from the WHOIS lookup agent to ensure the WHOIS service is always available and performing well for users. Each of Neustar's geographically diverse WHOIS sites use:

- Firewalls, to protect this sensitive data
- Dedicated servers for MQ Series, to ensure guaranteed delivery of WHOIS updates
- Packetshaper for source IP address-based bandwidth limiting
- Load balancers to distribute query load
- Multiple WHOIS servers for maximizing the performance of WHOIS service.

The WHOIS service uses HP BL 460C servers, each with 2 X Quad Core CPU and a 64GB of RAM. The existing infrastructure has 6 servers, but is designed to be easily scaled with additional servers should it be needed.
Figure 26-1 depicts the different components of the WHOIS architecture.

26.6 Interconnectivity with Other Registry System
As described in Question 24 about the SRS and further in response to Question 31, "Technical Overview", when an update is made by a registrar that impacts WHOIS data, a trigger is sent to the WHOIS system by the external notifier layer. The update agent processes these updates, transforms the data if necessary and then uses messaging oriented middleware to publish all updates to each WHOIS slave. The local update agent accepts the update and applies it to the local in-memory database. A separate auditor compares the data in WHOIS and the SRS daily and monthly to ensure accuracy of the published data.

26.7 Frequency of Synchronization between Servers
Updates from the SRS, through the external notifiers, to the constellation of independent WHOIS slaves happens in real-time via an asynchronous publish/subscribe messaging architecture. The updates are guaranteed to be updated in each slave within the required SLA of 95% ≤ 60 minutes. Please note that Neustar's current architecture is built towards the stricter SLAs (95% ≤ 15 minutes) of .BIZ. The vast majority of updates tend to happen within 2-3 minutes.

26.8 Provision for Searchable WHOIS Capabilities
Neustar will create a new web-based service to address the new search features based on requirements specified in Specification 4 Section 1.8. The application will enable users to search the WHOIS directory using any one or more of the following fields:

- Domain name
- Registrar ID
- Contacts and registrant's name
- Contact and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state or province, etc.)
- Name server name and name server IP address
- The system will also allow search using non-Latin character sets which are compliant with IDNA specification.

The user will choose one or more search criteria, combine them by Boolean operators (AND, OR, NOT) and provide partial or exact match regular expressions for each of the criterion name-value pairs. The domain names matching the search criteria will be returned to the user.
Figure 26-2 shows an architectural depiction of the new service.

Potential Forms of Abuse
As recognized by the Terms of Reference for Whois Misuse Studies, http://gnso.icann.org/issues/whois/tor-whois-misuse-studies-25sep09-en.pdf, a number of reported and recorded harmful acts, such as spam, phishing, identity theft, and stalking which Registrants believe were sent using WHOIS contact information. Although these Whois studies are still underway, there is a general belief that public access to Whois data may lead to a measurable degree of misuse – that is, to actions that cause actual harm, are illegal or illegitimate, or otherwise contrary to the stated legitimate purpose. One of the other key focuses of these studies will be to correlate the reported incidents of harmful acts with anti-harvesting measures that some Registrars and Registries apply to WHOIS queries (e.g., rate limiting, CAPTCHA, etc.).

Neustar firmly believes that adding the increased search capabilities, without appropriate controls could exacerbate the potential abuses associated with the Whois service. To mitigate the risk of this powerful search service being abused by unscrupulous data miners, a layer of security will be built around the query engine which will allow the registry to identify rogue activities and then take appropriate measures. Potential abuses include, but are not limited to:

- Data Mining
- Unauthorized Access
- Excessive Querying
- Denial of Service Attacks

To mitigate the abuses noted above, Neustar will implement any or all of these mechanisms as appropriate:

- Username-password based authentication
- Certificate based authentication
- Data encryption
- CAPTCHA mechanism to prevent robo invocation of Web query
- Fee-based advanced query capabilities for premium customers.

The searchable WHOIS application will adhere to all privacy laws and policies of the .MUSIC registry.

26.9 Resourcing Plans
As with the SRS, the development, customization, and on-going support of the WHOIS service is the responsibility of a combination of technical and operational teams. The primary groups responsible for managing the service include:

- Development/Engineering – 19 employees
- Database Administration – 10 employees
- Systems Administration – 24 employees
- Network Engineering – 5 employees

Additionally, if customization or modifications are required, the Product Management and Quality Assurance teams will also be involved. Finally, the Network Operations and Information Security play an important role in ensuring the systems involved are operating securely and reliably. The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. Neustar's WHOIS implementation is very mature, and has been in production for over 10 years. As such, very little new development will be required to support the implementation of the .MUSIC registry. The resources are more than adequate to support the WHOIS needs of all the TLDs operated by Neustar, including the .MUSIC registry.

---

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

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

The description of the registration lifecycle should be supplemented by the inclusion of a state diagram, which captures definitions, explanations of trigger points, and transitions from state to state.
If applicable, provide definitions for aspects of the registration lifecycle that are not covered by standard EPP RFCs.
A complete answer is expected to be no more than 5 pages.

27.1 Registration Life Cycle
Introduction
.MUSIC will follow the lifecycle and business rules found in the majority of gTLDs today. Our back-end operator, Neustar, has over ten years of experience managing numerous TLDs that utilize standard and unique business rules and lifecycles. This section describes the business rules, registration states, and the overall domain lifecycle that will be used for .MUSIC.
Domain Lifecycle - Description
The registry will use the EPP 1.0 standard for provisioning domain names, contacts and hosts. Each domain record is comprised of three registry object types: domain, contacts, and hosts Domains, contacts and hosts may be assigned various EPP defined statuses indicating either a particular state or restriction placed on the object. Some statuses may be applied by the Registrar; other statuses may only be applied by the Registry. Statuses are an integral part of the domain lifecycle and serve the dual purpose of indicating the particular state of the domain and indicating any restrictions placed on the domain. The EPP standard defines 17 statuses, however only 14 of these statuses will be used in the .MUSIC registry per the defined .MUSIC business rules.
The following is a brief description of each of the statuses. Server statuses may only be applied by the Registry, and client statuses may be applied by the Registrar.

- OK – Default status applied by the Registry.
- Inactive – Default status applied by the Registry if the domain has less than 2 nameservers.
- PendingCreate – Status applied by the Registry upon processing a successful Create command, and indicates further action is pending. This status will not be used in the .MUSIC registry.
- PendingTransfer – Status applied by the Registry upon processing a successful Transfer request command, and indicates further action is pending.
- PendingDelete – Status applied by the Registry upon processing a successful Delete command that does not result in the immediate deletion of the domain, and indicates further action is pending.
- PendingRenew – Status applied by the Registry upon processing a successful Renew command that does not result in the immediate renewal of the domain, and indicates further action is pending. This status will not be used in the .MUSIC registry.

PendingUpdate – Status applied by the Registry if an additional action is expected to complete the update, and indicates further action is pending. This status will not be used in the .MUSIC registry.
Hold – Removes the domain from the DNS zone.
UpdateProhibited – Prevents the object from being modified by an Update command.
TransferProhibited – Prevents the object from being transferred to another Registrar by the Transfer command.
RenewProhibited – Prevents a domain from being renewed by a Renew command.
DeleteProhibited – Prevents the object from being deleted by a Delete command.

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

Domain may be updated
Domain may be deleted, either within or after the add-grace period
Domain may be renewed at anytime during the term
Domain may be auto-renewed by the Registry
Domain may be transferred to another registrar.

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

27.1.1 Registration States

Domain Lifecycle – Registration States

As described above the .MUSIC registry will implement a standard domain lifecycle found in most gTLD registries today. There are five possible domain states:

Active
Inactive
Locked
Pending Transfer
Pending Delete.

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

Active State

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

Inactive State

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

Locked State

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

Pending Transfer State

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

Pending Delete State

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

27.1.2 Typical Registration Lifecycle Activities

Domain Creation Process

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

1. Contact objects are created in the SRS database. The same contact object may be used for each contact type, or they may all be different. If the contacts already exist in the database this step may be skipped.
2. Nameservers are created in the SRS database. Nameservers are not required to complete the registration process; however any domain with less than 2 name servers will not be resolvable.
3. The domain is created using the each of the objects created in the previous steps. In addition, the term and any client statuses may be assigned at the time of creation.

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

Update Process

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

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

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

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

Renew Process

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

Transfer Process

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

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

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

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

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

Deletion Process

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

27.1.3 Applicable Time Elements

The following section explains the time elements that are involved.

Grace Periods

There are six grace periods:

- Add-Delete Grace Period (AGP)
- Renew-Delete Grace Period
- Transfer-Delete Grace Period
- Auto-Renew-Delete Grace Period
- Auto-Renew Grace Period
- Redemption Grace Period (RGP).

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

The following describes each of these grace periods in detail.

Add-Delete Grace Period

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

billing account.

Renew-Delete Grace Period

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

Transfer-Delete Grace Period

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

Auto-Renew-Delete Grace Period

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

Auto-Renew Grace Period

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

Redemption Grace Period

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

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

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

27.2 State Diagram

Figure 27-1 provides a description of the registration lifecycle.

The different states of the lifecycle are active, inactive, locked, pending transfer, and pending delete. Please refer to section 27.1.1 for detail description of each of these states. The lines between the states represent triggers that transition a domain from one state to another.

The details of each trigger are described below:

Create: Registry receives a create domain EPP command.

WithNS: The domain has met the minimum number of nameservers required by registry policy in order to be published in the DNS zone.

WithOutNS: The domain has not met the minimum number of nameservers required by registry policy. The domain will not be in the DNS zone.

Remove Nameservers: Domain's nameserver(s) is removed as part of an update domain EPP command. The total nameserver is below the minimum number of nameservers required by registry policy in order to be published in the DNS zone.

Add Nameservers: Nameserver(s) has been added to domain as part of an update domain EPP command. The total number of nameservers has met the minimum number of nameservers required by registry policy in order to be published in the DNS zone.

Delete: Registry receives a delete domain EPP command.

DeleteAfterGrace: Domain deletion does not fall within the add grace period.

DeleteWithinAddGrace: Domain deletion falls within add grace period.

Restore: Domain is restored. Domain goes back to its original state prior to the delete command.

Transfer: Transfer request EPP command is received.

Transfer Approve/Cancel/Reject: Transfer requested is approved or cancel or rejected.

TransferProhibited: The domain is in clientTransferProhibited and/or serverTranferProhibited status. This will cause the transfer request to fail. The domain goes back to its original state.

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

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

27.2.1 EPP RFC Consistency

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

27.3 Resources
The registration lifecycle and associated business rules are largely determined by policy and business requirements; as such the Product Management and Policy teams will play a critical role in working with Amazon EU S.à r.l. to determine the precise rules that meet the requirements of the TLD. Implementation of the lifecycle rules will be the responsibility of Development/Engineering team, with testing performed by the Quality Assurance team.
Neustar's SRS implementation is very flexible and configurable, and in many case development is not required to support business rule changes.
The .MUSIC registry will be using standard lifecycle rules, and as such no customization is anticipated. However should modifications be required in the future, the necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:
Development/Engineering – 19 employees
Registry Product Management – 4 employees
These resources are more than adequate to support the development needs of all the TLDs operated by Neustar, including the .MUSIC registry.

---

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

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

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

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

from registrants to process update, transfers, and deletion requests;
- Requiring multiple, unique points of contact to request and/or approve update, transfer, and deletion requests; and
- Requiring the notification of multiple, unique points of contact when a domain has been updated, transferred, or deleted.

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

28.1 Abuse Prevention and Mitigation

Amazon EU S.à r.l. and its registry service provider, Neustar, recognize that preventing and mitigating abuse and malicious conduct in the <.TLD> registry is an important and significant responsibility. Amazon EU S.à r.l. will leverage Neustar's extensive experience in establishing and implementing registration policies to prevent and mitigate abusive and malicious domain activity within the proposed <.TLD> space.

Amazon will provision <.TLD> domains to third parties in accordance with the TLD registration policy. Opportunities for abusive and malicious domain activity in <.TLD> are therefore very restricted but we will nonetheless abide by our obligations to ICANN. A responsible domain name registry works towards the eradication of abusive domain name registrations and malicious activity, which may include conduct such as:

• Illegal or fraudulent actions
•Spam
• Phishing
• Pharming
• Distribution of malware
• Fast flux hosting
• Botnets
• Malicious hacking
• Distribution of child pornography
• Online sale or distribution of illegal pharmaceuticals.

By taking an active role in researching and monitoring abusive domain name registration and malicious conduct, Neustar has developed the ability to efficiently work with various law enforcement and security communities to mitigate fast flux DNS-using botnets.

Policies and Procedures to Minimize Abusive Registrations

A registry must have the policies, resources, personnel, and expertise in place to combat such abusive registration and malicious conduct. Neustar, Amazon EU S.à r.l.'s registry services provider, has played a leading role in preventing of such abusive practices, and has developed and implemented a "domain takedown" policy. Amazon EU S.à r.l. also believes that combating abusive use of the DNS is important in protecting registrants.

Removing a domain name from the DNS before it can cause harm is often the best preventative measure for thwarting certain malicious conduct such as botnets and malware distribution. Because removing a domain name from the zone will stop all activity associated with the domain name, including websites and e-mail, the decision to remove a domain name from the DNS must follow a documented process, culminating in a determination that the domain name to be removed poses a threat to the security and stability of the Internet or the registry. Amazon EU S.à r.l., via Neustar, has an extensive, defined, and documented process for taking the necessary action of removing a domain from the zone when its presence in the zone poses a threat to the security and stability of the infrastructure of the Internet or the registry.

Abuse Point of Contact

As required by the Registry Agreement, Amazon EU S.à r.l. will establish and publish on its website a single abuse point of contact responsible for addressing inquiries from law enforcement and the public related to malicious and abusive conduct. Amazon EU S.à r.l. will also provide such information to ICANN before delegating any domain names in <.TLD>. This information shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of malicious conduct complaints, and a telephone number and mailing address for the primary contact. Amazon EU S.à r.l. will ensure that this information is accurate and current, and that updates are provided to ICANN if and when changes are made. In addition, the registry services provider for <.TLD>, Neustar, shall continue to have an additional point of contact for requests from registrars related to abusive domain name practices.

28.2 Policies Regarding Abuse Complaints

Amazon EU S.à r.l. will adopt an Acceptable Use Policy that (i) clearly defines the types of activities that will not be permitted in <.TLD>; (ii) reserves Amazon EU S.à r.l.'s right to lock, cancel, transfer or otherwise suspend or take down domain names violating the Acceptable Use Policy; and (iii) identify the circumstances under which Amazon EU S.à r.l. may share information with law enforcement. Amazon EU S.à r.l. will incorporate its <.TLD> Acceptable User Policy into its Registry-Registrar Agreement.

Under the <.TLD> Acceptable Use Policy, which is set forth below, Amazon EU S.à r.l. may lock down the domain name to prevent any changes to the domain name contact and nameserver information, place the domain name "on hold" rendering the domain name non-resolvable, transfer the domain name to another registrar and/or in cases in which the domain name is associated with an ongoing law enforcement investigation, Amazon EU S.à r.l. will coordinate with law enforcement to assist in the investigation as described in more detail below.

It is Amazon EU S.à r.l.'s intention that all <.TLD> domain names will be registered and used by eligible users and that only ICANN-accredited registrars that have signed a Registry-Registrar Agreement will be permitted to register <.TLD> domain names. Accordingly, the potential for abusive registrations and malicious conduct in the <.TLD> registry is expected to be limited. In the unlikely event that such abuse should occur, Amazon EU S.à r.l. will work with its registry services provider, Neustar, to implement the following policies and processes to prevent and mitigate such activities. Below is initial Acceptable Use Policy for the <.TLD> registry.

<.TLD> Acceptable Use Policy

This Acceptable Use Policy gives the <.TLD> registry the ability to quickly lock, cancel, transfer or take ownership of any <.TLD> domain name, either temporarily or permanently, if the domain name is being used in a manner that appears to threaten the stability, integrity or security of the <.TLD> registry, or any of its registrar partners – and/or that may put the safety and security of any registrant or user at risk. The process also allows the <.TLD> registry to take preventive measures to avoid any such criminal or security threats.

The Acceptable Use Policy may be triggered through a variety of channels, including, among other things, private complaint, public alert, government or enforcement agency outreach, and the on-going monitoring by the <.TLD> registry or its partners. In all cases, the <.TLD> registry or its designees will alert <.TLD> registry's registrar partners about any identified threats and will work closely with them to bring offending sites into compliance.

The following are some (but not all) activities that may be subject to rapid domain compliance:

- Phishing: the attempt to acquire personally identifiable information by masquerading as a website other than <.TLD>'s own.
- Pharming: the redirection of Internet users to websites other than those the user intends to visit, usually through unauthorized changes to the Hosts file on a victim's computer or DNS records in DNS servers.
- Dissemination of Malware: the intentional creation and distribution of "malicious" software designed to infiltrate a computer system without the owner's consent, including, without limitation, computer viruses, worms, key loggers, and Trojans.
- Malicious Fast Flux Hosting: a technique used to shelter Phishing, Pharming and Malware sites and networks from detection and to frustrate methods employed to defend against such practices, whereby the IP address associated with fraudulent websites are changed rapidly so as to make the true location of the sites difficult to find.
- Botnetting: the development and use of a command, agent, motor, service, or software which is implemented: (1) to remotely control the computer or computer system of an Internet user without their knowledge or consent, (2) to generate direct denial of service (DDOS) attacks.
- Malicious Hacking: the attempt to gain unauthorized access (or exceed the level of authorized access) to a computer, information system, user account or profile, database, or security system.
- Child Pornography: the storage, publication, display and/or dissemination of pornographic materials depicting individuals under the age of majority in the relevant jurisdiction.

The <.TLD> registry reserves the right, in its sole discretion, to take any administrative and operational actions necessary, including the use of computer forensics and information security technological services, among other things, in order to implement the Acceptable Use Policy. In addition, the <.TLD> registry reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of the <.TLD> registry as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement, or (5) to correct mistakes made by the <.TLD> registry or any Registrar in connection with a domain name registration. The <.TLD> registry also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

Taking Action Against Abusive and/or Malicious Activity

The <.TLD> registry is committed to acting in a timely manner against those domain names associated with abuse or malicious conduct in violation of the Acceptable Use Policy. After a complaint is received from a trusted source or third-party, or detected by the <.TLD> registry, the registry will use commercially reasonable efforts to verify the information in the complaint. If that information can be verified to the best of the registry's ability, the sponsoring registrar will be notified and have 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. If the registrar has not acted

when the 12-hour period ends (i.e., is unresponsive to the request or refuses to take action), the <.TLD> registry will place the domain on “ServerHold”. (It is unlikely a registrar will not timely act because Amazon EU S.à r.l. intends to use a registrar contract reflecting these policies). ServerHold removes the domain name from the <.TLD> zone, but the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

Coordination with Law Enforcement

Amazon EU S.à r.l. will obtain assistance from Neustar to meet its obligations under Section 2.8 of the Registry Agreement to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the <.TLD> registry. The <.TLD> registry will respond to legitimate law enforcement inquiries promptly upon receiving the request.

The response shall include, at a minimum, an acknowledgement of receipt of the request, questions or comments concerning the request, and an outline of the next steps to be taken by Amazon EU S.à r.l. for rapid resolution of the request. If the request involves any of the activities that can be validated by the registry and implicates activity covered by the <.TLD> Acceptable Use Policy, the sponsoring registrar will have 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. The <.TLD> Registry will place the domain on “ServerHold” if the registrar has not acted within the 12-hour period.

Monitoring for Malicious Activity

Neustar, <.TLD>’s registry services provider, has developed and implemented an active “domain takedown” policy in which the registry itself takes down abusive domain names.

Neustar targets domain names verified to be abusive and removes them within 12 hours regardless of whether the domain name registrar cooperated. Neustar has determined that the benefit in removing such threats outweighs any potential damage to the registrar⁄registrant relationship. Amazon EU S.à r.l.’s registration policies make it unlikely that any <.TLD> domains will be taken down. Moreover, only registrars that contractually agree to cooperate in stemming abusive behaviors will be permitted to register <.TLD> domain names.

Neustar’s active prevention policies stem from the notion that registrants in <.TLD> have a reasonable expectation that they control the data associated with their domains, especially its presence in the DNS zone. Removing a domain name from the DNS before it can cause harm is often the best preventative measure for thwarting certain malicious conduct such as botnets and malware distribution that harms not only the domain name registrant, but also potentially millions of unsuspecting Internet users.

Rapid Takedown Process

Since implementing the program, Neustar has developed two basic variations of the process. The more common process variation is a lightweight process that is triggered by “typical” notices. The less common variation is the full process that is triggered by unusual notices, which generally allege that a domain name is being used to threaten the stability and security of the TLD, or is part of a real-time investigation by law enforcement or security researchers. In these cases, accelerated action by the registry is necessary. These processes are described below.

Lightweight Process

In addition to having an active Information Security group that, on its own initiatives, seeks out abusive practices in the <.TLD> registry, Neustar is an active member in a number of security organizations that have the expertise and experience in receiving and investigating reports of abusive DNS practices, including but not limited to, the Anti-Phishing Working Group, Castle Cops, NSP-SEC, the Registration Infrastructure Safety Group and others. Each of these sources is a well-known security organization that has a reputation for preventing abuse and malicious conduct on the Internet. Aside from these organizations, Neustar also actively participates in privately run security associations that operate based on trust and anonymity, making it much easier to obtain information regarding abusive DNS activity.

Once a complaint is received from a trusted source or third-party, or detected by Neustar’s internal security group, information about the abusive practice is forwarded to an internal mail distribution list that includes members of Neustar’s operations, legal, support, engineering, and security teams for immediate response (“CERT Team”). Although the impacted URL is included in the notification e-mail, the CERT Team is trained not to investigate the URLs themselves because the URLs in question often have scripts, bugs, etc. that can compromise the individual’s own computer and the network safety. Rather, the investigation is conducted by CERT team members who can access the URLs in a laboratory environment to avoid compromising the Neustar network. The lab environment is designed specifically for these types of tests and is scrubbed on a regular basis to ensure that none of Neustar’s internal or external network elements are harmed in any fashion.
Once the complaint has been reviewed and the alleged abusive domain name activity is verified to the best of the ability of the CERT Team, the sponsoring registrar has 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion,

or (b) provide the registry with a compelling argument why to keep the domain name in the zone.
The <.TLD> Registry will place the domain on “ServerHold” if the registrar has not acted within the 12-hour period.
ServerHold removes the domain name from the <.TLD> zone, but the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement.

Full Process

In the unlikely event that Neustar receives a complaint that claims that a domain name is being used to threaten the stability and security of the <.TLD> registry, or is a part of a real-time investigation by law enforcement or security, Neustar follows a slightly different course of action.
Upon initiation of this process, members of the CERT Team are paged and a teleconference bridge is immediately opened up for the CERT Team to assess whether the activity warrants immediate action. If the CERT Team determines the incident is not an immediate threat to the security and the stability of critical Internet infrastructure, the CERT Team provides documentation to the Neustar Network Operations Center to clearly capture the rationale for the decision and either refers the incident to the Lightweight process set forth above or closes the incident.

However, if the CERT TEAM determines that there is a reasonable likelihood that the incident warrants immediate action, a determination is made to immediately remove the domain from the zone. As such, Customer Support will contact the registrar immediately to communicate that there is a domain involved in a security and stability issue. The registrar is provided only the domain name in question and the broadly stated type of incident.

Coordination with Law Enforcement & Industry Groups

Neustar has a close working relationship with a number of law enforcement agencies, both in the United States and Internationally. For example, in the United States, Neustar is in constant communication with the Federal Bureau of Investigation, US CERT, Homeland Security, the Food and Drug Administration, and the National Center for Missing and Exploited Children.
Neustar also participates in a number of industry groups aimed at sharing information among key industry players about the abusive registration and use of domain names. These groups include the Anti-Phishing Working Group and the Registration Infrastructure Safety Group (where Neustar served for several years on the Board of Directors). Through these organizations and others, Neustar proactively shares information with other registries, registrars, ccTLDs, law enforcement, security professionals, etc. not only on abusive domain name registrations within its own TLDs, but also with respect to information uncovered with respect to domain names in other registries’ TLDs. Neustar has often found that rarely are abuses found only in the TLDs for which it manages, but also within other TLDs, such as .com and .info. Neustar routinely provides this information to the other registries so that the relevant registry can take the appropriate action.

With the assistance of Neustar as its registry services provider, Amazon EU S.à r.l. can meet its obligations under Section 2.8 of the Registry Agreement to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its <.TLD> registry. Amazon EU S.à r.l. and/or Neustar will respond to legitimate law enforcement inquiries promptly upon receiving the request. Such response shall include, at a minimum, an acknowledgement of receipt of the request, questions or comments concerning the request, and an outline of the next steps to be taken by Amazon EU S.à r.l. and/or Neustar for rapid resolution of the request.
If the request involves any of the activities that can be validated by the registry and/or Neustar and implicates the type of activity set forth in the Acceptable Use Policy, the sponsoring registrar will have 12 hours to investigate the activity further and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. The <.TLD> registry will place the domain on “ServerHold” if the registrar has not acted within the 12-hour period.

28.3 Measures for Removal of Orphan Glue Records

As the Security and Stability Advisory Committee of ICANN (SSAC) rightly acknowledges, although orphaned glue records may be used for abusive or malicious purposes, the “dominant use of orphaned glue supports the correct and ordinary operation of the DNS.” See http://www.icann.org/en/committees/security/sac048.pdf.

While orphan glue often support correct and ordinary operation of the DNS, such glue records can be used maliciously to point to name servers that host domains used in illegal phishing, bot-nets, malware, and other abusive behaviors. Problems occur when the parent domain of the glue record is deleted but its children glue records still remain in DNS. Therefore, when the <.TLD> registry has written evidence of actual abuse of orphaned glue, the <.TLD> registry will act to remove those records from the zone to mitigate such malicious conduct.

Neustar runs a daily audit of entries in its DNS systems and compares those with its provisioning system, which serves as an umbrella protection that items in the DNS zone are valid. Any DNS record that shows up in the DNS zone but not in the provisioning system is flagged for investigation and removed if necessary. This daily DNS audit prevents not only orphaned hosts but also other records that should not be in the zone.

In addition, if either Amazon EU S.à r.l. or Neustar becomes aware of actual abuse on orphaned glue after receiving written notification from a third party through its Abuse Contact or through its customer support, such glue records will be removed from the zone.

28.4 Measures to Promote WHOIS Accuracy

The <.TLD> registry will implement several measures to promote Whois accuracy.
Whois service for Amazon EU S.à r.l. will operate as follows. The registry will keep all basic contact details for each domain name in a unique internal system, which facilitates access to the domain information. In addition, Amazon EU S.à r.l. will perform internal monitoring checks and procedures that will only allow accurate Whois information and remove outdated data.

28.4.1. Authentication of Registrant Information

Amazon EU S.à r.l. will guarantee the adequate authentication of registrant data, ensuring the highest levels of accuracy and diligence when dealing with Whois data. In doing so, Amazon EU S.à r.l.'s solid internal system will undertake, but not be limited to the following measures: running checks against Whois internal records and regular verification of all contact details and other relevant registrant information. The registrar will also be charged with regularly checking Whois accuracy.

Amazon EU S.à r.l. will have a well-defined registration policy that will include a requirement that complete and accurate registrant details are provided by the requestor for a domain. These details will be validated by the registrar who will have a contractual duty to comply with Amazon EU S.à r.l.'s registration policy. The full details of every domain requestor will be kept in Amazon EU S.à r.l.'s on-line registry management dashboard which can be accessed by Amazon EU S.à r.l.'s Domain Management Team at any time.

28.4.2. Regular Monitoring of Registration Data

Amazon EU S.à r.l. will comply with ICANN's Whois requirements. Among other measures, Amazon EU S.à r.l. will regularly remind its internal personnel to comply with ICANN's Whois information Policy through regularly checking Whois data against internal records, offering Whois accuracy services, evaluating claims of fraudulent Whois data, and cancelling domain name registrations with outdated Whois details.

28.4.3. Policies and Procedures ensuring compliance

Amazon EU S.à r.l.'s Registry-Registrar Agreement will require a registrar to take steps necessary to ensure Whois data is complete and accurate and to implement the <.TLD> registration policies.

28.5 Resourcing Plans

Responsibility for abuse mitigation rests with a variety of functional groups at Neustar. The Neustar Abuse Monitoring team is primarily responsible for providing analysis and conducting investigations of reports of abuse. The Neustar Customer Service team also plays an important role in assisting with investigations, responding to customers, and notifying registrars of abusive domains. Finally, the Neustar Policy⁄Legal team is responsible for developing the relevant policies and procedures.

The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:

Customer Support – 12 employees

Policy⁄Legal – Two employees

The resources are more than adequate to support the abuse mitigation procedures of the <.TLD> registry.

Furthermore, Amazon EU S.à r.l. dedicates significant financial and personnel resources to combating malicious and abusive behavior in the DNS and across the internet. Amazon EU S.à r.l. will extend these resources to designating the unique abuse point of contact, regularly monitoring potential abusive and malicious activities with support from dedicated technical staff, analyzing reported abuse and malicious activity, and acting to address such reported activity.

The designated abuse prevention staff within Neustar and Amazon EU S.à r.l. will be subject to regular evaluations, receive adequate training and work under expert supervision. The abuse prevention resources will comprise both internal staff and external abuse prevention experts who would give extra advice and support when necessary. This external staff includes one legal expert and four operational experts.

Please note that in the above answer the terms "We", "Our" and "Amazon" may refer to either the applicant Amazon EU S.à r.l. or Amazon.com Inc., the ultimate parent, or sometimes NeuStar, the registry services provider.

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

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

>To be eligible for a score of 2, answers must also include additional measures specific to rights protection, such as abusive use policies, takedown procedures, registrant pre-verification, or authentication procedures, or other covenants.
A complete answer is expected to be no more than 10 pages.

29.1 Introduction

Amazon is applying for <.TLD> to provide a dedicated platform for stable and secure online communication and interaction. Amazon has several thousand registered intellectual property assets of all types including trademarks, designs, and domain names – we place the protection of our intellectual property as a high priority and we respect the intellectual property of others.

29.1.1 Rights protection in gTLD registry operation is a core objective of Amazon

We will require registrars to work with us on a four-step registration process featuring: (i) Eligibility Confirmation; (ii) Naming Convention Check; (iii) Acceptable Use Review; and (iv) Registration. As stated in our answer to Question 18, all domains in our registry will be subject to eligibility requirements.

We believe that the above registration process will ensure that abusive registrations are prevented, but we will continue to monitor ICANN policy developments, and update our procedures as required.

29.2 Core measures to prevent abusive registrations

To further prevent abusive registration or cybersquatting, we will adopt the following Rights Protection Mechanisms (RPMs) which have been mandated for new gTLD operators by ICANN:
• A 30 day Sunrise process
• A 60 day Trademark Claims process

Generally, these RPMs are targeted at abusive registrations undertaken by third parties. However, domains in our registry will be registered by Amazon and eligible trusted third parties through registrars who will be contractually required to ensure that stated rules covering eligibility and use of a domain are adhered to through a validation process. As a result, abusive registrations should be prevented.

29.2.1 Sunrise Eligibility

Our Sunrise Eligibility Requirements will clearly set out criteria for registration in this TLD. Notice of our Sunrise will be provided to third party holders of validated trademarks in the Trademark Clearinghouse as required by ICANN. Our Sunrise Eligibility Requirements will be published on the website of our registry.

29.2.2 Sunrise Window

As required in the Applicant Guidebook in section 7.1, our Sunrise window will recognize "all word marks: (i) nationally or regionally registered and for which proof of use – which can be a declaration and a single specimen of current use – was submitted to, and validated by, the Trademark
Clearinghouse; or (ii) that have been court-validated; or (iii) that are specifically protected by a statute or treaty currently in effect and that was in effect on or before 26 June 2008".

Our Sunrise window will last for 30 days. Applications received from an ICANN-accredited registrar will be accepted for registration if they are (i) supported by an entry in the Trademark Clearinghouse (TMCH) during our Sunrise window and (ii) satisfy our Sunrise Eligibility Requirements. Once registered, those domain names will normally have a one year term of registration. Any domain names registered will be managed by a registrar.

29.2.3 Sunrise Dispute Resolution Policy

We will devise and publish the rules for our Sunrise Dispute Resolution Policy (SDRP) on our registry website. Our SDRP will allow any party to raise a challenge on the following four grounds as required in the Applicant Guidebook (6.2.4):

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

Complaints can be submitted through our registry website within 30 days following the closure of the Sunrise, and will be initially processed by a registrar which will promptly report to us: (i) the challenger; (ii) the challenged domain name; (iii) the grounds upon which the complaint is based; and (iv) why the challenger believes the grounds are satisfied.

29.2.4 Trademark Claims Service

Our Trademark Claims Service (TMCS) will run for a 60 day period following the closure of our 30 day Sunrise. Our TMCS will be supported by the Trademark Clearinghouse and will provide a notice to third parties interested in filing a character string in our registry of a registered trademark right that matches the character string in the TMCH.

We will honor and recognize in our TMCS the following types of marks as defined in the Applicant Guidebook section 7.1: (i) nationally or regionally registered; (ii) court-validated; or (iii) specifically protected by a statute or treaty in effect at the time the mark is submitted to the Clearinghouse for inclusion.

Once received from the TMCH, with which our registry provider will interface, a claim will be initially processed by a registrar who will provide a report to us on the eligibility of the applicant.

29.2.5 Implementation and Resourcing Plans of core services to prevent abusive registration

Our Sunrise and IP Claims service will be introduced with the following timetable:

Day One: Announcement of Registry Launch and publication of registry website with details of the Sunrise and Trademark Claim Service (“TMCS”)
Day 30: Sunrise opens for 30 days on a first-come, first served basis. Once registrations are approved, they will be entered into the Shared Registry System (SRS) and published in our Thick-Whois database.
Day 60-75: Registry Open, domains applied for in the Sunrise registered and TMCS begins for a minimum of 60 days

Day 120-135: TMCS ends; normal operations continue.

Our Implementation Team will comprise the following:

From Amazon: the Director of IP will lead a team of up to seven experts with experience of domain name management and on-line legal dispute resolution, with access to other teams in Amazon Legal if required.

From NeuStar, registry service provider to Amazon: A Customer Support team of 12, a Product Management Team of four and a Development ⁄ Engineering Team of 19 will be available as required to support the legal team, led by Jeff Neuman. This team has over 10 years’ experience with implementing registry launches including rights protection schemes such as the .biz Sunrise and IP Claims.

In addition, Amazon will be supported externally by two legal specialists, four client managers and six operational staff. The operational staff will undertake the validation checks on registration requests.
The Implementation Team will create a formal Registry Launch plan. This plan will set out the exact process for the launch of each Amazon registry and will define responsibilities and budgets. The Registry website, which is budgeted for in the three year plans provided in our answers to Question 46, will feature Rules of Registration, Rules of Eligibility, Terms & Conditions of Registration, Acceptable Use Policies as well as the Rules of the Sunrise, the Rules of the Sunrise Dispute Resolution Policy and the Rules of the Trademark Claims Service.

Technical implementation between the registry and the Trademark Clearinghouse will be undertaken by the registry service provider as soon as practical after the Trademark Clearinghouse is operational and announces its integration process.

As demonstrated in our answer to question 46, a budget has been set aside to pay fees charged by the Trademark Clearinghouse Operator for this integration.

The contract we have with our registrars (the RRA) will require that registrars use the TMCH, adhere to the Terms & Conditions of the TMCH and will prohibit registrars from filing domains in our registries on their own behalf or utilizing any data from the TMCH except in the provision of their duties as a registrar.

When processing TMCS claims, our registrars will be required to use the specific form of notice provided by ICANN in the Applicant Guidebook.
We will also require our registrars to implement appropriate privacy policies reflecting local requirements. For example, Amazon is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union.

29.3 Mechanisms to identify and address the abusive use of registered domain names on an ongoing basis

To prevent the abusive use of registered domain names on an ongoing basis we will adopt the following Rights Protection Mechanisms (RPMs) which have been mandated by ICANN:

- The Uniform Domain Name Dispute Resolution Policy (UDRP) to address domain names that have been registered and used in bad faith in the TLD.

- The Uniform Rapid Suspension (URS) scheme which is a faster, more efficient alternative to the Uniform Dispute Resolution Policy to deal with clear-cut cases of cybersquatting.

- The Post Delegation Dispute Resolution Procedure (PDDRP).

- Implementation of a Thick WHOIS making it easier for rights holders to identify and locate infringing parties.

The UDRP and the URS are targeted at abusive registrations undertaken by third parties and the PDDRP at so called “Bad Actor” registries.

Abusive behavior by eligible registrants will be prevented by our internal processes, for example the pre-registration validation checks and monitoring of use of our registrars.

We acknowledge that we are subject to the UDRP, the URS and the PDDRP and we will co-operate fully with ICANN and appropriate registries in the unlikely circumstances that complaints are made.

29.3.1 The Uniform Dispute Resolution Policy (UDRP)

The UDRP is an out-of-court dispute resolution mechanism for trademark owners to resolve clear cases of bad faith, abusive registration and use of domain names. The UDRP applies by contract to all domain name registrations in gTLDs. Standing to file a UDRP complaint is limited to trademark owners who must demonstrate their rights. To prevail in a UDRP complaint, the complainant must further demonstrate that the domain name registrant has no rights or legitimate interests in the disputed domain name, and that the disputed domain name has been registered and is being used in bad faith. In the event of a successful claim, the infringing domain name registration is transferred to the complainant’s control.

In the event of a UDRP case ordering transfer of a domain name to a UDRP complainant, any transfer would be subject to the prevailing party meeting the registration eligibility requirements; if such requirements were not met, we may place the domain name that is the subject of the successful complaint on a list that prevents it from being registered again.

29.3.2 The URS

The URS is intended to be a lighter, quicker complement to the UDRP. Like the UDRP, it is intended for clear-cut cases of trademark abuse. Under the URS, the only remedy which a panel may grant is the temporary suspension of a domain name for the duration of the registration period (which may be extended by the prevailing complainant for one year, at commercial rates). URS substantive criteria mirror those of the UDRP but with a higher burden of proof for complainants, and additional registrant defences. Once a determination is rendered, a losing registrant has several appeal possibilities from 30 days up to one year. Either party may file a de novo appeal within 14 days of a decision. There are penalties for filing “abusive complaints” which may result in a ban on future URS filings.

Should a complaint be made, we will respond in a timely fashion, reflecting our contractual responsibility to ICANN as a registry operator.
Should a successful complaint be made, we will suspend the domain name for the duration of the registration period.
We will co-operate with the URS panel providers and panelists as we will co-operate with UDRP panel providers and panelists.

29.3.3 The Post-Delegation Dispute Resolution Procedure (PDDRP)

The PDDRP is an administrative option for trademark owners to file an objection against a registry whose “affirmative conduct” in its operation or use of its gTLD is alleged to cause or materially contribute to trademark abuse. In this way, the PDDRP is intended to act as a higher-level enforcement tool to assist ICANN compliance activities, where rights holders may not be able to continue to turn solely to lower-level multijurisdictional enforcement options in a vastly expanded DNS.

The PDDRP involves a number of procedural layers, such as an administrative compliance review, appointment of a “threshold review panel”, an expert determination as to liability under the procedure (with implementation of any remedies at ICANN’s discretion), a possible de novo appeal and further appeal to arbitration under ICANN’s registry terms. The PDDRP requires specific bad faith conduct including profit from encouraging infringement in addition to “the typical registration fee.”

As set out in the Applicant Guidebook in the appendix summarizing the PDDRP, the grounds for a complaint on a second level registration are that, “(a) there is a substantial pattern or practice of specific bad faith intent by the registry operator to profit from the sale of trademark infringing domain names; and (b) the registry operator’s bad faith intent to profit from the systematic registration of domain names within the gTLD that are identical or confusingly similar to the complainant’s mark, which (i) takes unfair advantage of the distinctive character or the reputation of the complainant’s mark or (ii) impairs the distinctive character or the reputation of the complainant’s mark, or(iii) creates a likelihood of confusion with the complainant’s mark.”

29.3.4 Thick Whois

As required in Specification 4 of the Registry agreement, all Amazon registries will provide Thick Whois. A Thick WHOIS provides a centralized location of registrant information within the control of the registry (as opposed to thin Whois where the data is dispersed across registrars).
Thick Whois will provide rights owners and law enforcement with the ability to review the registration record easily.

We will place a requirement on registrars to ensure that all registrations are filed with accurate Whois details.
Amazon will create and publish a Whois Query email address so that third parties can submit queries about any domains in our registry.

29.3.5 Implementation and Resourcing Plans for mechanisms to identify and address the abusive use of registered domain names on an ongoing basis

Our post-launch rights protection mechanisms will be in place from Day One of the launch of the registry.

To ensure that we are compliant with our obligations as a registry operator, we will develop a section of our registry website to assist third parties involved in UDRP, URS and PDDRP complaints including third parties wishing to make a complaint, ICANN compliance staff and the providers of UDRP and URS panels. This will feature an email address for enquiries relating to disputes or seeking further information on specific domains. We will monitor this address for all of the following: Notice of Complaint, Notice of Default, URS Determination, UDRP Determination, Notice of Appeal and Appeal Panel Findings where appropriate.

As stated in our answer to Question 18, Amazon’s Intellectual Property group will be responsible for the development, maintenance and enforcement of the Domain Management Policy. This will include ensuring that the following implementation targets are met:

- Locking domains that are the subject of URS complaints within 24 hours of receipt of a URS complaint, and ensuring a registrar locks domains that are the subject of UDRP complaints within 24 hours of receipt of a UDRP complaint.

- Confirming the implementation of the lock to the relevant URS provider, and ensure a registrar confirms the implementation of the lock to the relevant UDRP provider.

- Ensuring that a registrar cancels domain names that are the subject of a successful UDRP complaint within 24 hours

- Redirecting servers to a website with the ICANN mandated information following a successful URS within 24 hours

The human resources dedicated to managing post-launch RPM include:

From Amazon: the Director of IP will lead a team of up to seven experts with experience of domain name management and on-line legal dispute resolution, with access to other teams in Amazon Legal if required.

From NeuStar, registry service provider to Amazon: A Customer Support team of 12, a Product

Management Team of four and a Development / Engineering Team of 19 will be available as required to support the legal team, led by Jeff Neuman. This team has over 10 years' experience with implementing registry launches including rights protection schemes including the .biz Sunrise and IP Claims.

In addition, Amazon will be supported externally by two legal specialists, four client managers and six operational staff. The operational staff will undertake the validation checks on registration requests.

We are confident that this staffing is more than adequate for the initial stages of registry operation. Of course, should business goals change requiring more resources, Amazon will closely review any expansion plans, and plan for additional financial, technical, and team-member support to put the Registry in the best position for success.

We will also require registrars to implement appropriate privacy policies reflecting the high standards that we operate. For information on our Privacy Policies, please see: http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496

29.4 Additional Mechanism that exceed requirements

Rights protection is at the core of Amazon's objective in applying for this registry. Therefore we are committed to providing the following additional mechanisms:

29.4.1 Registry Legal Manager

Amazon will appoint a Legal Manager to ensure that we are compliant with ICANN policies. The Legal Manager will also handle all disputes relating to RPMs. This will involve evaluating complaints, working with external legal counsel and law enforcement, and resolving disputes. The Legal Manager will also liaise with external stakeholders including URS and UDRP panel providers, the TMCH operator and trademark holders as needed.

29.4.2 Rights Protection Help Line

Amazon will maintain a Rights Protection Help Line. Calls to this line will be allocated a Case Number and the following details will be recorded: (i) the contact details of the complainant; (ii) the domain name that is the subject of the complaint or query; (iii) the registered right, if any, that is associated with the request; and (iv) an explanation of the concerns.
An initial response to a query or complaint will be made within 24 hours. The Rights Protection Help Line will be in place on Day One of the registry. The cost of the Rights Help Line is reflected in the Projections Templates provided at Question 46 as part of on-going registry maintenance costs.
The aim of the Rights Protection Help Line is to assist third parties in understanding the mission and purpose of our registry and to see if a resolution can be found that is quicker and easier than the filing of a UDRP or URS complaint.

The Legal Manager will oversee the Rights Protection Help Line.

29.4.3 Registrar Accreditation

Amazon may audit the performance of registrars every six months and re-validate our Registry-Registrar Agreements annually. Our audits may include site visits to ensure the security of data etc.

29.4.4 Audits of registration records

Every three months, whichever is the most of 250 or 2% of the total of domain names registered in that period will be reviewed with registrars to ensure accurate registration records and use that is compliant with our Acceptable Use guidelines.

29.4.5 Maintenance of Registry Website

Amazon will create a website for all our registries and we will make it easy for third parties including representatives of law enforcement to contact us by featuring our full contact details (physical, email address and phone number).

29.4.6 Click Wrapping our Terms & Conditions

We may bring to the attention of requestors of domain names the Terms & Conditions of registration and, especially, Acceptable Use terms through Click Wrapping.

29.4.7 Annual Report

Amazon will publish an Annual Report on Rights Protection in our registries on our Registry Website. This will include relevant statistics and it will outline all cases and how they were resolved.

29.4.8 Contacts with WIPO and other DRS providers

Amazon may invite representatives of WIPO and other DRS providers to review our RPMs and to make suggestions on any improvements that we might make after the first full year of

operation.

29.4.9 Registrant Pre-Verification

All requests for registration will be verified by registrars to ensure that they come from eligible applicants. A record of the request will be kept in our on-line domain management console including the requestor's email address and other contact information.

29.4.10 Take down Procedures

Amazon has described Takedown Procedures for domains supporting Abusive Behaviors in Question 28. We will reserve the right to terminate a registration and to take down all associated services after a review by our Legal Manager if a takedown for reasons of rights protection is requested by law enforcement, a representative of a court we recognize etc.

29.4.11 Speed of Response

Wherever possible, as outlined above, Amazon is committed to a response within 24 hours of a complaint being made. This exceeds the guidelines for the UDRP and the URS.

Please note that in the above answer the terms "We", "Our" and "Amazon" may refer to either the applicant Amazon EU S.à r.l. or Amazon.com Inc., the ultimate parent.

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

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

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

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

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

Amazon EU S.à r.l. and our back-end operator, Neustar, recognize the vital need to secure the systems and the integrity of the data in commercial solutions. The .MUSIC registry solution will leverage industry-best security practices including the consideration of physical, network, server, and application elements.
Neustar's approach to information security starts with comprehensive information security policies. These are based on the industry best practices for security including SANS (SysAdmin, Audit, Network, Security) Institute, NIST (National Institute of Standards and Technology), and Center for Internet Security (CIS). Policies are reviewed annually by Neustar's information security team.
The following is a summary of the security policies that will be used in the .MUSIC registry, including:
1. Summary of the security policies used in the registry operations
2. Description of independent security assessments
3. Description of security features that are appropriate for .MUSIC
4. List of commitments made to registrants regarding security levels

All of the security policies and levels described in this section are appropriate for the .MUSIC registry.
30.(a).1 Summary of Security Policies

Neustar, Inc. has developed a comprehensive Information Security Program in order to create effective administrative, technical, and physical safeguards for the protection of its information assets, and to comply with Neustar's obligations under applicable law, regulations, and contracts. This Program establishes Neustar's policies for accessing, collecting, storing, using, transmitting, and protecting electronic, paper, and other records containing sensitive information.
The Program defines:

The policies for internal users and our clients to ensure the safe, organized and fair use of information resources.
The rights that can be expected with that use.
The standards that must be met to effectively comply with policy.
The responsibilities of the owners, maintainers, and users of Neustar's information resources.
Rules and principles used at Neustar to approach information security issues

The following policies are included in the Program:

1. Acceptable Use Policy

The Acceptable Use Policy provides the "rules of behavior" covering all Neustar Associates for using Neustar resources or accessing sensitive information.

2. Information Risk Management Policy

The Information Risk Management Policy describes the requirements for the on-going information security risk management program, including defining roles and responsibilities for conducting and evaluating risk assessments, assessments of technologies used to provide information security and monitoring procedures used to measure policy compliance.

3. Data Protection Policy

The Data Protection Policy provides the requirements for creating, storing, transmitting, disclosing, and disposing of sensitive information, including data classification and labeling requirements, the requirements for data retention. Encryption and related technologies such as digital certificates are also covered under this policy.

4. Third Party Policy

The Third Party Policy provides the requirements for handling service provider contracts, including specifically the vetting process, required contract reviews, and on-going monitoring of service providers for policy compliance.

5. Security Awareness and Training Policy

The Security Awareness and Training Policy provide the requirements for managing the on-going awareness and training program at Neustar. This includes awareness and training activities provided to all Neustar Associates.

6. Incident Response Policy

The Incident Response Policy provides the requirements for reacting to reports of potential security policy violations. This policy defines the necessary steps for identifying and reporting security incidents, remediation of problems, and conducting "lessons learned" post-mortem reviews in order to provide feedback on the effectiveness of this Program. Additionally, this policy contains the requirement for reporting data security breaches to the appropriate authorities and to the public, as required by law, contractual requirements, or regulatory bodies.

7. Physical and Environmental Controls Policy

The Physical and Environment Controls Policy provides the requirements for securely storing sensitive information and the supporting information technology equipment and infrastructure. This policy includes details on the storage of paper records as well as access to computer systems and equipment locations by authorized personnel and visitors.

8. Privacy Policy

Neustar supports the right to privacy, including the rights of individuals to control the dissemination and use of personal data that describes them, their personal choices, or life experiences. Neustar supports domestic and international laws and regulations that seek to protect the privacy rights of such individuals.

9. Identity and Access Management Policy

The Identity and Access Management Policy covers user accounts (login ID naming convention, assignment, authoritative source) as well as ID lifecycle (request, approval, creation, use, suspension, deletion, review), including provisions for system/application accounts, shared/group accounts, guest/public accounts, temporary/emergency accounts, administrative access, and remote access. This policy also includes the user password policy requirements.

10. Network Security Policy

The Network Security Policy covers aspects of Neustar network infrastructure and the technical controls in place to prevent and detect security policy violations.

11. Platform Security Policy

The Platform Security Policy covers the requirements for configuration management of servers, shared systems, applications, databases, middle-ware, and desktops and laptops owned or operated by Neustar Associates.

12. Mobile Device Security Policy

The Mobile Device Policy covers the requirements specific to mobile devices with information storage or processing capabilities. This policy includes laptop standards, as well as requirements for PDAs, mobile phones, digital cameras and music players, and any other removable device capable of transmitting, processing or storing information.

13. Vulnerability and Threat Management Policy

The Vulnerability and Threat Management Policy provides the requirements for patch management, vulnerability scanning, penetration testing, threat management (modeling and monitoring) and the appropriate ties to the Risk Management Policy.

14. Monitoring and Audit Policy

The Monitoring and Audit Policy covers the details regarding which types of computer events to record, how to maintain the logs, and the roles and responsibilities for how to review, monitor, and respond to log information. This policy also includes the requirements for backup, archival, reporting, forensics use, and retention of audit logs.

15. Project and System Development and Maintenance Policy

The System Development and Maintenance Policy covers the minimum security requirements for all software, application, and system development performed by or on behalf of Neustar and the minimum security requirements for maintaining information systems.

30. (a).2 Independent Assessment Reports

Neustar IT Operations is subject to yearly Sarbanes-Oxley (SOX), Statement on Auditing Standards #70 (SAS70) and ISO audits. Testing of controls implemented by Neustar management in the areas of access to programs and data, change management and IT Operations are subject to testing by both internal and external SOX and SAS70 audit groups. Audit Findings are communicated to process owners, Quality Management Group and Executive Management. Actions are taken to make process adjustments where required and remediation of issues is monitored by internal audit and QM groups.

External Penetration Test is conducted by a third party on a yearly basis. As authorized by Neustar, the third party performs an external Penetration Test to review potential security weaknesses of network devices and hosts and demonstrate the impact to the environment. The assessment is conducted remotely from the Internet with testing divided into four phases:

A network survey is performed in order to gain a better knowledge of the network that was being tested

Vulnerability scanning is initiated with all the hosts that are discovered in the previous phase

Identification of key systems for further exploitation is conducted

Exploitation of the identified systems is attempted.

Each phase of the audit is supported by detailed documentation of audit procedures and results. Identified vulnerabilities are classified as high, medium and low risk to facilitate management's prioritization of remediation efforts. Tactical and strategic recommendations are provided to management supported by reference to industry best practices.

30.(a).3 Augmented Security Levels and Capabilities

There are no increased security levels specific for .MUSIC. However, Neustar will provide the same high level of security provided across all of the registries it manages.

A key to Neustar's Operational success is Neustar's highly structured operations practices. The standards and governance of these processes:

Include annual independent review of information security practices

Include annual external penetration tests by a third party

Conform to the ISO 9001 standard (Part of Neustar's ISO-based Quality Management System)

Are aligned to Information Technology Infrastructure Library (ITIL) and CoBIT best practices

Are aligned with all aspects of ISO IEC 17799

Are in compliance with Sarbanes-Oxley (SOX) requirements (audited annually)

Are focused on continuous process improvement (metrics driven with product scorecards reviewed monthly).

A summary view to Neustar's security policy in alignment with ISO 17799 can be found in section 30.(a).4 below.

30.(a).4 Commitments and Security Levels

The .MUSIC registry commits to high security levels that are consistent with the needs of the TLD. These commitments include:

Compliance with High Security Standards

Security procedures and practices that are in alignment with ISO 17799

Annual SOC 2 Audits on all critical registry systems

Annual 3rd Party Penetration Tests

Annual Sarbanes Oxley Audits

Highly Developed and Document Security Policies

Compliance with all provisions described in section 30.(a).4 below and in the attached security policy document.

Resources necessary for providing information security

Fully documented security policies

Annual security training for all operations personnel

High Levels of Registry Security

Multiple redundant data centers

High Availability Design

Architecture that includes multiple layers of security

Diversified firewall and networking hardware vendors

Multi-factor authentication for accessing registry systems

Physical security access controls

A 24x7 manned Network Operations Center that monitors all systems and applications

A 24x7 manned Security Operations Center that monitors and mitigates DDoS attacks

DDoS mitigation using traffic scrubbing technologies

New gTLD Application Submitted to ICANN by: Amazon EU S.à r.l.

Application Downloaded On: 01 May 2014

String: SONG

Application ID: 1-1317-53837

Applicant Information

1. Full legal name

Amazon EU S.à r.l.

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact nformation Redacted

4. Fax number

Contact nformation Redacted

5. If applicable, website or URL

http://www.amazon.com/

Primary Contact

6(a). Name

Lorna Gradden

6(b). Title

Operations Director

6(c). Address

6(d). Phone Number

Con ac nforma ion Redac ed

6(e). Fax Number

Contact nformation Redacted

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Dana Northcott

7(b). Title

Associate General Counsel, IP

7(c). Address

7(d). Phone Number

Contact nformation Redacted

7(e). Fax Number

Contact nformation Redacted

7(f). Email Address

Contact Informat on Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Corporation (Société à responsabilité limitée)

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

Luxembourg

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

Attachments are not displayed on this form.

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

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

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

Amazon EU S.à r.l. is not a joint venture.

Applicant Background

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

Name	Position

Allan Lyall	Manager
Eric Laurent Broussard	Manager
Eva Charlotte Gehlin	Manager
Gregory William Greeley	Manager
John Timothy Leslie	Manager

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

Name	Position
Allan Lyall	Manager
Eric Laurent Broussard	Manager
Eva Charlotte Gehlin	Manager
Gregory William Greeley	Manager
John Timothy Leslie	Manager

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

Name	Position
Amazon Europe Holding Technologies S.C.S.	Not Applicable

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

Applied-for gTLD string

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

SONG

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

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

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

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

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

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

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

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

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

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

15C. List any variants to the applied-for gTLD string according to the relevant IDN tables.

---

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

Neustar, Amazon EU S.à r.l.'s provider of back end registry services, confirms that it does not anticipate any problems in the operation or rendering of this ASCII string. The string conforms to accepted standards and poses no threat to the operational security and stability of the Internet.

---

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

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

Founded in 1994, Amazon opened on the World Wide Web in July 1995 and today offers Earth's Biggest Selection. Amazon seeks to be Earth's most customer-centric company, where customers can find and discover anything they might want to buy online, and endeavors to offer its customers the lowest possible prices. Amazon and other sellers offer millions of unique new, refurbished and used items in categories such as Books; Movies, Music & Games; Digital Downloads; Electronics & Computers; Home & Garden; Toys, Kids & Baby; Grocery; Apparel, Shoes & Jewelry; Health & Beauty; Sports & Outdoors; and Tools, Auto & Industrial. Amazon Web Services provides Amazon's developer customers with access to in-the-cloud infrastructure services based on Amazon's own back-end technology platform, which developers can use to enable virtually any type of business. The new latest generation Kindle is the lightest, most compact Kindle ever and features the same 6-inch, most advanced electronic ink display that reads like real paper even in bright sunlight. Kindle Touch is a new addition to the Kindle family with an easy-to-use touch screen that makes it easier than ever to turn pages, search, shop, and take notes – still with all the benefits of the most advanced electronic ink display. Kindle Touch 3G is the top of the line e-reader and offers the same new design and features of Kindle Touch, with the unparalleled added convenience of free 3G. Kindle Fire is the Kindle for movies, TV shows, music, books, magazines, apps, games and web browsing with all the content, free storage in the Amazon Cloud, Whispersync, Amazon Silk (Amazon's new revolutionary cloud-accelerated web browser), vibrant color touch screen, and powerful dual-core processor.

The mission of the <.TLD> registry is:

To provide a unique and dedicated platform while simultaneously protecting the integrity of Amazon's brand and reputation.

A <.TLD> registry will:

- Offer a stable and secure foundation for online communication and interaction.
- Provide a platform for innovation.

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

The <.TLD> registry will benefit registrants and internet users by offering a stable and secure foundation for online communication and interaction.

What is the goal of your proposed gTLD in terms of areas of specialty, service levels or reputation?

Amazon intends for its new <.TLD> gTLD to provide a unique and dedicated platform for stable and secure online communication and interaction. The <.TLD> registry will be run in line with current industry standards of good registry practice.

What do you anticipate your proposed gTLD will add to the current space in terms of competition, differentiation or innovation?

Amazon values the opportunity to be one of the first companies to own a gTLD.

A <.TLD> registry will:

- Offer a stable and secure foundation for online communication and interaction.
- Provide a platform for innovation.

What goals does your proposed gTLD have in terms of user experience?

Amazon intends for its new <.TLD> gTLD to provide a unique and dedicated platform for stable and secure online communication and interaction.

Provide a complete description of the applicant's intended registration policies in support of the goals above Amazon's Intellectual Property group will be responsible for the development, maintenance and enforcement of a Domain Management Policy. The Domain Management Policy will define (i) the rules associated with eligibility and domain name allocation, (ii) the license terms governing the use of a <.TLD> domain name, and (iii) the dispute resolution policies for the <.TLD> gTLD. Amazon will update the Domain Management Policy as needed to reflect the registry's business goals and, where appropriate, ICANN consensus policies.
Registration of a domain name in the <.TLD> registry will be undertaken in four steps: (i)

Eligibility Confirmation, (ii) Naming Convention Check, (iii) Acceptable Use Review, and (iv) Registration.

For example, on the rules of eligibility, each applied for character string must conform to the <.TLD> rules of eligibility. Each <.TLD> name must:

• be at least 1 character and no more than 63 characters long
• not contain a hyphen on the 3rd and 4th position (tagged domains)
• contain only letters (a-z), numbers (0-9) and hyphens or a combination of these
• start and end with an alphanumeric character, not a hyphen
• not match any character strings reserved by ICANN
• not match any protected country names or geographical terms

Additionally:

• Internationalized domain names (IDN) may be supported in the <.TLD> registry at the second level.
• The <.TLD> registry will respect third party intellectual property rights.

• All <.TLD> domains will carry accurate and up-to-date registration records.

Amazon's Intellectual Property group reserves the right to revoke a license to use a <.TLD> domain name, at any time, if any use of a <.TLD> domain name violates the Domain Management Policy.

Will your proposed gTLD impose any measures for protecting the privacy of confidential information of registrants or users?

Yes. Amazon will implement appropriate privacy policies respecting requirements of local jurisdictions. For example, Amazon is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union.

Describe whether and in what ways outreach and communications will help to achieve your projected benefits?

Amazon will assess the need to undertake public outreach or mass communication about its new gTLD registry in line with the goals for the TLD.

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

Amazon intends to initially provision a relatively small number of domains in the <.TLD> registry to support the goals of the TLD. These initiatives should not impose social costs of any type on consumers.

How will multiple applications for a particular domain be resolved, for example, by auction or on a first come first served basis?

Applications from eligible requestors for domains in the <.TLD> registry will be considered by Amazon's Intellectual Property group on a first come first served basis and allocated in line with the goals of the TLD.

Explain any cost benefits for registrants you intend to implement (e.g. advantageous pricing, introductory discounts, bulk registration discounts).
Domains in the <.TLD> registry will be provisioned to support the goals of the TLD. Accordingly, "cost benefits" may be explored depending on the goals of the TLD. Amazon shares the goals of enhancing customer trust and choice.

The Registry Agreement requires that registrars be offered the option to obtain initial domain name registrations for periods of one to ten years at the discretion of the registrar, but no greater than 10 years. Additionally the Registry Agreement requires advance written notice of price increases. Do you intend to make contractual commitments to registrants regarding the magnitude of price escalation?

The Domain Management Policy will include the costs and benefits of a unique and dedicated platform for stable and secure online communication and interaction.

---

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

No

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

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

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

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

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

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

21A. Is the application for a geographic name?

No

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

Amazon EU S.à r.l., with support of its ultimate parent company, Amazon.com, Inc. (collectively referred to in this response throughout as "Amazon"), is committed to managing the <.TLD> registry in full compliance with all applicable laws, consensus policies, ICANN guidelines, RFCs and the Specifications of the Registry Agreement. In the management of domain names in the <.TLD> registry, based on GAC advice and Specification 5, Amazon intends to block from initial registration all required domain names.

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

security or stability concerns.
The following registry services are customary services offered by a registry operator:

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

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

23.1 Introduction

Amazon EU S.à r.l. has elected to partner with Neustar, Inc. to provide back-end services for the .SONG registry. In making this decision, Amazon EU S.à r.l. recognized that Neustar already possesses a production-proven registry system that can be quickly deployed and smoothly operated over its robust, flexible, and scalable world-class infrastructure. The existing registry services will be leveraged for the .SONG registry. The following section describes the registry services to be provided.
23.2 Standard Technical and Business Components
Neustar will provide the highest level of service while delivering a secure, stable and comprehensive registry platform. Amazon EU S.à r.l. will use Neustar's Registry Services platform to deploy the .SONG registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to .SONG.

Registry-Registrar Shared Registration Service (SRS)
Extensible Provisioning Protocol (EPP)
Domain Name System (DNS)
WHOIS
DNSSEC
Data Escrow
Dissemination of Zone Files using Dynamic Updates
Access to Bulk Zone Files
Dynamic WHOIS Updates
IPv6 Support
Rights Protection Mechanisms
Internationalized Domain Names (IDN).

The following is a description of each of the services.
SRS
Neustar's secure and stable SRS is a production-proven, standards-based, highly reliable, and high-performance domain name registration and management system. The SRS includes an EPP interface for receiving data from registrars for the purpose of provisioning and managing domain names and name servers. The response to Question 24 provides specific SRS information.
EPP
The .SONG registry will use the Extensible Provisioning Protocol (EPP) for the provisioning of domain names. The EPP implementation will be fully compliant with all RFCs. Registrars are provided with access via an EPP API and an EPP based Web GUI. With more than 10 gTLD, ccTLD, and private TLDs implementations, Neustar has extensive experience building EPP-based registries. Additional discussion on the EPP approach is presented in the response to Question 25.
DNS
Amazon EU S.à r.l. will leverage Neustar's world-class DNS network of geographically distributed nameserver sites to provide the highest level of DNS service. The service utilizes "Anycast" routing technology, and supports both IPv4 and IPv6. The DNS network is highly proven, and currently provides service to over 20 TLDs and thousands of enterprise companies. Additional information on the DNS solution is presented in the response to Questions 35.
WHOIS
Neustar's existing standard WHOIS solution will be used for .SONG. The service provides supports for near real-time dynamic updates. The design and construction is agnostic with regard to data display policy is flexible enough to accommodate any data model. In addition, a searchable WHOIS service that complies with all ICANN requirements will be provided. The following WHOIS options will be provided:
Standard WHOIS (Port 43)
Standard WHOIS (Web)
Searchable WHOIS (Web)
DNSSEC
An RFC compliant DNSSEC implementation will be provided using existing DNSSEC capabilities. Neustar is an experienced provider of DNSSEC services, and currently manages signed zones for three large top level domains: .biz, .us, and .co. Registrars are provided with the ability to submit and manage DS records using EPP, or through a web GUI. Additional information on DNSSEC, including the management of security extensions is found in the response to Question

43.
Data Escrow
Data escrow will be performed in compliance with all ICANN requirements in conjunction with an approved data escrow provider. The data escrow service will:

- Protect against data loss
- Follow industry best practices
- Ensure easy, accurate, and timely retrieval and restore capability in the event of a hardware failure
- Minimizes the impact of software or business failure.

Additional information on the Data Escrow service is provided in the response to Question 38.
Dissemination of Zone Files using Dynamic Updates
Dissemination of zone files will be provided through a dynamic, near real-time process. Updates will be performed within the specified performance levels. The proven technology ensures that updates pushed to all nodes within a few minutes of the changes being received by the SRS. Additional information on the DNS updates may be found in the response to Question 35.
Access to Bulk Zone Files
Amazon EU S.à r.l. will provide third party access to the bulk zone file in accordance with specification 4, Section 2 of the Registry Agreement. Credentialing and dissemination of the zone files will be facilitated through the Central Zone Data Access Provider.
Dynamic WHOIS Updates
Updates to records in the WHOIS database will be provided via dynamic, near real-time updates. Guaranteed delivery message oriented middleware is used to ensure each individual WHOIS server is refreshed with dynamic updates. This component ensures that all WHOIS servers are kept current as changes occur in the SRS, while also decoupling WHOIS from the SRS. Additional information on WHOIS updates is presented in response to Question 26.
IPv6 Support
The .SONG registry will provide IPv6 support in the following registry services: SRS, WHOIS, and DNS/DNSSEC. In addition, the registry supports the provisioning of IPv6 AAAA records. A detailed description on IPv6 is presented in the response to Question 36.
Required Rights Protection Mechanisms
Amazon EU S.à r.l. will provide all ICANN required Rights Mechanisms, including:

- Trademark Claims Service
- Trademark Post-Delegation Dispute Resolution Procedure (PDDRP)
- Registration Restriction Dispute Resolution Procedure (RRDRP)
- UDRP
- URS
- Sunrise service.

More information is presented in the response to Question 29.
Internationalized Domain Names (IDN)

IDN registrations are provided in full compliance with the IDNA protocol. Neustar possesses extensive experience offering IDN registrations in numerous TLDs, and its IDN implementation uses advanced technology to accommodate the unique bundling needs of certain languages. Character mappings are easily constructed to block out characters that may be deemed as confusing to users. A detailed description of the IDN implementation is presented in response to Question 44.
23.3 Unique Services
Amazon EU S.à r.l. will not be offering services that are unique to .SONG.
23.4 Security or Stability Concerns
All services offered are standard registry services that have no known security or stability concerns. Neustar has demonstrated a strong track record of security and stability within the industry.

---

24. Shared Registration System (SRS) Performance:
describe

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

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

24.1 Introduction

Amazon EU S.à r.l. has partnered with Neustar, Inc., an experienced TLD registry operator, for the operation of the .SONG Registry. Amazon EU S.à r.l. is confident that the plan in place for the operation of a robust and reliable Shared Registration System (SRS) as currently provided by Neustar will satisfy the criterion established by ICANN.

Neustar built its SRS from the ground up as an EPP based platform and has been operating it reliably and at scale since 2001. The software currently provides registry services to five TLDs (.BIZ, .US, TEL, .CO and .TRAVEL) and is used to provide gateway services to the .CN and .TW registries. Neustar's state of the art registry has a proven track record of being secure, stable, and robust. It manages more than 6 million domains, and has over 300 registrars connected today.

The following describes a detailed plan for a robust and reliable SRS that meets all ICANN requirements including compliance with Specifications 6 and 10.

24.2 The Plan for Operation of a Robust and Reliable SRS

High-level SRS System Description

The SRS to be used for .SONG will leverage a production-proven, standards-based, highly reliable and high-performance domain name registration and management system that fully meets or exceeds the requirements as identified in the new gTLD Application Guidebook.

The SRS is the central component of any registry implementation and its quality, reliability and capabilities are essential to the overall stability of the TLD. Neustar has a documented history of deploying SRS implementations with proven and verifiable performance, reliability and availability. The SRS adheres to all industry standards and protocols. By leveraging an existing SRS platform, Amazon EU S.à r.l. is mitigating the significant risks and costs associated with the development of a new system. Highlights of the SRS include:

State-of-the-art, production proven multi-layer design
Ability to rapidly and easily scale from low to high volume as a TLD grows
Fully redundant architecture at two sites
Support for IDN registrations in compliance with all standards
Use by over 300 Registrars
EPP connectivity over IPv6
Performance being measured using 100% of all production transactions (not sampling).

SRS Systems, Software, Hardware, and Interoperability

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

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

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

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

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

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

SRS Design

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

Protocol Layer
Business Policy Layer
Database.

Each of the layers is described below.

Protocol Layer

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

horizontally scalable as dictated by volume.
The EPP servers authenticate against a series of security controls before granting service, as follows:

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

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

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

Business Policy Layer

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

Similar to the EPP protocol farm, the SRS consists of a farm of application servers within this layer. This design ensures that there is sufficient capacity to process every transaction in a manner that meets or exceeds all service level requirements. Some registries couple the business logic layer directly in the protocol layer or within the database. This architecture limits the ability to scale the registry. Using a decoupled architecture enables the load to be distributed among farms of inexpensive servers that can be scaled up or down as demand changes. The SRS today processes over 30 million EPP transactions daily.

Database

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

Figure 24-1 depicts the overall SRS architecture including network components.

Number of Servers

As depicted in the SRS architecture diagram above Neustar operates a high availability architecture where at each level of the stack there are no single points of failures. Each of the network level devices run with dual pairs as do the databases. For the .SONG registry, the SRS will operate with 8 protocol servers and 6 policy engine servers. These expand horizontally as volume increases due to additional TLDs, increased load, and through organic growth. In addition to the SRS servers described above, there are multiple backend servers for services such as DNS and WHOIS. These are discussed in detail within those respective response sections.

Description of Interconnectivity with Other Registry Systems

The core SRS service interfaces with other external systems via Neustar’s external systems layer. The services that the SRS interfaces with include:

WHOIS
DNS
Billing
Data Warehouse (Reporting and Data Escrow).

Other external interfaces may be deployed to meet the unique needs of a TLD. At this time there are no additional interfaces planned for .SONG.

The SRS includes an “external notifier” concept in its business policy engine as a message dispatcher. This design allows time-consuming backend processing to be decoupled from critical online registrar transactions. Using an external notifier solution, the registry can utilize “control levers” that allow it to tune or to disable processes to ensure optimal performance at all times. For example, during the early minutes of a TLD launch, when unusually high volumes of transactions are expected, the registry can elect to suspend processing of one or more back end systems in order to ensure that greater processing power is available to handle the increased load requirements. This proven architecture has been used with numerous TLD launches, some of which have involved the processing of over tens of millions of transactions in the opening hours. The following are the standard three external notifiers used the SRS:

WHOIS External Notifier

The WHOIS external notifier dispatches a work item for any EPP transaction that may potentially have an impact on WHOIS. It is important to note that, while the WHOIS external notifier feeds the WHOIS system, it intentionally does not have visibility into the actual contents of the WHOIS system. The WHOIS external notifier serves just as a tool to send a signal to the WHOIS system that a change is ready to occur. The WHOIS system possesses the intelligence and data visibility to know exactly what needs to change in WHOIS. See response to Question 26 for greater detail.

DNS External Notifier

The DNS external notifier dispatches a work item for any EPP transaction that may potentially have an impact on DNS. Like the WHOIS external notifier, the DNS external notifier does not have visibility into the actual contents of the DNS zones. The work items that are generated by the notifier indicate to the dynamic DNS update sub-system that a change occurred that may impact DNS. That DNS system has the ability to decide what actual changes must be propagated out to the DNS constellation. See response to Question 35 for greater detail.

Billing External Notifier

The billing external notifier is responsible for sending all billable transactions to the downstream financial systems for billing and collection. This external notifier contains the necessary logic to determine what types of transactions are billable. The financial systems use this information to apply appropriate debits and credits based on registrar.

Data Warehouse
The data warehouse is responsible for managing reporting services, including registrar reports, business intelligence dashboards, and the processing of data escrow files. The Reporting Database is used to create both internal and external reports, primarily to support registrar billing and contractual reporting requirement. The data warehouse databases are updated on a daily basis with full copies of the production SRS data.
Frequency of Synchronization between Servers
The external notifiers discussed above perform updates in near real-time, well within the prescribed service level requirements. As transactions from registrars update the core SRS, update notifications are pushed to the external systems such as DNS and WHOIS. These updates are typically live in the external system within 2-3 minutes.
Synchronization Scheme (e.g., hot standby, cold standby)
Neustar operates two hot databases within the data center that is operating in primary mode. These two databases are kept in sync via synchronous replication. Additionally, there are two databases in the secondary data center. These databases are updated real time through asynchronous replication. This model allows for high performance while also ensuring protection of data. See response to Question 33 for greater detail.
Compliance with Specification 6 Section 1.2
The SRS implementation for .SONG is fully compliant with Specification 6, including section 1.2. EPP Standards are described and embodied in a number of IETF RFCs, ICANN contracts and practices, and registry-registrar agreements. Extensible Provisioning Protocol or EPP is defined by a core set of RFCs that standardize the interface that make up the registry-registrar model. The SRS interface supports EPP 1.0 as defined in the following RFCs shown in Table 24-1.

Additional information on the EPP implementation and compliance with RFCs can be found in the response to Question 25.
Compliance with Specification 10
Specification 10 of the New TLD Agreement defines the performance specifications of the TLD, including service level requirements related to DNS, RDDS (WHOIS), and EPP. The requirements include both availability and transaction response time measurements. As an experienced registry operator, Neustar has a long and verifiable track record of providing registry services that consistently exceed the performance specifications stipulated in ICANN agreements. This same high level of service will be provided for the .SONG Registry. The following section describes Neustar's experience and its capabilities to meet the requirements in the new agreement.
To properly measure the technical performance and progress of TLDs, Neustar collects data on key essential operating metrics. These measurements are key indicators of the performance and health of the registry. Neustar's current .biz SLA commitments are among the most stringent in the industry today, and exceed the requirements for new TLDs. Table 24-2 compares the current SRS performance levels compared to the requirements for new TLDs, and clearly demonstrates the ability of the SRS to exceed those requirements.

Their ability to commit and meet such high performance standards is a direct result of their philosophy towards operational excellence. See response to Question 31 for a full description of their philosophy for building and managing for performance.
24.3 Resourcing Plans
The development, customization, and on-going support of the SRS are the responsibility of a combination of technical and operational teams, including:

- Development/Engineering
- Database Administration
- Systems Administration
- Network Engineering.

Additionally, if customization or modifications are required, the Product Management and Quality Assurance teams will be involved in the design and testing. Finally, the Network Operations and Information Security play an important role in ensuring the systems involved are operating securely and reliably.
The necessary resources will be pulled from the pool of operational resources described in detail in the response to Question 31. Neustar's SRS implementation is very mature, and has been in production for over 10 years. As such, very little new development related to the SRS will be required for the implementation of the .SONG registry. The following resources are available from those teams:
Development/Engineering – 19 employees
Database Administration- 10 employees
Systems Administration – 24 employees
Network Engineering – 5 employees
The resources are more than adequate to support the SRS needs of all the TLDs operated by Neustar, including the .SONG registry.

---

25. Extensible Provisioning Protocol (EPP): provide a detailed description of the interface with registrars, including how the applicant will comply with EPP in RFCs 3735 (if applicable), and 5730-5734.
If intending to provide proprietary EPP extensions, provide documentation consistent with RFC 3735, including the EPP templates and schemas that will be used.

Describe resourcing plans (number and description of personnel roles allocated to this area).
A complete answer is expected to be no more than 5 pages. If there are proprietary EPP extensions, a complete answer is also expected to be no more than 5 pages per EPP extension.

25.1 Introduction
Amazon EU S.à r.l.'s back-end registry operator, Neustar, has over 10 years of experience operating EPP based registries. They deployed one of the first EPP registries in 2001 with the launch of .biz. In 2004, they were the first gTLD to implement EPP 1.0. Over the last ten years Neustar has implemented numerous extensions to meet various unique TLD requirements. Neustar will leverage its extensive experience to ensure Amazon EU S.à r.l. is provided with an unparalleled EPP based registry. The following discussion explains the EPP interface which will be used for the .SONG registry. This interface exists within the protocol farm layer as described in Question 24 and is depicted in Figure 25-1.

25.2 EPP Interface
Registrars are provided with two different interfaces for interacting with the registry. Both are EPP based, and both contain all the functionality necessary to provision and manage domain names. The primary mechanism is an EPP interface to connect directly with the registry. This is the interface registrars will use for most of their interactions with the registry. However, an alternative web GUI (Registry Administration Tool) that can also be used to perform EPP transactions will be provided. The primary use of the Registry Administration Tool is for performing administrative or customer support tasks.
The main features of the EPP implementation are:
Standards Compliance: The EPP XML interface is compliant to the EPP RFCs. As future EPP RFCs are published or existing RFCs are updated, Neustar makes changes to the implementation keeping in mind of any backward compatibility issues.
Scalability: The system is deployed keeping in mind that it may be required to grow and shrink the footprint of the Registry system for a particular TLD.
Fault-tolerance: The EPP servers are deployed in two geographically separate data centers to provide for quick failover capability in case of a major outage in a particular data center. The EPP servers adhere to strict availability requirements defined in the SLAs.
Configurability: The EPP extensions are built in a way that they can be easily configured to turn on or off for a particular TLD.
Extensibility: The software is built ground up using object oriented design. This allows for easy extensibility of the software without risking the possibility of the change rippling through the whole application.
Auditable: The system stores detailed information about EPP transactions from provisioning to DNS and WHOIS publishing. In case of a dispute regarding a name registration, the Registry can provide comprehensive audit information on EPP transactions.
Security: The system provides IP address based access control, client credential-based authorization test, digital certificate exchange, and connection limiting to the protocol layer.
25.3 Compliance with RFCs and Specifications
The registry-registrar model is described and embodied in a number of IETF RFCs, ICANN contracts and practices, and registry-registrar agreements. As shown in Table 25-1, EPP is defined by the core set of RFCs that standardize the interface that registrars use to provision domains with the SRS. As a core component of the SRS architecture, the implementation is fully compliant with all EPP RFCs.

Neustar ensures compliance with all RFCs through a variety of processes and procedures. Members from the engineering and standards teams actively monitor and participate in the development of RFCs that impact the registry services, including those related to EPP. When new RFCs are introduced or existing ones are updated, the team performs a full compliance review of each system impacted by the change. Furthermore, all code releases include a full regression test that includes specific test cases to verify RFC compliance.

Neustar has a long history of providing exceptional service that exceeds all performance specifications. The SRS and EPP interface have been designed to exceed the EPP specifications defined in Specification 10 of the Registry Agreement and profiled in Table 25-2. Evidence of Neustar's ability to perform at these levels can be found in the .biz monthly progress reports found on the ICANN website.

EPP Toolkits
Toolkits, under open source licensing, are freely provided to registrars for interfacing with the SRS. Both Java and C++ toolkits will be provided, along with the accompanying documentation. The Registrar Tool Kit (RTK) is a software development kit (SDK) that supports the development of a registrar software system for registering domain names in the registry using EPP. The SDK consists of software and documentation as described below.
The software consists of working Java and C++ EPP common APIs and samples that implement the EPP core functions and EPP extensions used to communicate between the registry and registrar. The RTK illustrates how XML requests (registration events) can be assembled and forwarded to the registry for processing. The software provides the registrar with the basis for a reference implementation that conforms to the EPP registry-registrar protocol. The software component of the SDK also includes XML schema definition files for all Registry EPP objects and EPP object extensions. The RTK also includes a "dummy" server to aid in the testing of EPP clients.
The accompanying documentation describes the EPP software package hierarchy, the object data

model, and the defined objects and methods (including calling parameter lists and expected response behavior). New versions of the RTK are made available from time to time to provide support for additional features as they become available and support for other platforms and languages.

25.4 Proprietary EPP Extensions

The .SONG registry will not include proprietary EPP extensions. Neustar has implemented various EPP extensions for both internal and external use in other TLD registries. These extensions use the standard EPP extension framework described in RFC 5730. Table 25-3 provides a list of extensions developed for other TLDs. Should the .SONG registry require an EPP extension at some point in the future, the extension will be implemented in compliance with all RFC specifications including RFC 3735.

The full EPP schema to be used in the .SONG registry is attached in the document titled “EPP Schema.”

25.5 Resourcing Plans

The development and support of EPP is largely the responsibility of the Development/Engineering and Quality Assurance teams. As an experience registry operator with a fully developed EPP solution, on-going support is largely limited to periodic updates to the standard and the implementation of TLD specific extensions.

The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:

Development/Engineering – 19 employees

Quality Assurance - 7 employees.

These resources are more than adequate to support any EPP modification needs of the .SONG registry.

---

26. Whois: describe

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

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

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

Frequency of synchronization between servers.

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

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

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

26.1 Introduction

Amazon EU S.à r.l. recognizes the importance of an accurate, reliable, and up-to-date WHOIS database to governments, law enforcement, intellectual property holders and the public as a whole and is firmly committed to complying with all of the applicable WHOIS specifications for data objects, bulk access, and lookups as defined in Specifications 4 and 10 to the Registry Agreement. Amazon EU S.à r.l.’s back-end registry services provider, Neustar, has extensive experience providing ICANN and RFC-compliant WHOIS services for each of the TLDs that it operates both as a Registry Operator for gTLDs, ccTLDs and back-end registry services provider. As one of the first “thick” registry operators in the gTLD space, Neustar’s WHOIS service has been designed from the ground up to display as much information as required by a TLD and

respond to a very stringent availability and performance requirement.
Some of the key features of .SONG's solution include:

- Fully compliant with all relevant RFCs including 3912
- Production proven, highly flexible, and scalable with a track record of 100% availability over the past 10 years
- Exceeds current and proposed performance specifications
- Supports dynamic updates with the capability of doing bulk updates
- Geographically distributed sites to provide greater stability and performance

In addition, .SONG's thick-WHOIS solution also provides for additional search capabilities and mechanisms to mitigate potential forms of abuse as discussed below. (e.g., IDN, registrant data).

26.2 Software Components

The WHOIS architecture comprises the following components:

An in-memory database local to each WHOIS node: To provide for the performance needs, the WHOIS data is served from an in-memory database indexed by searchable keys.

Redundant servers: To provide for redundancy, the WHOIS updates are propagated to a cluster of WHOIS servers that maintain an independent copy of the database.

Attack resistant: To ensure that the WHOIS system cannot be abused using malicious queries or DOS attacks, the WHOIS server is only allowed to query the local database and rate limits on queries based on IPs and IP ranges can be readily applied.

Accuracy auditor: To ensure the accuracy of the information served by the WHOIS servers, a daily audit is done between the SRS information and the WHOIS responses for the domain names which are updated during the last 24-hour period. Any discrepancies are resolved proactively.

Modular design: The WHOIS system allows for filtering and translation of data elements between the SRS and the WHOIS database to allow for customizations.

Scalable architecture: The WHOIS system is scalable and has a very small footprint. Depending on the query volume, the deployment size can grow and shrink quickly.

Flexible: It is flexible enough to accommodate thin, thick, or modified thick models and can accommodate any future ICANN policy, such as different information display levels based on user categorization.

SRS master database: The SRS database is the main persistent store of the Registry information. The Update Agent computes what WHOIS updates need to be pushed out. A publish-subscribe mechanism then takes these incremental updates and pushes to all the WHOIS slaves that answer queries.

26.3 Compliance with RFC and Specifications 4 and 10

Neustar has been running thick-WHOIS Services for over 10+ years in full compliance with RFC 3912 and with Specifications 4 and 10 of the Registry Agreement.RFC 3912 is a simple text based protocol over TCP that describes the interaction between the server and client on port 43. Neustar built a home-grown solution for this service. It processes millions of WHOIS queries per day.

Table 26-1 describes Neustar's compliance with Specifications 4 and 10.

Neustar ensures compliance with all RFCs through a variety of processes and procedures. Members from the engineering and standards teams actively monitor and participate in the development of RFCs that impact the registry services, including those related to WHOIS. When new RFCs are introduced or existing ones are updated, the team performs a full compliance review of each system impacted by the change. Furthermore, all code releases include a full regression test that includes specific test cases to verify RFC compliance.

26.4 High-level WHOIS System Description

26.4.1 WHOIS Service (port 43)

The WHOIS service is responsible for handling port 43 queries. Our WHOIS is optimized for speed using an in-memory database and master-slave architecture between the SRS and WHOIS slaves.

The WHOIS service also has built-in support for IDN. If the domain name being queried is an IDN, the returned results include the language of the domain name, the domain name's UTF-8 encoded representation along with the Unicode code page.

26.4.2 Web Page for WHOIS queries

In addition to the WHOIS Service on port 43, Neustar provides a web based WHOIS application (www.whois.SONG). It is an intuitive and easy to use application for the general public to use. WHOIS web application provides all of the features available in the port 43 WHOIS. This includes full and partial search on:

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

It also provides features not available on the port 43 service. These include:

1. Redemption Grace Period calculation: Based on the registry's policy, domains in pendingDelete can be restorable or scheduled for release depending on the date/time the domain went into pendingDelete. For these domains, the web based WHOIS displays "Restorable" or "Scheduled for Release" to clearly show this additional status to the user.
2. Extensive support for international domain names (IDN)
3. Ability to perform WHOIS lookups on the actual Unicode IDN
4. Display of the actual Unicode IDN in addition to the ACE-encoded name
5. A Unicode to Punycode and Punycode to Unicode translator
6. An extensive FAQ
7. A list of upcoming domain deletions

26.5 IT and Infrastructure Resources

As described above the WHOIS architecture uses a workflow that decouples the update process

from the SRS. This ensures SRS performance is not adversely affected by the load requirements of dynamic updates. It is also decoupled from the WHOIS lookup agent to ensure the WHOIS service is always available and performing well for users. Each of Neustar's geographically diverse WHOIS sites use:

- Firewalls, to protect this sensitive data
- Dedicated servers for MQ Series, to ensure guaranteed delivery of WHOIS updates
- Packetshaper for source IP address-based bandwidth limiting
- Load balancers to distribute query load
- Multiple WHOIS servers for maximizing the performance of WHOIS service.

The WHOIS service uses HP BL 460C servers, each with 2 X Quad Core CPU and a 64GB of RAM. The existing infrastructure has 6 servers, but is designed to be easily scaled with additional servers should it be needed.
Figure 26-1 depicts the different components of the WHOIS architecture.

26.6 Interconnectivity with Other Registry System
As described in Question 24 about the SRS and further in response to Question 31, "Technical Overview", when an update is made by a registrar that impacts WHOIS data, a trigger is sent to the WHOIS system by the external notifier layer. The update agent processes these updates, transforms the data if necessary and then uses messaging oriented middleware to publish all updates to each WHOIS slave. The local update agent accepts the update and applies it to the local in-memory database. A separate auditor compares the data in WHOIS and the SRS daily and monthly to ensure accuracy of the published data.
26.7 Frequency of Synchronization between Servers
Updates from the SRS, through the external notifiers, to the constellation of independent WHOIS slaves happens in real-time via an asynchronous publish/subscribe messaging architecture. The updates are guaranteed to be updated in each slave within the required SLA of 95% ≤ 60 minutes. Please note that Neustar's current architecture is built towards the stricter SLAs (95% ≤ 15 minutes) of .BIZ. The vast majority of updates tend to happen within 2-3 minutes.
26.8 Provision for Searchable WHOIS Capabilities
Neustar will create a new web-based service to address the new search features based on requirements specified in Specification 4 Section 1.8. The application will enable users to search the WHOIS directory using any one or more of the following fields:

- Domain name
- Registrar ID
- Contacts and registrant's name
- Contact and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state or province, etc.)
- Name server name and name server IP address
- The system will also allow search using non-Latin character sets which are compliant with IDNA specification.

The user will choose one or more search criteria, combine them by Boolean operators (AND, OR, NOT) and provide partial or exact match regular expressions for each of the criterion name-value pairs. The domain names matching the search criteria will be returned to the user.
Figure 26-2 shows an architectural depiction of the new service.

Potential Forms of Abuse
As recognized by the Terms of Reference for Whois Misuse Studies, http://gnso.icann.org/issues/whois/tor-whois-misuse-studies-25sep09-en.pdf, a number of reported and recorded harmful acts, such as spam, phishing, identity theft, and stalking which Registrants believe were sent using WHOIS contact information. Although these Whois studies are still underway, there is a general belief that public access to Whois data may lead to a measurable degree of misuse – that is, to actions that cause actual harm, are illegal or illegitimate, or otherwise contrary to the stated legitimate purpose. One of the other key focuses of these studies will be to correlate the reported incidents of harmful acts with anti-harvesting measures that some Registrars and Registries apply to WHOIS queries (e.g., rate limiting, CAPTCHA, etc.).

Neustar firmly believes that adding the increased search capabilities, without appropriate controls could exacerbate the potential abuses associated with the Whois service. To mitigate the risk of this powerful search service being abused by unscrupulous data miners, a layer of security will be built around the query engine which will allow the registry to identify rogue activities and then take appropriate measures. Potential abuses include, but are not limited to:

- Data Mining
- Unauthorized Access
- Excessive Querying
- Denial of Service Attacks

To mitigate the abuses noted above, Neustar will implement any or all of these mechanisms as appropriate:

- Username-password based authentication
- Certificate based authentication
- Data encryption
- CAPTCHA mechanism to prevent robo invocation of Web query
- Fee-based advanced query capabilities for premium customers.

The searchable WHOIS application will adhere to all privacy laws and policies of the .SONG registry.
26.9 Resourcing Plans
As with the SRS, the development, customization, and on-going support of the WHOIS service is the responsibility of a combination of technical and operational teams. The primary groups responsible for managing the service include:

Development/Engineering – 19 employees
Database Administration – 10 employees
Systems Administration – 24 employees
Network Engineering – 5 employees

Additionally, if customization or modifications are required, the Product Management and Quality Assurance teams will also be involved. Finally, the Network Operations and Information Security play an important role in ensuring the systems involved are operating securely and reliably. The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. Neustar's WHOIS implementation is very mature, and has been in production for over 10 years. As such, very little new development will be required to support the implementation of the .SONG registry. The resources are more than adequate to support the WHOIS needs of all the TLDs operated by Neustar, including the .SONG registry.

---

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

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

The description of the registration lifecycle should be supplemented by the inclusion of a state diagram, which captures definitions, explanations of trigger points, and transitions from state to state.
If applicable, provide definitions for aspects of the registration lifecycle that are not covered by standard EPP RFCs.
A complete answer is expected to be no more than 5 pages.

27.1 Registration Life Cycle

Introduction

.SONG will follow the lifecycle and business rules found in the majority of gTLDs today. Our back-end operator, Neustar, has over ten years of experience managing numerous TLDs that utilize standard and unique business rules and lifecycles. This section describes the business rules, registration states, and the overall domain lifecycle that will be used for .SONG.

Domain Lifecycle - Description

The registry will use the EPP 1.0 standard for provisioning domain names, contacts and hosts. Each domain record is comprised of three registry object types: domain, contacts, and hosts Domains, contacts and hosts may be assigned various EPP defined statuses indicating either a particular state or restriction placed on the object. Some statuses may be applied by the Registrar; other statuses may only be applied by the Registry. Statuses are an integral part of the domain lifecycle and serve the dual purpose of indicating the particular state of the domain and indicating any restrictions placed on the domain. The EPP standard defines 17 statuses, however only 14 of these statuses will be used in the .SONG registry per the defined .SONG business rules.

The following is a brief description of each of the statuses. Server statuses may only be applied by the Registry, and client statuses may be applied by the Registrar.

OK – Default status applied by the Registry.

Inactive – Default status applied by the Registry if the domain has less than 2 nameservers.

PendingCreate – Status applied by the Registry upon processing a successful Create command, and indicates further action is pending. This status will not be used in the .SONG registry.

PendingTransfer – Status applied by the Registry upon processing a successful Transfer request command, and indicates further action is pending.

PendingDelete – Status applied by the Registry upon processing a successful Delete command that does not result in the immediate deletion of the domain, and indicates further action is pending.

PendingRenew – Status applied by the Registry upon processing a successful Renew command that does not result in the immediate renewal of the domain, and indicates further action is pending. This status will not be used in the .SONG registry.

PendingUpdate – Status applied by the Registry if an additional action is expected to complete the update, and indicates further action is pending. This status will not be used in

the .SONG registry.

Hold – Removes the domain from the DNS zone.

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

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

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

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

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

Domain may be updated

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

Domain may be renewed at anytime during the term

Domain may be auto-renewed by the Registry

Domain may be transferred to another registrar.

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

27.1.1 Registration States

Domain Lifecycle – Registration States

As described above the .SONG registry will implement a standard domain lifecycle found in most gTLD registries today. There are five possible domain states:

Active

Inactive

Locked

Pending Transfer

Pending Delete.

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

Active State

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

Inactive State

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

Locked State

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

Pending Transfer State

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

Pending Delete State

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

27.1.2 Typical Registration Lifecycle Activities

Domain Creation Process

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

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

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

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

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

Update Process

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

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

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

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

Renew Process

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

Transfer Process

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

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

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

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

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

Deletion Process

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

27.1.3 Applicable Time Elements

The following section explains the time elements that are involved.

Grace Periods

There are six grace periods:

- Add-Delete Grace Period (AGP)
- Renew-Delete Grace Period
- Transfer-Delete Grace Period
- Auto-Renew-Delete Grace Period
- Auto-Renew Grace Period
- Redemption Grace Period (RGP).

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

The following describes each of these grace periods in detail.

Add-Delete Grace Period

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

Renew-Delete Grace Period

The Renew-Delete Grace Period is associated with the date the Domain was renewed. Domains may

be deleted for credit during the 120 hours after a renewal. The grace period is intended to allow Registrars to correct domains that were mistakenly renewed. It should be noted that domains that are deleted during the renew grace period will be placed into pendingDelete and will enter the RGP (see below).

Transfer-Delete Grace Period

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

Auto-Renew-Delete Grace Period

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

Auto-Renew Grace Period

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

Redemption Grace Period

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

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

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

27.2 State Diagram

Figure 27-1 provides a description of the registration lifecycle.

The different states of the lifecycle are active, inactive, locked, pending transfer, and pending delete. Please refer to section 27.1.1 for detail description of each of these states. The lines between the states represent triggers that transition a domain from one state to another.

The details of each trigger are described below:

Create: Registry receives a create domain EPP command.

WithNS: The domain has met the minimum number of nameservers required by registry policy in order to be published in the DNS zone.

WithOutNS: The domain has not met the minimum number of nameservers required by registry policy. The domain will not be in the DNS zone.

Remove Nameservers: Domain's nameserver(s) is removed as part of an update domain EPP command. The total nameserver is below the minimum number of nameservers required by registry policy in order to be published in the DNS zone.

Add Nameservers: Nameserver(s) has been added to domain as part of an update domain EPP command. The total number of nameservers has met the minimum number of nameservers required by registry policy in order to be published in the DNS zone.

Delete: Registry receives a delete domain EPP command.

DeleteAfterGrace: Domain deletion does not fall within the add grace period.

DeleteWithinAddGrace: Domain deletion falls within add grace period.

Restore: Domain is restored. Domain goes back to its original state prior to the delete command.

Transfer: Transfer request EPP command is received.

Transfer Approve/Cancel/Reject: Transfer requested is approved or cancel or rejected.

TransferProhibited: The domain is in clientTransferProhibited and/or serverTranferProhibited status. This will cause the transfer request to fail. The domain goes back to its original state.

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

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

27.2.1 EPP RFC Consistency

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

27.3 Resources

The registration lifecycle and associated business rules are largely determined by policy and business requirements; as such the Product Management and Policy teams will play a critical

role in working with Amazon EU S.à r.l. to determine the precise rules that meet the requirements of the TLD. Implementation of the lifecycle rules will be the responsibility of Development/Engineering team, with testing performed by the Quality Assurance team.
Neustar's SRS implementation is very flexible and configurable, and in many case development is not required to support business rule changes.
The .SONG registry will be using standard lifecycle rules, and as such no customization is anticipated. However should modifications be required in the future, the necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:
Development/Engineering – 19 employees
Registry Product Management – 4 employees
These resources are more than adequate to support the development needs of all the TLDs operated by Neustar, including the .SONG registry.

---

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

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

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

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

deletion requests; and
- Requiring the notification of multiple, unique points of contact when a domain has been updated, transferred, or deleted.

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

28.1 Abuse Prevention and Mitigation

Amazon EU S.à r.l. and its registry service provider, Neustar, recognize that preventing and mitigating abuse and malicious conduct in the <.TLD> registry is an important and significant responsibility. Amazon EU S.à r.l. will leverage Neustar's extensive experience in establishing and implementing registration policies to prevent and mitigate abusive and malicious domain activity within the proposed <.TLD> space.

Amazon will provision <.TLD> domains to third parties in accordance with the TLD registration policy. Opportunities for abusive and malicious domain activity in <.TLD> are therefore very restricted but we will nonetheless abide by our obligations to ICANN. A responsible domain name registry works towards the eradication of abusive domain name registrations and malicious activity, which may include conduct such as:

• Illegal or fraudulent actions
•Spam
• Phishing
• Pharming
• Distribution of malware
• Fast flux hosting
• Botnets
• Malicious hacking
• Distribution of child pornography
• Online sale or distribution of illegal pharmaceuticals.

By taking an active role in researching and monitoring abusive domain name registration and malicious conduct, Neustar has developed the ability to efficiently work with various law enforcement and security communities to mitigate fast flux DNS-using botnets.

Policies and Procedures to Minimize Abusive Registrations

A registry must have the policies, resources, personnel, and expertise in place to combat such abusive registration and malicious conduct. Neustar, Amazon EU S.à r.l.'s registry services provider, has played a leading role in preventing of such abusive practices, and has developed and implemented a "domain takedown" policy. Amazon EU S.à r.l. also believes that combating abusive use of the DNS is important in protecting registrants.

Removing a domain name from the DNS before it can cause harm is often the best preventative measure for thwarting certain malicious conduct such as botnets and malware distribution. Because removing a domain name from the zone will stop all activity associated with the domain name, including websites and e-mail, the decision to remove a domain name from the DNS must follow a documented process, culminating in a determination that the domain name to be removed poses a threat to the security and stability of the Internet or the registry. Amazon EU S.à r.l., via Neustar, has an extensive, defined, and documented process for taking the necessary action of removing a domain from the zone when its presence in the zone poses a threat to the security and stability of the infrastructure of the Internet or the registry.

Abuse Point of Contact

As required by the Registry Agreement, Amazon EU S.à r.l. will establish and publish on its website a single abuse point of contact responsible for addressing inquiries from law enforcement and the public related to malicious and abusive conduct. Amazon EU S.à r.l. will also provide such information to ICANN before delegating any domain names in <.TLD>. This information shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of malicious conduct complaints, and a telephone number and mailing address for the primary contact. Amazon EU S.à r.l. will ensure that this information is accurate and current, and that updates are provided to ICANN if and when changes are made. In addition, the registry services provider for <.TLD>, Neustar, shall continue to have an additional point of contact for requests from registrars related to abusive domain name practices.

28.2 Policies Regarding Abuse Complaints

Amazon EU S.à r.l. will adopt an Acceptable Use Policy that (i) clearly defines the types of activities that will not be permitted in <.TLD>; (ii) reserves Amazon EU S.à r.l.'s right to lock, cancel, transfer or otherwise suspend or take down domain names violating the Acceptable Use Policy; and (iii) identify the circumstances under which Amazon EU S.à r.l. may share information with law enforcement. Amazon EU S.à r.l. will incorporate its <.TLD> Acceptable User Policy into its Registry-Registrar Agreement.
Under the <.TLD> Acceptable Use Policy, which is set forth below, Amazon EU S.à r.l. may lock down the domain name to prevent any changes to the domain name contact and nameserver information, place the domain name "on hold" rendering the domain name non-resolvable, transfer

the domain name to another registrar and/or in cases in which the domain name is associated with an ongoing law enforcement investigation, Amazon EU S.à r.l. will coordinate with law enforcement to assist in the investigation as described in more detail below.

It is Amazon EU S.à r.l.'s intention that all <.TLD> domain names will be registered and used by eligible users and that only ICANN-accredited registrars that have signed a Registry-Registrar Agreement will be permitted to register <.TLD> domain names. Accordingly, the potential for abusive registrations and malicious conduct in the <.TLD> registry is expected to be limited. In the unlikely event that such abuse should occur, Amazon EU S.à r.l. will work with its registry services provider, Neustar, to implement the following policies and processes to prevent and mitigate such activities. Below is initial Acceptable Use Policy for the <.TLD> registry.

<.TLD> Acceptable Use Policy

This Acceptable Use Policy gives the <.TLD> registry the ability to quickly lock, cancel, transfer or take ownership of any <.TLD> domain name, either temporarily or permanently, if the domain name is being used in a manner that appears to threaten the stability, integrity or security of the <.TLD> registry, or any of its registrar partners – and/or that may put the safety and security of any registrant or user at risk. The process also allows the <.TLD> registry to take preventive measures to avoid any such criminal or security threats.

The Acceptable Use Policy may be triggered through a variety of channels, including, among other things, private complaint, public alert, government or enforcement agency outreach, and the on-going monitoring by the <.TLD> registry or its partners. In all cases, the <.TLD> registry or its designees will alert <.TLD> registry's registrar partners about any identified threats and will work closely with them to bring offending sites into compliance.

The following are some (but not all) activities that may be subject to rapid domain compliance:

- Phishing: the attempt to acquire personally identifiable information by masquerading as a website other than <.TLD>'s own.
- Pharming: the redirection of Internet users to websites other than those the user intends to visit, usually through unauthorized changes to the Hosts file on a victim's computer or DNS records in DNS servers.
- Dissemination of Malware: the intentional creation and distribution of "malicious" software designed to infiltrate a computer system without the owner's consent, including, without limitation, computer viruses, worms, key loggers, and Trojans.
- Malicious Fast Flux Hosting: a technique used to shelter Phishing, Pharming and Malware sites and networks from detection and to frustrate methods employed to defend against such practices, whereby the IP address associated with fraudulent websites are changed rapidly so as to make the true location of the sites difficult to find.
- Botnetting: the development and use of a command, agent, motor, service, or software which is implemented: (1) to remotely control the computer or computer system of an Internet user without their knowledge or consent, (2) to generate direct denial of service (DDOS) attacks.
- Malicious Hacking: the attempt to gain unauthorized access (or exceed the level of authorized access) to a computer, information system, user account or profile, database, or security system.
- Child Pornography: the storage, publication, display and/or dissemination of pornographic materials depicting individuals under the age of majority in the relevant jurisdiction.

The <.TLD> registry reserves the right, in its sole discretion, to take any administrative and operational actions necessary, including the use of computer forensics and information security technological services, among other things, in order to implement the Acceptable Use Policy. In addition, the <.TLD> registry reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of the <.TLD> registry as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement, or (5) to correct mistakes made by the <.TLD> registry or any Registrar in connection with a domain name registration. The <.TLD> registry also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

Taking Action Against Abusive and/or Malicious Activity

The <.TLD> registry is committed to acting in a timely manner against those domain names associated with abuse or malicious conduct in violation of the Acceptable Use Policy. After a complaint is received from a trusted source or third-party, or detected by the <.TLD> registry, the registry will use commercially reasonable efforts to verify the information in the complaint. If that information can be verified to the best of the registry's ability, the sponsoring registrar will be notified and have 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. If the registrar has not acted when the 12-hour period ends (i.e., is unresponsive to the request or refuses to take action), the <.TLD> registry will place the domain on "ServerHold". (It is unlikely a registrar will not timely act because Amazon EU S.à r.l. intends to use a registrar contract reflecting these

policies). ServerHold removes the domain name from the <.TLD> zone, but the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

Coordination with Law Enforcement

Amazon EU S.à r.l. will obtain assistance from Neustar to meet its obligations under Section 2.8 of the Registry Agreement to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the <.TLD> registry. The <.TLD> registry will respond to legitimate law enforcement inquiries promptly upon receiving the request.

The response shall include, at a minimum, an acknowledgement of receipt of the request, questions or comments concerning the request, and an outline of the next steps to be taken by Amazon EU S.à r.l. for rapid resolution of the request. If the request involves any of the activities that can be validated by the registry and implicates activity covered by the <.TLD> Acceptable Use Policy, the sponsoring registrar will have 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. The <.TLD> Registry will place the domain on “ServerHold” if the registrar has not acted within the 12-hour period.

Monitoring for Malicious Activity

Neustar, <.TLD>’s registry services provider, has developed and implemented an active “domain takedown” policy in which the registry itself takes down abusive domain names.

Neustar targets domain names verified to be abusive and removes them within 12 hours regardless of whether the domain name registrar cooperated. Neustar has determined that the benefit in removing such threats outweighs any potential damage to the registrar/registrant relationship. Amazon EU S.à r.l.’s registration policies make it unlikely that any <.TLD> domains will be taken down. Moreover, only registrars that contractually agree to cooperate in stemming abusive behaviors will be permitted to register <.TLD> domain names.

Neustar’s active prevention policies stem from the notion that registrants in <.TLD> have a reasonable expectation that they control the data associated with their domains, especially its presence in the DNS zone. Removing a domain name from the DNS before it can cause harm is often the best preventative measure for thwarting certain malicious conduct such as botnets and malware distribution that harms not only the domain name registrant, but also potentially millions of unsuspecting Internet users.

Rapid Takedown Process

Since implementing the program, Neustar has developed two basic variations of the process. The more common process variation is a lightweight process that is triggered by “typical” notices. The less common variation is the full process that is triggered by unusual notices, which generally allege that a domain name is being used to threaten the stability and security of the TLD, or is part of a real-time investigation by law enforcement or security researchers. In these cases, accelerated action by the registry is necessary. These processes are described below.

Lightweight Process

In addition to having an active Information Security group that, on its own initiatives, seeks out abusive practices in the <.TLD> registry, Neustar is an active member in a number of security organizations that have the expertise and experience in receiving and investigating reports of abusive DNS practices, including but not limited to, the Anti-Phishing Working Group, Castle Cops, NSP-SEC, the Registration Infrastructure Safety Group and others. Each of these sources is a well-known security organization that has a reputation for preventing abuse and malicious conduct on the Internet. Aside from these organizations, Neustar also actively participates in privately run security associations that operate based on trust and anonymity, making it much easier to obtain information regarding abusive DNS activity.

Once a complaint is received from a trusted source or third-party, or detected by Neustar’s internal security group, information about the abusive practice is forwarded to an internal mail distribution list that includes members of Neustar’s operations, legal, support, engineering, and security teams for immediate response (“CERT Team”). Although the impacted URL is included in the notification e-mail, the CERT Team is trained not to investigate the URLs themselves because the URLs in question often have scripts, bugs, etc. that can compromise the individual’s own computer and the network safety. Rather, the investigation is conducted by CERT team members who can access the URLs in a laboratory environment to avoid compromising the Neustar network. The lab environment is designed specifically for these types of tests and is scrubbed on a regular basis to ensure that none of Neustar’s internal or external network elements are harmed in any fashion.
Once the complaint has been reviewed and the alleged abusive domain name activity is verified to the best of the ability of the CERT Team, the sponsoring registrar has 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone.
The <.TLD> Registry will place the domain on “ServerHold” if the registrar has not acted within

the 12-hour period.
ServerHold removes the domain name from the <.TLD> zone, but the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement.

Full Process

In the unlikely event that Neustar receives a complaint that claims that a domain name is being used to threaten the stability and security of the <.TLD> registry, or is a part of a real-time investigation by law enforcement or security, Neustar follows a slightly different course of action.
Upon initiation of this process, members of the CERT Team are paged and a teleconference bridge is immediately opened up for the CERT Team to assess whether the activity warrants immediate action. If the CERT Team determines the incident is not an immediate threat to the security and the stability of critical Internet infrastructure, the CERT Team provides documentation to the Neustar Network Operations Center to clearly capture the rationale for the decision and either refers the incident to the Lightweight process set forth above or closes the incident.

However, if the CERT TEAM determines that there is a reasonable likelihood that the incident warrants immediate action, a determination is made to immediately remove the domain from the zone. As such, Customer Support will contact the registrar immediately to communicate that there is a domain involved in a security and stability issue. The registrar is provided only the domain name in question and the broadly stated type of incident.

Coordination with Law Enforcement & Industry Groups

Neustar has a close working relationship with a number of law enforcement agencies, both in the United States and Internationally. For example, in the United States, Neustar is in constant communication with the Federal Bureau of Investigation, US CERT, Homeland Security, the Food and Drug Administration, and the National Center for Missing and Exploited Children.
Neustar also participates in a number of industry groups aimed at sharing information among key industry players about the abusive registration and use of domain names. These groups include the Anti-Phishing Working Group and the Registration Infrastructure Safety Group (where Neustar served for several years on the Board of Directors). Through these organizations and others, Neustar proactively shares information with other registries, registrars, ccTLDs, law enforcement, security professionals, etc. not only on abusive domain name registrations within its own TLDs, but also with respect to information uncovered with respect to domain names in other registries' TLDs. Neustar has often found that rarely are abuses found only in the TLDs for which it manages, but also within other TLDs, such as .com and .info. Neustar routinely provides this information to the other registries so that the relevant registry can take the appropriate action.

With the assistance of Neustar as its registry services provider, Amazon EU S.à r.l. can meet its obligations under Section 2.8 of the Registry Agreement to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its <.TLD> registry. Amazon EU S.à r.l. and/or Neustar will respond to legitimate law enforcement inquiries promptly upon receiving the request. Such response shall include, at a minimum, an acknowledgement of receipt of the request, questions or comments concerning the request, and an outline of the next steps to be taken by Amazon EU S.à r.l. and/or Neustar for rapid resolution of the request.
If the request involves any of the activities that can be validated by the registry and/or Neustar and implicates the type of activity set forth in the Acceptable Use Policy, the sponsoring registrar will have 12 hours to investigate the activity further and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. The <.TLD> registry will place the domain on "ServerHold" if the registrar has not acted within the 12-hour period.

28.3 Measures for Removal of Orphan Glue Records

As the Security and Stability Advisory Committee of ICANN (SSAC) rightly acknowledges, although orphaned glue records may be used for abusive or malicious purposes, the "dominant use of orphaned glue supports the correct and ordinary operation of the DNS." See http://www.icann.org/en/committees/security/sac048.pdf.

While orphan glue often support correct and ordinary operation of the DNS, such glue records can be used maliciously to point to name servers that host domains used in illegal phishing, bot-nets, malware, and other abusive behaviors. Problems occur when the parent domain of the glue record is deleted but its children glue records still remain in DNS. Therefore, when the <.TLD> registry has written evidence of actual abuse of orphaned glue, the <.TLD> registry will act to remove those records from the zone to mitigate such malicious conduct.

Neustar runs a daily audit of entries in its DNS systems and compares those with its provisioning system, which serves as an umbrella protection that items in the DNS zone are valid. Any DNS record that shows up in the DNS zone but not in the provisioning system is flagged for investigation and removed if necessary. This daily DNS audit prevents not only orphaned hosts but also other records that should not be in the zone.
In addition, if either Amazon EU S.à r.l. or Neustar becomes aware of actual abuse on orphaned glue after receiving written notification from a third party through its Abuse Contact or through its customer support, such glue records will be removed from the zone.

28.4 Measures to Promote WHOIS Accuracy

The <.TLD> registry will implement several measures to promote Whois accuracy. Whois service for Amazon EU S.à r.l. will operate as follows. The registry will keep all basic contact details for each domain name in a unique internal system, which facilitates access to the domain information. In addition, Amazon EU S.à r.l. will perform internal monitoring checks and procedures that will only allow accurate Whois information and remove outdated data.

28.4.1. Authentication of Registrant Information

Amazon EU S.à r.l. will guarantee the adequate authentication of registrant data, ensuring the highest levels of accuracy and diligence when dealing with Whois data. In doing so, Amazon EU S.à r.l.'s solid internal system will undertake, but not be limited to the following measures: running checks against Whois internal records and regular verification of all contact details and other relevant registrant information. The registrar will also be charged with regularly checking Whois accuracy.

Amazon EU S.à r.l. will have a well-defined registration policy that will include a requirement that complete and accurate registrant details are provided by the requestor for a domain. These details will be validated by the registrar who will have a contractual duty to comply with Amazon EU S.à r.l.'s registration policy. The full details of every domain requestor will be kept in Amazon EU S.à r.l.'s on-line registry management dashboard which can be accessed by Amazon EU S.à r.l.'s Domain Management Team at any time.

28.4.2. Regular Monitoring of Registration Data

Amazon EU S.à r.l. will comply with ICANN's Whois requirements. Among other measures, Amazon EU S.à r.l. will regularly remind its internal personnel to comply with ICANN's Whois information Policy through regularly checking Whois data against internal records, offering Whois accuracy services, evaluating claims of fraudulent Whois data, and cancelling domain name registrations with outdated Whois details.

28.4.3. Policies and Procedures ensuring compliance

Amazon EU S.à r.l.'s Registry-Registrar Agreement will require a registrar to take steps necessary to ensure Whois data is complete and accurate and to implement the <.TLD> registration policies.

28.5 Resourcing Plans

Responsibility for abuse mitigation rests with a variety of functional groups at Neustar. The Neustar Abuse Monitoring team is primarily responsible for providing analysis and conducting investigations of reports of abuse. The Neustar Customer Service team also plays an important role in assisting with investigations, responding to customers, and notifying registrars of abusive domains. Finally, the Neustar Policy/Legal team is responsible for developing the relevant policies and procedures.

The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:

Customer Support – 12 employees

Policy/Legal – Two employees

The resources are more than adequate to support the abuse mitigation procedures of the <.TLD> registry.

Furthermore, Amazon EU S.à r.l. dedicates significant financial and personnel resources to combating malicious and abusive behavior in the DNS and across the internet. Amazon EU S.à r.l. will extend these resources to designating the unique abuse point of contact, regularly monitoring potential abusive and malicious activities with support from dedicated technical staff, analyzing reported abuse and malicious activity, and acting to address such reported activity.

The designated abuse prevention staff within Neustar and Amazon EU S.à r.l. will be subject to regular evaluations, receive adequate training and work under expert supervision. The abuse prevention resources will comprise both internal staff and external abuse prevention experts who would give extra advice and support when necessary. This external staff includes one legal expert and four operational experts.

Please note that in the above answer the terms "We", "Our" and "Amazon" may refer to either the applicant Amazon EU S.à r.l. or Amazon.com Inc., the ultimate parent, or sometimes NeuStar, the registry services provider.

---

29. Rights Protection Mechanisms: Applicants must describe how their registry will comply with policies

and practices that minimize abusive registrations and other activities that affect the legal rights of others, such as the Uniform Domain Name Dispute Resolution Policy (UDRP), Uniform Rapid Suspension (URS) system, and Trademark Claims and Sunrise services at startup.
A complete answer should include:

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

>To be eligible for a score of 2, answers must also include additional measures specific to rights protection, such as abusive use policies, takedown procedures, registrant pre-verification, or authentication procedures, or other covenants.
A complete answer is expected to be no more than 10 pages.

29.1 Introduction

Amazon is applying for <.TLD> to provide a dedicated platform for stable and secure online communication and interaction. Amazon has several thousand registered intellectual property assets of all types including trademarks, designs, and domain names – we place the protection of our intellectual property as a high priority and we respect the intellectual property of others.

29.1.1 Rights protection in gTLD registry operation is a core objective of Amazon

We will require registrars to work with us on a four-step registration process featuring: (i) Eligibility Confirmation; (ii) Naming Convention Check; (iii) Acceptable Use Review; and (iv) Registration. As stated in our answer to Question 18, all domains in our registry will be subject to eligibility requirements.

We believe that the above registration process will ensure that abusive registrations are prevented, but we will continue to monitor ICANN policy developments, and update our procedures as required.

29.2 Core measures to prevent abusive registrations

To further prevent abusive registration or cybersquatting, we will adopt the following Rights Protection Mechanisms (RPMs) which have been mandated for new gTLD operators by ICANN:

- A 30 day Sunrise process
- A 60 day Trademark Claims process

Generally, these RPMs are targeted at abusive registrations undertaken by third parties. However, domains in our registry will be registered by Amazon and eligible trusted third parties through registrars who will be contractually required to ensure that stated rules covering eligibility and use of a domain are adhered to through a validation process. As a result, abusive registrations should be prevented.

29.2.1 Sunrise Eligibility

Our Sunrise Eligibility Requirements will clearly set out criteria for registration in this TLD. Notice of our Sunrise will be provided to third party holders of validated trademarks in the Trademark Clearinghouse as required by ICANN. Our Sunrise Eligibility Requirements will be published on the website of our registry.

29.2.2 Sunrise Window

As required in the Applicant Guidebook in section 7.1, our Sunrise window will recognize "all word marks: (i) nationally or regionally registered and for which proof of use – which can be a declaration and a single specimen of current use – was submitted to, and validated by, the Trademark
Clearinghouse; or (ii) that have been court-validated; or (iii) that are specifically protected by a statute or treaty currently in effect and that was in effect on or before 26 June 2008".

Our Sunrise window will last for 30 days. Applications received from an ICANN-accredited registrar will be accepted for registration if they are (i) supported by an entry in the Trademark Clearinghouse (TMCH) during our Sunrise window and (ii) satisfy our Sunrise Eligibility Requirements. Once registered, those domain names will normally have a one year term of registration. Any domain names registered will be managed by a registrar.

29.2.3 Sunrise Dispute Resolution Policy

We will devise and publish the rules for our Sunrise Dispute Resolution Policy (SDRP) on our registry website. Our SDRP will allow any party to raise a challenge on the following four grounds as required in the Applicant Guidebook (6.2.4):

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

Complaints can be submitted through our registry website within 30 days following the closure of the Sunrise, and will be initially processed by a registrar which will promptly report to us: (i) the challenger; (ii) the challenged domain name; (iii) the grounds upon which the complaint is based; and (iv) why the challenger believes the grounds are satisfied.

29.2.4 Trademark Claims Service

Our Trademark Claims Service (TMCS) will run for a 60 day period following the closure of our 30 day Sunrise. Our TMCS will be supported by the Trademark Clearinghouse and will provide a notice to third parties interested in filing a character string in our registry of a registered trademark right that matches the character string in the TMCH.

We will honor and recognize in our TMCS the following types of marks as defined in the Applicant Guidebook section 7.1: (i) nationally or regionally registered; (ii) court-validated; or (iii) specifically protected by a statute or treaty in effect at the time the mark is submitted to the Clearinghouse for inclusion.

Once received from the TMCH, with which our registry provider will interface, a claim will be initially processed by a registrar who will provide a report to us on the eligibility of the applicant.

29.2.5 Implementation and Resourcing Plans of core services to prevent abusive registration

Our Sunrise and IP Claims service will be introduced with the following timetable:

Day One: Announcement of Registry Launch and publication of registry website with details of the Sunrise and Trademark Claim Service (“TMCS”)
Day 30: Sunrise opens for 30 days on a first-come, first served basis. Once registrations are approved, they will be entered into the Shared Registry System (SRS) and published in our Thick-Whois database.
Day 60-75: Registry Open, domains applied for in the Sunrise registered and TMCS begins for a minimum of 60 days

Day 120-135: TMCS ends; normal operations continue.

Our Implementation Team will comprise the following:

From Amazon: the Director of IP will lead a team of up to seven experts with experience of domain name management and on-line legal dispute resolution, with access to other teams in Amazon Legal if required.

From NeuStar, registry service provider to Amazon: A Customer Support team of 12, a Product Management Team of four and a Development ⁄ Engineering Team of 19 will be available as required to support the legal team, led by Jeff Neuman. This team has over 10 years’ experience with implementing registry launches including rights protection schemes such as the .biz Sunrise and IP Claims.

In addition, Amazon will be supported externally by two legal specialists, four client managers and six operational staff. The operational staff will undertake the validation checks on registration requests.
The Implementation Team will create a formal Registry Launch plan. This plan will set out the exact process for the launch of each Amazon registry and will define responsibilities and budgets. The Registry website, which is budgeted for in the three year plans provided in our answers to Question 46, will feature Rules of Registration, Rules of Eligibility, Terms & Conditions of Registration, Acceptable Use Policies as well as the Rules of the Sunrise, the Rules of the Sunrise Dispute Resolution Policy and the Rules of the Trademark Claims Service.

Technical implementation between the registry and the Trademark Clearinghouse will be undertaken by the registry service provider as soon as practical after the Trademark Clearinghouse is operational and announces its integration process.

As demonstrated in our answer to question 46, a budget has been set aside to pay fees charged by the Trademark Clearinghouse Operator for this integration.

The contract we have with our registrars (the RRA) will require that registrars use the TMCH, adhere to the Terms & Conditions of the TMCH and will prohibit registrars from filing domains in our registries on their own behalf or utilizing any data from the TMCH except in the provision of their duties as a registrar.

When processing TMCS claims, our registrars will be required to use the specific form of notice provided by ICANN in the Applicant Guidebook.
We will also require our registrars to implement appropriate privacy policies reflecting local requirements. For example, Amazon is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union.

29.3 Mechanisms to identify and address the abusive use of registered domain names on an ongoing basis

To prevent the abusive use of registered domain names on an ongoing basis we will adopt the following Rights Protection Mechanisms (RPMs) which have been mandated by ICANN:

- The Uniform Domain Name Dispute Resolution Policy (UDRP) to address domain names that have been registered and used in bad faith in the TLD.

- The Uniform Rapid Suspension (URS) scheme which is a faster, more efficient alternative to the Uniform Dispute Resolution Policy to deal with clear-cut cases of cybersquatting.

- The Post Delegation Dispute Resolution Procedure (PDDRP).

- Implementation of a Thick WHOIS making it easier for rights holders to identify and locate infringing parties.

The UDRP and the URS are targeted at abusive registrations undertaken by third parties and the PDDRP at so called “Bad Actor” registries.

Abusive behavior by eligible registrants will be prevented by our internal processes, for example the pre-registration validation checks and monitoring of use of our registrars.

We acknowledge that we are subject to the UDRP, the URS and the PDDRP and we will co-operate fully with ICANN and appropriate registries in the unlikely circumstances that complaints are made.

29.3.1 The Uniform Dispute Resolution Policy (UDRP)

The UDRP is an out-of-court dispute resolution mechanism for trademark owners to resolve clear cases of bad faith, abusive registration and use of domain names. The UDRP applies by contract to all domain name registrations in gTLDs. Standing to file a UDRP complaint is limited to trademark owners who must demonstrate their rights. To prevail in a UDRP complaint, the complainant must further demonstrate that the domain name registrant has no rights or legitimate interests in the disputed domain name, and that the disputed domain name has been registered and is being used in bad faith. In the event of a successful claim, the infringing domain name registration is transferred to the complainant’s control.

In the event of a UDRP case ordering transfer of a domain name to a UDRP complainant, any transfer would be subject to the prevailing party meeting the registration eligibility requirements; if such requirements were not met, we may place the domain name that is the subject of the successful complaint on a list that prevents it from being registered again.

29.3.2 The URS

The URS is intended to be a lighter, quicker complement to the UDRP. Like the UDRP, it is intended for clear-cut cases of trademark abuse. Under the URS, the only remedy which a panel may grant is the temporary suspension of a domain name for the duration of the registration period (which may be extended by the prevailing complainant for one year, at commercial rates). URS substantive criteria mirror those of the UDRP but with a higher burden of proof for complainants, and additional registrant defences. Once a determination is rendered, a losing registrant has several appeal possibilities from 30 days up to one year. Either party may file a de novo appeal within 14 days of a decision. There are penalties for filing “abusive complaints” which may result in a ban on future URS filings.

Should a complaint be made, we will respond in a timely fashion, reflecting our contractual responsibility to ICANN as a registry operator.
Should a successful complaint be made, we will suspend the domain name for the duration of the registration period.
We will co-operate with the URS panel providers and panelists as we will co-operate with UDRP panel providers and panelists.

29.3.3 The Post-Delegation Dispute Resolution Procedure (PDDRP)

The PDDRP is an administrative option for trademark owners to file an objection against a registry whose “affirmative conduct” in its operation or use of its gTLD is alleged to cause or materially contribute to trademark abuse. In this way, the PDDRP is intended to act as a higher-level enforcement tool to assist ICANN compliance activities, where rights holders may not be able to continue to turn solely to lower-level multijurisdictional enforcement options in a vastly expanded DNS.

The PDDRP involves a number of procedural layers, such as an administrative compliance review, appointment of a “threshold review panel”, an expert determination as to liability under the procedure (with implementation of any remedies at ICANN’s discretion), a possible de novo appeal and further appeal to arbitration under ICANN’s registry terms. The PDDRP requires specific bad faith conduct including profit from encouraging infringement in addition to “the typical registration fee.”

As set out in the Applicant Guidebook in the appendix summarizing the PDDRP, the grounds for a complaint on a second level registration are that, “(a) there is a substantial pattern or practice of specific bad faith intent by the registry operator to profit from the sale of trademark infringing domain names; and (b) the registry operator’s bad faith intent to profit from the systematic registration of domain names within the gTLD that are identical or confusingly similar to the complainant’s mark, which (i) takes unfair advantage of the distinctive character or the reputation of the complainant’s mark or (ii) impairs the distinctive character or the reputation of the complainant’s mark, or(iii) creates a likelihood of confusion with the complainant’s mark.”

29.3.4 Thick Whois

As required in Specification 4 of the Registry agreement, all Amazon registries will provide Thick Whois. A Thick WHOIS provides a centralized location of registrant information within the control of the registry (as opposed to thin Whois where the data is dispersed across registrars).
Thick Whois will provide rights owners and law enforcement with the ability to review the registration record easily.

We will place a requirement on registrars to ensure that all registrations are filed with accurate Whois details.
Amazon will create and publish a Whois Query email address so that third parties can submit queries about any domains in our registry.

29.3.5 Implementation and Resourcing Plans for mechanisms to identify and address the abusive use of registered domain names on an ongoing basis

Our post-launch rights protection mechanisms will be in place from Day One of the launch of the registry.

To ensure that we are compliant with our obligations as a registry operator, we will develop a section of our registry website to assist third parties involved in UDRP, URS and PDDRP complaints including third parties wishing to make a complaint, ICANN compliance staff and the providers of UDRP and URS panels. This will feature an email address for enquiries relating to disputes or seeking further information on specific domains. We will monitor this address for all of the following: Notice of Complaint, Notice of Default, URS Determination, UDRP Determination, Notice of Appeal and Appeal Panel Findings where appropriate.

As stated in our answer to Question 18, Amazon’s Intellectual Property group will be responsible for the development, maintenance and enforcement of the Domain Management Policy. This will include ensuring that the following implementation targets are met:

- Locking domains that are the subject of URS complaints within 24 hours of receipt of a URS complaint, and ensuring a registrar locks domains that are the subject of UDRP complaints within 24 hours of receipt of a UDRP complaint.

- Confirming the implementation of the lock to the relevant URS provider, and ensure a registrar confirms the implementation of the lock to the relevant UDRP provider.

- Ensuring that a registrar cancels domain names that are the subject of a successful UDRP complaint within 24 hours

- Redirecting servers to a website with the ICANN mandated information following a successful URS within 24 hours

The human resources dedicated to managing post-launch RPM include:

From Amazon: the Director of IP will lead a team of up to seven experts with experience of domain name management and on-line legal dispute resolution, with access to other teams in Amazon Legal if required.

From NeuStar, registry service provider to Amazon: A Customer Support team of 12, a Product

Management Team of four and a Development / Engineering Team of 19 will be available as required to support the legal team, led by Jeff Neuman. This team has over 10 years' experience with implementing registry launches including rights protection schemes including the .biz Sunrise and IP Claims.

In addition, Amazon will be supported externally by two legal specialists, four client managers and six operational staff. The operational staff will undertake the validation checks on registration requests.

We are confident that this staffing is more than adequate for the initial stages of registry operation. Of course, should business goals change requiring more resources, Amazon will closely review any expansion plans, and plan for additional financial, technical, and team-member support to put the Registry in the best position for success.

We will also require registrars to implement appropriate privacy policies reflecting the high standards that we operate. For information on our Privacy Policies, please see: http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496

29.4 Additional Mechanism that exceed requirements

Rights protection is at the core of Amazon's objective in applying for this registry. Therefore we are committed to providing the following additional mechanisms:

29.4.1 Registry Legal Manager

Amazon will appoint a Legal Manager to ensure that we are compliant with ICANN policies. The Legal Manager will also handle all disputes relating to RPMs. This will involve evaluating complaints, working with external legal counsel and law enforcement, and resolving disputes. The Legal Manager will also liaise with external stakeholders including URS and UDRP panel providers, the TMCH operator and trademark holders as needed.

29.4.2 Rights Protection Help Line

Amazon will maintain a Rights Protection Help Line. Calls to this line will be allocated a Case Number and the following details will be recorded: (i) the contact details of the complainant; (ii) the domain name that is the subject of the complaint or query; (iii) the registered right, if any, that is associated with the request; and (iv) an explanation of the concerns.
An initial response to a query or complaint will be made within 24 hours. The Rights Protection Help Line will be in place on Day One of the registry. The cost of the Rights Help Line is reflected in the Projections Templates provided at Question 46 as part of on-going registry maintenance costs.
The aim of the Rights Protection Help Line is to assist third parties in understanding the mission and purpose of our registry and to see if a resolution can be found that is quicker and easier than the filing of a UDRP or URS complaint.

The Legal Manager will oversee the Rights Protection Help Line.

29.4.3 Registrar Accreditation

Amazon may audit the performance of registrars every six months and re-validate our Registry-Registrar Agreements annually. Our audits may include site visits to ensure the security of data etc.

29.4.4 Audits of registration records

Every three months, whichever is the most of 250 or 2% of the total of domain names registered in that period will be reviewed with registrars to ensure accurate registration records and use that is compliant with our Acceptable Use guidelines.

29.4.5 Maintenance of Registry Website

Amazon will create a website for all our registries and we will make it easy for third parties including representatives of law enforcement to contact us by featuring our full contact details (physical, email address and phone number).

29.4.6 Click Wrapping our Terms & Conditions

We may bring to the attention of requestors of domain names the Terms & Conditions of registration and, especially, Acceptable Use terms through Click Wrapping.

29.4.7 Annual Report

Amazon will publish an Annual Report on Rights Protection in our registries on our Registry Website. This will include relevant statistics and it will outline all cases and how they were resolved.

29.4.8 Contacts with WIPO and other DRS providers

Amazon may invite representatives of WIPO and other DRS providers to review our RPMs and to make suggestions on any improvements that we might make after the first full year of

operation.

29.4.9 Registrant Pre-Verification

All requests for registration will be verified by registrars to ensure that they come from eligible applicants. A record of the request will be kept in our on-line domain management console including the requestor's email address and other contact information.

29.4.10 Take down Procedures

Amazon has described Takedown Procedures for domains supporting Abusive Behaviors in Question 28. We will reserve the right to terminate a registration and to take down all associated services after a review by our Legal Manager if a takedown for reasons of rights protection is requested by law enforcement, a representative of a court we recognize etc.

29.4.11 Speed of Response

Wherever possible, as outlined above, Amazon is committed to a response within 24 hours of a complaint being made. This exceeds the guidelines for the UDRP and the URS.

Please note that in the above answer the terms "We", "Our" and "Amazon" may refer to either the applicant Amazon EU S.à r.l. or Amazon.com Inc., the ultimate parent.

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

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

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

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

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

Amazon EU S.à r.l. and our back-end operator, Neustar, recognize the vital need to secure the systems and the integrity of the data in commercial solutions. The .SONG registry solution will leverage industry-best security practices including the consideration of physical, network, server, and application elements.
Neustar's approach to information security starts with comprehensive information security policies. These are based on the industry best practices for security including SANS (SysAdmin, Audit, Network, Security) Institute, NIST (National Institute of Standards and Technology), and Center for Internet Security (CIS). Policies are reviewed annually by Neustar's information security team.
The following is a summary of the security policies that will be used in the .SONG registry, including:
1. Summary of the security policies used in the registry operations
2. Description of independent security assessments
3. Description of security features that are appropriate for .SONG
4. List of commitments made to registrants regarding security levels

All of the security policies and levels described in this section are appropriate for the .SONG registry.
30.(a).1 Summary of Security Policies

Neustar, Inc. has developed a comprehensive Information Security Program in order to create effective administrative, technical, and physical safeguards for the protection of its information assets, and to comply with Neustar's obligations under applicable law, regulations, and contracts. This Program establishes Neustar's policies for accessing, collecting, storing, using, transmitting, and protecting electronic, paper, and other records containing sensitive information.
The Program defines:

The policies for internal users and our clients to ensure the safe, organized and fair use of information resources.
The rights that can be expected with that use.
The standards that must be met to effectively comply with policy.
The responsibilities of the owners, maintainers, and users of Neustar's information resources.
Rules and principles used at Neustar to approach information security issues

The following policies are included in the Program:

1. Acceptable Use Policy

The Acceptable Use Policy provides the "rules of behavior" covering all Neustar Associates for using Neustar resources or accessing sensitive information.

2. Information Risk Management Policy

The Information Risk Management Policy describes the requirements for the on-going information security risk management program, including defining roles and responsibilities for conducting and evaluating risk assessments, assessments of technologies used to provide information security and monitoring procedures used to measure policy compliance.

3. Data Protection Policy

The Data Protection Policy provides the requirements for creating, storing, transmitting, disclosing, and disposing of sensitive information, including data classification and labeling requirements, the requirements for data retention. Encryption and related technologies such as digital certificates are also covered under this policy.

4. Third Party Policy

The Third Party Policy provides the requirements for handling service provider contracts, including specifically the vetting process, required contract reviews, and on-going monitoring of service providers for policy compliance.

5. Security Awareness and Training Policy

The Security Awareness and Training Policy provide the requirements for managing the on-going awareness and training program at Neustar. This includes awareness and training activities provided to all Neustar Associates.

6. Incident Response Policy

The Incident Response Policy provides the requirements for reacting to reports of potential security policy violations. This policy defines the necessary steps for identifying and reporting security incidents, remediation of problems, and conducting "lessons learned" post-mortem reviews in order to provide feedback on the effectiveness of this Program. Additionally, this policy contains the requirement for reporting data security breaches to the appropriate authorities and to the public, as required by law, contractual requirements, or regulatory bodies.

7. Physical and Environmental Controls Policy

The Physical and Environment Controls Policy provides the requirements for securely storing sensitive information and the supporting information technology equipment and infrastructure. This policy includes details on the storage of paper records as well as access to computer systems and equipment locations by authorized personnel and visitors.

8. Privacy Policy

Neustar supports the right to privacy, including the rights of individuals to control the dissemination and use of personal data that describes them, their personal choices, or life experiences. Neustar supports domestic and international laws and regulations that seek to protect the privacy rights of such individuals.

9. Identity and Access Management Policy

The Identity and Access Management Policy covers user accounts (login ID naming convention, assignment, authoritative source) as well as ID lifecycle (request, approval, creation, use, suspension, deletion, review), including provisions for system/application accounts, shared/group accounts, guest/public accounts, temporary/emergency accounts, administrative access, and remote access. This policy also includes the user password policy requirements.

10. Network Security Policy

The Network Security Policy covers aspects of Neustar network infrastructure and the technical controls in place to prevent and detect security policy violations.

11. Platform Security Policy

The Platform Security Policy covers the requirements for configuration management of servers, shared systems, applications, databases, middle-ware, and desktops and laptops owned or operated by Neustar Associates.

12. Mobile Device Security Policy

The Mobile Device Policy covers the requirements specific to mobile devices with information storage or processing capabilities. This policy includes laptop standards, as well as requirements for PDAs, mobile phones, digital cameras and music players, and any other removable device capable of transmitting, processing or storing information.

13. Vulnerability and Threat Management Policy

The Vulnerability and Threat Management Policy provides the requirements for patch management, vulnerability scanning, penetration testing, threat management (modeling and monitoring) and the appropriate ties to the Risk Management Policy.

14. Monitoring and Audit Policy

The Monitoring and Audit Policy covers the details regarding which types of computer events to record, how to maintain the logs, and the roles and responsibilities for how to review, monitor, and respond to log information. This policy also includes the requirements for backup, archival, reporting, forensics use, and retention of audit logs.

15. Project and System Development and Maintenance Policy

The System Development and Maintenance Policy covers the minimum security requirements for all software, application, and system development performed by or on behalf of Neustar and the minimum security requirements for maintaining information systems.

30. (a).2 Independent Assessment Reports

Neustar IT Operations is subject to yearly Sarbanes-Oxley (SOX), Statement on Auditing Standards #70 (SAS70) and ISO audits. Testing of controls implemented by Neustar management in the areas of access to programs and data, change management and IT Operations are subject to testing by both internal and external SOX and SAS70 audit groups. Audit Findings are communicated to process owners, Quality Management Group and Executive Management. Actions are taken to make process adjustments where required and remediation of issues is monitored by internal audit and QM groups.

External Penetration Test is conducted by a third party on a yearly basis. As authorized by Neustar, the third party performs an external Penetration Test to review potential security weaknesses of network devices and hosts and demonstrate the impact to the environment. The assessment is conducted remotely from the Internet with testing divided into four phases:

A network survey is performed in order to gain a better knowledge of the network that was being tested

Vulnerability scanning is initiated with all the hosts that are discovered in the previous phase

Identification of key systems for further exploitation is conducted

Exploitation of the identified systems is attempted.

Each phase of the audit is supported by detailed documentation of audit procedures and results. Identified vulnerabilities are classified as high, medium and low risk to facilitate management's prioritization of remediation efforts. Tactical and strategic recommendations are provided to management supported by reference to industry best practices.

30.(a).3 Augmented Security Levels and Capabilities

There are no increased security levels specific for .SONG. However, Neustar will provide the same high level of security provided across all of the registries it manages.

A key to Neustar's Operational success is Neustar's highly structured operations practices. The standards and governance of these processes:

Include annual independent review of information security practices

Include annual external penetration tests by a third party

Conform to the ISO 9001 standard (Part of Neustar's ISO-based Quality Management System)

Are aligned to Information Technology Infrastructure Library (ITIL) and CoBIT best practices

Are aligned with all aspects of ISO IEC 17799

Are in compliance with Sarbanes-Oxley (SOX) requirements (audited annually)

Are focused on continuous process improvement (metrics driven with product scorecards reviewed monthly).

A summary view to Neustar's security policy in alignment with ISO 17799 can be found in section 30.(a).4 below.

30.(a).4 Commitments and Security Levels

The .SONG registry commits to high security levels that are consistent with the needs of the TLD. These commitments include:

Compliance with High Security Standards

Security procedures and practices that are in alignment with ISO 17799

Annual SOC 2 Audits on all critical registry systems

Annual 3rd Party Penetration Tests

Annual Sarbanes Oxley Audits

Highly Developed and Document Security Policies

Compliance with all provisions described in section 30.(a).4 below and in the attached security policy document.

Resources necessary for providing information security

Fully documented security policies

Annual security training for all operations personnel

High Levels of Registry Security

Multiple redundant data centers

High Availability Design

Architecture that includes multiple layers of security

Diversified firewall and networking hardware vendors

Multi-factor authentication for accessing registry systems

Physical security access controls

A 24x7 manned Network Operations Center that monitors all systems and applications

A 24x7 manned Security Operations Center that monitors and mitigates DDoS attacks

DDoS mitigation using traffic scrubbing technologies

New gTLD Application Submitted to ICANN by: Amazon EU S.à r.l.

Application Downloaded On: 01 May 2014

String: TUNES

Application ID: 1-1317-30761

Applicant Information

1. Full legal name

Amazon EU S.à r.l.

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact Informat on Redacted

4. Fax number

Contact nformation Redacted

5. If applicable, website or URL

http://www.amazon.com/

Primary Contact

6(a). Name

Lorna Gradden

6(b). Title

Operations Director

6(c). Address

6(d). Phone Number

Contact nformation Redacted

6(e). Fax Number

Contact nformation Redacted

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Dana Northcott

7(b). Title

Associate General Counsel, IP

7(c). Address

7(d). Phone Number

Contact nformation Redacted

7(e). Fax Number

Contact nformation Redacted

7(f). Email Address

Contact Informat on Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Corporation (Société à responsabilité limitée)

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

Luxembourg

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

Attachments are not displayed on this form.

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

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

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

Amazon EU S.à r.l. is not a joint venture.

Applicant Background

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

Name	Position

Allan Lyall	Manager
Eric Laurent Broussard	Manager
Eva Charlotte Gehlin	Manager
Gregory William Greeley	Manager
John Timothy Leslie	Manager

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

Name	Position
Allan Lyall	Manager
Eric Laurent Broussard	Manager
Eva Charlotte Gehlin	Manager
Gregory William Greeley	Manager
John Timothy Leslie	Manager

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

Name	Position
Amazon Europe Holding Technologies S.C.S.	Not Applicable

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

Applied-for gTLD string

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

TUNES

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

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

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

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

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

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

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

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

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

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

15C. List any variants to the applied-for gTLD string according to the relevant IDN tables.

---

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

Neustar, Amazon EU S.à r.l.'s provider of back end registry services, confirms that it does not anticipate any problems in the operation or rendering of this ASCII string. The string conforms to accepted standards and poses no threat to the operational security and stability of the Internet.

---

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

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

Founded in 1994, Amazon opened on the World Wide Web in July 1995 and today offers Earth's Biggest Selection. Amazon seeks to be Earth's most customer-centric company, where customers can find and discover anything they might want to buy online, and endeavors to offer its customers the lowest possible prices. Amazon and other sellers offer millions of unique new, refurbished and used items in categories such as Books; Movies, Music & Games; Digital Downloads; Electronics & Computers; Home & Garden; Toys, Kids & Baby; Grocery; Apparel, Shoes & Jewelry; Health & Beauty; Sports & Outdoors; and Tools, Auto & Industrial. Amazon Web Services provides Amazon's developer customers with access to in-the-cloud infrastructure services based on Amazon's own back-end technology platform, which developers can use to enable virtually any type of business. The new latest generation Kindle is the lightest, most compact Kindle ever and features the same 6-inch, most advanced electronic ink display that reads like real paper even in bright sunlight. Kindle Touch is a new addition to the Kindle family with an easy-to-use touch screen that makes it easier than ever to turn pages, search, shop, and take notes – still with all the benefits of the most advanced electronic ink display. Kindle Touch 3G is the top of the line e-reader and offers the same new design and features of Kindle Touch, with the unparalleled added convenience of free 3G. Kindle Fire is the Kindle for movies, TV shows, music, books, magazines, apps, games and web browsing with all the content, free storage in the Amazon Cloud, Whispersync, Amazon Silk (Amazon's new revolutionary cloud-accelerated web browser), vibrant color touch screen, and powerful dual-core processor.

The mission of the <.TLD> registry is:

To provide a unique and dedicated platform while simultaneously protecting the integrity of Amazon's brand and reputation.

A <.TLD> registry will:

- Offer a stable and secure foundation for online communication and interaction.
- Provide a platform for innovation.

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

The <.TLD> registry will benefit registrants and internet users by offering a stable and secure foundation for online communication and interaction.

What is the goal of your proposed gTLD in terms of areas of specialty, service levels or reputation?

Amazon intends for its new <.TLD> gTLD to provide a unique and dedicated platform for stable and secure online communication and interaction. The <.TLD> registry will be run in line with current industry standards of good registry practice.

What do you anticipate your proposed gTLD will add to the current space in terms of competition, differentiation or innovation?

Amazon values the opportunity to be one of the first companies to own a gTLD.

A <.TLD> registry will:

- Offer a stable and secure foundation for online communication and interaction.
- Provide a platform for innovation.

What goals does your proposed gTLD have in terms of user experience?

Amazon intends for its new <.TLD> gTLD to provide a unique and dedicated platform for stable and secure online communication and interaction.

Provide a complete description of the applicant's intended registration policies in support of the goals above Amazon's Intellectual Property group will be responsible for the development, maintenance and enforcement of a Domain Management Policy. The Domain Management Policy will define (i) the rules associated with eligibility and domain name allocation, (ii) the license terms governing the use of a <.TLD> domain name, and (iii) the dispute resolution policies for the <.TLD> gTLD. Amazon will update the Domain Management Policy as needed to reflect the registry's business goals and, where appropriate, ICANN consensus policies.
Registration of a domain name in the <.TLD> registry will be undertaken in four steps: (i)

Eligibility Confirmation, (ii) Naming Convention Check, (iii) Acceptable Use Review, and (iv) Registration.

For example, on the rules of eligibility, each applied for character string must conform to the <.TLD> rules of eligibility. Each <.TLD> name must:

• be at least 1 character and no more than 63 characters long
• not contain a hyphen on the 3rd and 4th position (tagged domains)
• contain only letters (a-z), numbers (0-9) and hyphens or a combination of these
• start and end with an alphanumeric character, not a hyphen
• not match any character strings reserved by ICANN
• not match any protected country names or geographical terms

Additionally:

• Internationalized domain names (IDN) may be supported in the <.TLD> registry at the second level.
• The <.TLD> registry will respect third party intellectual property rights.

• All <.TLD> domains will carry accurate and up-to-date registration records.

Amazon's Intellectual Property group reserves the right to revoke a license to use a <.TLD> domain name, at any time, if any use of a <.TLD> domain name violates the Domain Management Policy.

Will your proposed gTLD impose any measures for protecting the privacy of confidential information of registrants or users?

Yes. Amazon will implement appropriate privacy policies respecting requirements of local jurisdictions. For example, Amazon is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union.

Describe whether and in what ways outreach and communications will help to achieve your projected benefits?

Amazon will assess the need to undertake public outreach or mass communication about its new gTLD registry in line with the goals for the TLD.

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

Amazon intends to initially provision a relatively small number of domains in the <.TLD> registry to support the goals of the TLD. These initiatives should not impose social costs of any type on consumers.

How will multiple applications for a particular domain be resolved, for example, by auction or on a first come first served basis?

Applications from eligible requestors for domains in the <.TLD> registry will be considered by Amazon's Intellectual Property group on a first come first served basis and allocated in line with the goals of the TLD.

Explain any cost benefits for registrants you intend to implement (e.g. advantageous pricing, introductory discounts, bulk registration discounts).
Domains in the <.TLD> registry will be provisioned to support the goals of the TLD. Accordingly, "cost benefits" may be explored depending on the goals of the TLD. Amazon shares the goals of enhancing customer trust and choice.

The Registry Agreement requires that registrars be offered the option to obtain initial domain name registrations for periods of one to ten years at the discretion of the registrar, but no greater than 10 years. Additionally the Registry Agreement requires advance written notice of price increases. Do you intend to make contractual commitments to registrants regarding the magnitude of price escalation?

The Domain Management Policy will include the costs and benefits of a unique and dedicated platform for stable and secure online communication and interaction.

---

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

No

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

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

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

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

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

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

21A. Is the application for a geographic name?

No

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

Amazon EU S.à r.l., with support of its ultimate parent company, Amazon.com, Inc. (collectively referred to in this response throughout as "Amazon"), is committed to managing the <.TLD> registry in full compliance with all applicable laws, consensus policies, ICANN guidelines, RFCs and the Specifications of the Registry Agreement. In the management of domain names in the <.TLD> registry, based on GAC advice and Specification 5, Amazon intends to block from initial registration all required domain names.

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

security or stability concerns.
The following registry services are customary services offered by a registry operator:

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

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

23.1 Introduction

Amazon EU S.à r.l. has elected to partner with Neustar, Inc. to provide back-end services for the .TUNES registry. In making this decision, Amazon EU S.à r.l. recognized that Neustar already possesses a production-proven registry system that can be quickly deployed and smoothly operated over its robust, flexible, and scalable world-class infrastructure. The existing registry services will be leveraged for the .TUNES registry. The following section describes the registry services to be provided.
23.2 Standard Technical and Business Components
Neustar will provide the highest level of service while delivering a secure, stable and comprehensive registry platform. Amazon EU S.à r.l. will use Neustar's Registry Services platform to deploy the .TUNES registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to .TUNES.

- Registry-Registrar Shared Registration Service (SRS)
- Extensible Provisioning Protocol (EPP)
- Domain Name System (DNS)
- WHOIS
- DNSSEC
- Data Escrow
- Dissemination of Zone Files using Dynamic Updates
- Access to Bulk Zone Files
- Dynamic WHOIS Updates
- IPv6 Support
- Rights Protection Mechanisms
- Internationalized Domain Names (IDN).

The following is a description of each of the services.
SRS
Neustar's secure and stable SRS is a production-proven, standards-based, highly reliable, and high-performance domain name registration and management system. The SRS includes an EPP interface for receiving data from registrars for the purpose of provisioning and managing domain names and name servers. The response to Question 24 provides specific SRS information.
EPP
The .TUNES registry will use the Extensible Provisioning Protocol (EPP) for the provisioning of domain names. The EPP implementation will be fully compliant with all RFCs. Registrars are provided with access via an EPP API and an EPP based Web GUI. With more than 10 gTLD, ccTLD, and private TLDs implementations, Neustar has extensive experience building EPP-based registries. Additional discussion on the EPP approach is presented in the response to Question 25.
DNS
Amazon EU S.à r.l. will leverage Neustar's world-class DNS network of geographically distributed nameserver sites to provide the highest level of DNS service. The service utilizes "Anycast" routing technology, and supports both IPv4 and IPv6. The DNS network is highly proven, and currently provides service to over 20 TLDs and thousands of enterprise companies. Additional information on the DNS solution is presented in the response to Questions 35.
WHOIS
Neustar's existing standard WHOIS solution will be used for .TUNES. The service provides supports for near real-time dynamic updates. The design and construction is agnostic with regard to data display policy is flexible enough to accommodate any data model. In addition, a searchable WHOIS service that complies with all ICANN requirements will be provided. The following WHOIS options will be provided:
Standard WHOIS (Port 43)
Standard WHOIS (Web)
Searchable WHOIS (Web)
DNSSEC
An RFC compliant DNSSEC implementation will be provided using existing DNSSEC capabilities. Neustar is an experienced provider of DNSSEC services, and currently manages signed zones for three large top level domains: .biz, .us, and .co. Registrars are provided with the ability to submit and manage DS records using EPP, or through a web GUI. Additional information on DNSSEC, including the management of security extensions is found in the response to Question

43.
Data Escrow
Data escrow will be performed in compliance with all ICANN requirements in conjunction with an approved data escrow provider. The data escrow service will:

- Protect against data loss
- Follow industry best practices
- Ensure easy, accurate, and timely retrieval and restore capability in the event of a hardware failure
- Minimizes the impact of software or business failure.

Additional information on the Data Escrow service is provided in the response to Question 38.
Dissemination of Zone Files using Dynamic Updates
Dissemination of zone files will be provided through a dynamic, near real-time process. Updates will be performed within the specified performance levels. The proven technology ensures that updates pushed to all nodes within a few minutes of the changes being received by the SRS. Additional information on the DNS updates may be found in the response to Question 35.
Access to Bulk Zone Files
Amazon EU S.à r.l. will provide third party access to the bulk zone file in accordance with specification 4, Section 2 of the Registry Agreement. Credentialing and dissemination of the zone files will be facilitated through the Central Zone Data Access Provider.
Dynamic WHOIS Updates
Updates to records in the WHOIS database will be provided via dynamic, near real-time updates. Guaranteed delivery message oriented middleware is used to ensure each individual WHOIS server is refreshed with dynamic updates. This component ensures that all WHOIS servers are kept current as changes occur in the SRS, while also decoupling WHOIS from the SRS. Additional information on WHOIS updates is presented in response to Question 26.
IPv6 Support
The .TUNES registry will provide IPv6 support in the following registry services: SRS, WHOIS, and DNS/DNSSEC. In addition, the registry supports the provisioning of IPv6 AAAA records. A detailed description on IPv6 is presented in the response to Question 36.
Required Rights Protection Mechanisms
Amazon EU S.à r.l. will provide all ICANN required Rights Mechanisms, including:

- Trademark Claims Service
- Trademark Post-Delegation Dispute Resolution Procedure (PDDRP)
- Registration Restriction Dispute Resolution Procedure (RRDRP)
- UDRP
- URS
- Sunrise service.

More information is presented in the response to Question 29.
Internationalized Domain Names (IDN)

IDN registrations are provided in full compliance with the IDNA protocol. Neustar possesses extensive experience offering IDN registrations in numerous TLDs, and its IDN implementation uses advanced technology to accommodate the unique bundling needs of certain languages. Character mappings are easily constructed to block out characters that may be deemed as confusing to users. A detailed description of the IDN implementation is presented in response to Question 44.
23.3 Unique Services
Amazon EU S.à r.l. will not be offering services that are unique to .TUNES.
23.4 Security or Stability Concerns
All services offered are standard registry services that have no known security or stability concerns. Neustar has demonstrated a strong track record of security and stability within the industry.

---

24. Shared Registration System (SRS) Performance:
describe

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

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

24.1 Introduction

Amazon EU S.à r.l. has partnered with Neustar, Inc., an experienced TLD registry operator, for the operation of the .TUNES Registry. Amazon EU S.à r.l. is confident that the plan in place for the operation of a robust and reliable Shared Registration System (SRS) as currently provided by Neustar will satisfy the criterion established by ICANN.

Neustar built its SRS from the ground up as an EPP based platform and has been operating it reliably and at scale since 2001. The software currently provides registry services to five TLDs (.BIZ, .US, TEL, .CO and .TRAVEL) and is used to provide gateway services to the .CN and .TW registries. Neustar's state of the art registry has a proven track record of being secure, stable, and robust. It manages more than 6 million domains, and has over 300 registrars connected today.

The following describes a detailed plan for a robust and reliable SRS that meets all ICANN requirements including compliance with Specifications 6 and 10.

24.2 The Plan for Operation of a Robust and Reliable SRS

High-level SRS System Description

The SRS to be used for .TUNES will leverage a production-proven, standards-based, highly reliable and high-performance domain name registration and management system that fully meets or exceeds the requirements as identified in the new gTLD Application Guidebook.

The SRS is the central component of any registry implementation and its quality, reliability and capabilities are essential to the overall stability of the TLD. Neustar has a documented history of deploying SRS implementations with proven and verifiable performance, reliability and availability. The SRS adheres to all industry standards and protocols. By leveraging an existing SRS platform, Amazon EU S.à r.l. is mitigating the significant risks and costs associated with the development of a new system. Highlights of the SRS include:

State-of-the-art, production proven multi-layer design
Ability to rapidly and easily scale from low to high volume as a TLD grows
Fully redundant architecture at two sites
Support for IDN registrations in compliance with all standards
Use by over 300 Registrars
EPP connectivity over IPv6
Performance being measured using 100% of all production transactions (not sampling).

SRS Systems, Software, Hardware, and Interoperability

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

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

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

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

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

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

SRS Design

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

Protocol Layer
Business Policy Layer
Database.

Each of the layers is described below.

Protocol Layer

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

horizontally scalable as dictated by volume.
The EPP servers authenticate against a series of security controls before granting service, as follows:

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

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

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

Business Policy Layer

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

Similar to the EPP protocol farm, the SRS consists of a farm of application servers within this layer. This design ensures that there is sufficient capacity to process every transaction in a manner that meets or exceeds all service level requirements. Some registries couple the business logic layer directly in the protocol layer or within the database. This architecture limits the ability to scale the registry. Using a decoupled architecture enables the load to be distributed among farms of inexpensive servers that can be scaled up or down as demand changes. The SRS today processes over 30 million EPP transactions daily.

Database

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

Figure 24-1 depicts the overall SRS architecture including network components.

Number of Servers

As depicted in the SRS architecture diagram above Neustar operates a high availability architecture where at each level of the stack there are no single points of failures. Each of the network level devices run with dual pairs as do the databases. For the .TUNES registry, the SRS will operate with 8 protocol servers and 6 policy engine servers. These expand horizontally as volume increases due to additional TLDs, increased load, and through organic growth. In addition to the SRS servers described above, there are multiple backend servers for services such as DNS and WHOIS. These are discussed in detail within those respective response sections.

Description of Interconnectivity with Other Registry Systems

The core SRS service interfaces with other external systems via Neustar's external systems layer. The services that the SRS interfaces with include:

WHOIS

DNS

Billing

Data Warehouse (Reporting and Data Escrow).

Other external interfaces may be deployed to meet the unique needs of a TLD. At this time there are no additional interfaces planned for .TUNES.

The SRS includes an "external notifier" concept in its business policy engine as a message dispatcher. This design allows time-consuming backend processing to be decoupled from critical online registrar transactions. Using an external notifier solution, the registry can utilize "control levers" that allow it to tune or to disable processes to ensure optimal performance at all times. For example, during the early minutes of a TLD launch, when unusually high volumes of transactions are expected, the registry can elect to suspend processing of one or more back end systems in order to ensure that greater processing power is available to handle the increased load requirements. This proven architecture has been used with numerous TLD launches, some of which have involved the processing of over tens of millions of transactions in the opening hours. The following are the standard three external notifiers used the SRS:

WHOIS External Notifier

The WHOIS external notifier dispatches a work item for any EPP transaction that may potentially have an impact on WHOIS. It is important to note that, while the WHOIS external notifier feeds the WHOIS system, it intentionally does not have visibility into the actual contents of the WHOIS system. The WHOIS external notifier serves just as a tool to send a signal to the WHOIS system that a change is ready to occur. The WHOIS system possesses the intelligence and data visibility to know exactly what needs to change in WHOIS. See response to Question 26 for greater detail.

DNS External Notifier

The DNS external notifier dispatches a work item for any EPP transaction that may potentially have an impact on DNS. Like the WHOIS external notifier, the DNS external notifier does not have visibility into the actual contents of the DNS zones. The work items that are generated by the notifier indicate to the dynamic DNS update sub-system that a change occurred that may impact DNS. That DNS system has the ability to decide what actual changes must be propagated out to the DNS constellation. See response to Question 35 for greater detail.

Billing External Notifier

The billing external notifier is responsible for sending all billable transactions to the downstream financial systems for billing and collection. This external notifier contains the necessary logic to determine what types of transactions are billable. The financial systems use this information to apply appropriate debits and credits based on registrar.

Data Warehouse
The data warehouse is responsible for managing reporting services, including registrar reports, business intelligence dashboards, and the processing of data escrow files. The Reporting Database is used to create both internal and external reports, primarily to support registrar billing and contractual reporting requirement. The data warehouse databases are updated on a daily basis with full copies of the production SRS data.
Frequency of Synchronization between Servers
The external notifiers discussed above perform updates in near real-time, well within the prescribed service level requirements. As transactions from registrars update the core SRS, update notifications are pushed to the external systems such as DNS and WHOIS. These updates are typically live in the external system within 2-3 minutes.
Synchronization Scheme (e.g., hot standby, cold standby)
Neustar operates two hot databases within the data center that is operating in primary mode. These two databases are kept in sync via synchronous replication. Additionally, there are two databases in the secondary data center. These databases are updated real time through asynchronous replication. This model allows for high performance while also ensuring protection of data. See response to Question 33 for greater detail.
Compliance with Specification 6 Section 1.2
The SRS implementation for .TUNES is fully compliant with Specification 6, including section 1.2. EPP Standards are described and embodied in a number of IETF RFCs, ICANN contracts and practices, and registry-registrar agreements. Extensible Provisioning Protocol or EPP is defined by a core set of RFCs that standardize the interface that make up the registry-registrar model. The SRS interface supports EPP 1.0 as defined in the following RFCs shown in Table 24-1.

Additional information on the EPP implementation and compliance with RFCs can be found in the response to Question 25.
Compliance with Specification 10
Specification 10 of the New TLD Agreement defines the performance specifications of the TLD, including service level requirements related to DNS, RDDS (WHOIS), and EPP. The requirements include both availability and transaction response time measurements. As an experienced registry operator, Neustar has a long and verifiable track record of providing registry services that consistently exceed the performance specifications stipulated in ICANN agreements. This same high level of service will be provided for the .TUNES Registry. The following section describes Neustar's experience and its capabilities to meet the requirements in the new agreement.
To properly measure the technical performance and progress of TLDs, Neustar collects data on key essential operating metrics. These measurements are key indicators of the performance and health of the registry. Neustar's current .biz SLA commitments are among the most stringent in the industry today, and exceed the requirements for new TLDs. Table 24-2 compares the current SRS performance levels compared to the requirements for new TLDs, and clearly demonstrates the ability of the SRS to exceed those requirements.

Their ability to commit and meet such high performance standards is a direct result of their philosophy towards operational excellence. See response to Question 31 for a full description of their philosophy for building and managing for performance.
24.3 Resourcing Plans
The development, customization, and on-going support of the SRS are the responsibility of a combination of technical and operational teams, including:

- Development/Engineering
- Database Administration
- Systems Administration
- Network Engineering.

Additionally, if customization or modifications are required, the Product Management and Quality Assurance teams will be involved in the design and testing. Finally, the Network Operations and Information Security play an important role in ensuring the systems involved are operating securely and reliably.
The necessary resources will be pulled from the pool of operational resources described in detail in the response to Question 31. Neustar's SRS implementation is very mature, and has been in production for over 10 years. As such, very little new development related to the SRS will be required for the implementation of the .TUNES registry. The following resources are available from those teams:
Development/Engineering – 19 employees
Database Administration- 10 employees
Systems Administration – 24 employees
Network Engineering – 5 employees
The resources are more than adequate to support the SRS needs of all the TLDs operated by Neustar, including the .TUNES registry.

---

25. Extensible Provisioning Protocol (EPP): provide a detailed description of the interface with registrars, including how the applicant will comply with EPP in RFCs 3735 (if applicable), and 5730-5734.
If intending to provide proprietary EPP extensions, provide documentation consistent with RFC 3735, including the EPP templates and schemas that will be used.

Describe resourcing plans (number and description of personnel roles allocated to this area).
A complete answer is expected to be no more than 5 pages. If there are proprietary EPP extensions, a complete answer is also expected to be no more than 5 pages per EPP extension.

25.1 Introduction
Amazon EU S.à r.l.'s back-end registry operator, Neustar, has over 10 years of experience operating EPP based registries. They deployed one of the first EPP registries in 2001 with the launch of .biz. In 2004, they were the first gTLD to implement EPP 1.0. Over the last ten years Neustar has implemented numerous extensions to meet various unique TLD requirements. Neustar will leverage its extensive experience to ensure Amazon EU S.à r.l. is provided with an unparalleled EPP based registry. The following discussion explains the EPP interface which will be used for the .TUNES registry. This interface exists within the protocol farm layer as described in Question 24 and is depicted in Figure 25-1.

25.2 EPP Interface
Registrars are provided with two different interfaces for interacting with the registry. Both are EPP based, and both contain all the functionality necessary to provision and manage domain names. The primary mechanism is an EPP interface to connect directly with the registry. This is the interface registrars will use for most of their interactions with the registry. However, an alternative web GUI (Registry Administration Tool) that can also be used to perform EPP transactions will be provided. The primary use of the Registry Administration Tool is for performing administrative or customer support tasks.
The main features of the EPP implementation are:
Standards Compliance: The EPP XML interface is compliant to the EPP RFCs. As future EPP RFCs are published or existing RFCs are updated, Neustar makes changes to the implementation keeping in mind of any backward compatibility issues.
Scalability: The system is deployed keeping in mind that it may be required to grow and shrink the footprint of the Registry system for a particular TLD.
Fault-tolerance: The EPP servers are deployed in two geographically separate data centers to provide for quick failover capability in case of a major outage in a particular data center. The EPP servers adhere to strict availability requirements defined in the SLAs.
Configurability: The EPP extensions are built in a way that they can be easily configured to turn on or off for a particular TLD.
Extensibility: The software is built ground up using object oriented design. This allows for easy extensibility of the software without risking the possibility of the change rippling through the whole application.
Auditable: The system stores detailed information about EPP transactions from provisioning to DNS and WHOIS publishing. In case of a dispute regarding a name registration, the Registry can provide comprehensive audit information on EPP transactions.
Security: The system provides IP address based access control, client credential-based authorization test, digital certificate exchange, and connection limiting to the protocol layer.
25.3 Compliance with RFCs and Specifications
The registry-registrar model is described and embodied in a number of IETF RFCs, ICANN contracts and practices, and registry-registrar agreements. As shown in Table 25-1, EPP is defined by the core set of RFCs that standardize the interface that registrars use to provision domains with the SRS. As a core component of the SRS architecture, the implementation is fully compliant with all EPP RFCs.

Neustar ensures compliance with all RFCs through a variety of processes and procedures. Members from the engineering and standards teams actively monitor and participate in the development of RFCs that impact the registry services, including those related to EPP. When new RFCs are introduced or existing ones are updated, the team performs a full compliance review of each system impacted by the change. Furthermore, all code releases include a full regression test that includes specific test cases to verify RFC compliance.

Neustar has a long history of providing exceptional service that exceeds all performance specifications. The SRS and EPP interface have been designed to exceed the EPP specifications defined in Specification 10 of the Registry Agreement and profiled in Table 25-2. Evidence of Neustar's ability to perform at these levels can be found in the .biz monthly progress reports found on the ICANN website.

EPP Toolkits
Toolkits, under open source licensing, are freely provided to registrars for interfacing with the SRS. Both Java and C++ toolkits will be provided, along with the accompanying documentation. The Registrar Tool Kit (RTK) is a software development kit (SDK) that supports the development of a registrar software system for registering domain names in the registry using EPP. The SDK consists of software and documentation as described below.
The software consists of working Java and C++ EPP common APIs and samples that implement the EPP core functions and EPP extensions used to communicate between the registry and registrar. The RTK illustrates how XML requests (registration events) can be assembled and forwarded to the registry for processing. The software provides the registrar with the basis for a reference implementation that conforms to the EPP registry-registrar protocol. The software component of the SDK also includes XML schema definition files for all Registry EPP objects and EPP object extensions. The RTK also includes a "dummy" server to aid in the testing of EPP clients.
The accompanying documentation describes the EPP software package hierarchy, the object data

model, and the defined objects and methods (including calling parameter lists and expected response behavior). New versions of the RTK are made available from time to time to provide support for additional features as they become available and support for other platforms and languages.

25.4 Proprietary EPP Extensions

The .TUNES registry will not include proprietary EPP extensions. Neustar has implemented various EPP extensions for both internal and external use in other TLD registries. These extensions use the standard EPP extension framework described in RFC 5730. Table 25-3 provides a list of extensions developed for other TLDs. Should the .TUNES registry require an EPP extension at some point in the future, the extension will be implemented in compliance with all RFC specifications including RFC 3735.

The full EPP schema to be used in the .TUNES registry is attached in the document titled “EPP Schema.”

25.5 Resourcing Plans

The development and support of EPP is largely the responsibility of the Development/Engineering and Quality Assurance teams. As an experience registry operator with a fully developed EPP solution, on-going support is largely limited to periodic updates to the standard and the implementation of TLD specific extensions.

The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:

Development/Engineering – 19 employees

Quality Assurance - 7 employees.

These resources are more than adequate to support any EPP modification needs of the .TUNES registry.

---

26. Whois: describe

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

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

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

Frequency of synchronization between servers.

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

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

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

26.1 Introduction

Amazon EU S.à r.l. recognizes the importance of an accurate, reliable, and up-to-date WHOIS database to governments, law enforcement, intellectual property holders and the public as a whole and is firmly committed to complying with all of the applicable WHOIS specifications for data objects, bulk access, and lookups as defined in Specifications 4 and 10 to the Registry Agreement. Amazon EU S.à r.l.’s back-end registry services provider, Neustar, has extensive experience providing ICANN and RFC-compliant WHOIS services for each of the TLDs that it operates both as a Registry Operator for gTLDs, ccTLDs and back-end registry services provider. As one of the first “thick” registry operators in the gTLD space, Neustar’s WHOIS service has been designed from the ground up to display as much information as required by a TLD and

respond to a very stringent availability and performance requirement.
Some of the key features of .TUNES's solution include:

- Fully compliant with all relevant RFCs including 3912
- Production proven, highly flexible, and scalable with a track record of 100% availability over the past 10 years
- Exceeds current and proposed performance specifications
- Supports dynamic updates with the capability of doing bulk updates
- Geographically distributed sites to provide greater stability and performance

In addition, .TUNES's thick-WHOIS solution also provides for additional search capabilities and mechanisms to mitigate potential forms of abuse as discussed below. (e.g., IDN, registrant data).

26.2 Software Components

The WHOIS architecture comprises the following components:

An in-memory database local to each WHOIS node: To provide for the performance needs, the WHOIS data is served from an in-memory database indexed by searchable keys.

Redundant servers: To provide for redundancy, the WHOIS updates are propagated to a cluster of WHOIS servers that maintain an independent copy of the database.

Attack resistant: To ensure that the WHOIS system cannot be abused using malicious queries or DOS attacks, the WHOIS server is only allowed to query the local database and rate limits on queries based on IPs and IP ranges can be readily applied.

Accuracy auditor: To ensure the accuracy of the information served by the WHOIS servers, a daily audit is done between the SRS information and the WHOIS responses for the domain names which are updated during the last 24-hour period. Any discrepancies are resolved proactively.

Modular design: The WHOIS system allows for filtering and translation of data elements between the SRS and the WHOIS database to allow for customizations.

Scalable architecture: The WHOIS system is scalable and has a very small footprint. Depending on the query volume, the deployment size can grow and shrink quickly.

Flexible: It is flexible enough to accommodate thin, thick, or modified thick models and can accommodate any future ICANN policy, such as different information display levels based on user categorization.

SRS master database: The SRS database is the main persistent store of the Registry information. The Update Agent computes what WHOIS updates need to be pushed out. A publish-subscribe mechanism then takes these incremental updates and pushes to all the WHOIS slaves that answer queries.

26.3 Compliance with RFC and Specifications 4 and 10

Neustar has been running thick-WHOIS Services for over 10+ years in full compliance with RFC 3912 and with Specifications 4 and 10 of the Registry Agreement.RFC 3912 is a simple text based protocol over TCP that describes the interaction between the server and client on port 43. Neustar built a home-grown solution for this service. It processes millions of WHOIS queries per day.

Table 26-1 describes Neustar's compliance with Specifications 4 and 10.

Neustar ensures compliance with all RFCs through a variety of processes and procedures. Members from the engineering and standards teams actively monitor and participate in the development of RFCs that impact the registry services, including those related to WHOIS. When new RFCs are introduced or existing ones are updated, the team performs a full compliance review of each system impacted by the change. Furthermore, all code releases include a full regression test that includes specific test cases to verify RFC compliance.

26.4 High-level WHOIS System Description

26.4.1 WHOIS Service (port 43)

The WHOIS service is responsible for handling port 43 queries. Our WHOIS is optimized for speed using an in-memory database and master-slave architecture between the SRS and WHOIS slaves.

The WHOIS service also has built-in support for IDN. If the domain name being queried is an IDN, the returned results include the language of the domain name, the domain name's UTF-8 encoded representation along with the Unicode code page.

26.4.2 Web Page for WHOIS queries

In addition to the WHOIS Service on port 43, Neustar provides a web based WHOIS application (www.whois.TUNES). It is an intuitive and easy to use application for the general public to use. WHOIS web application provides all of the features available in the port 43 WHOIS. This includes full and partial search on:

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

It also provides features not available on the port 43 service. These include:

1. Redemption Grace Period calculation: Based on the registry's policy, domains in pendingDelete can be restorable or scheduled for release depending on the date/time the domain went into pendingDelete. For these domains, the web based WHOIS displays "Restorable" or "Scheduled for Release" to clearly show this additional status to the user.
2. Extensive support for international domain names (IDN)
3. Ability to perform WHOIS lookups on the actual Unicode IDN
4. Display of the actual Unicode IDN in addition to the ACE-encoded name
5. A Unicode to Punycode and Punycode to Unicode translator
6. An extensive FAQ
7. A list of upcoming domain deletions

26.5 IT and Infrastructure Resources

As described above the WHOIS architecture uses a workflow that decouples the update process

from the SRS. This ensures SRS performance is not adversely affected by the load requirements of dynamic updates. It is also decoupled from the WHOIS lookup agent to ensure the WHOIS service is always available and performing well for users. Each of Neustar's geographically diverse WHOIS sites use:

- Firewalls, to protect this sensitive data
- Dedicated servers for MQ Series, to ensure guaranteed delivery of WHOIS updates
- Packetshaper for source IP address-based bandwidth limiting
- Load balancers to distribute query load
- Multiple WHOIS servers for maximizing the performance of WHOIS service.

The WHOIS service uses HP BL 460C servers, each with 2 X Quad Core CPU and a 64GB of RAM. The existing infrastructure has 6 servers, but is designed to be easily scaled with additional servers should it be needed.
Figure 26-1 depicts the different components of the WHOIS architecture.

26.6 Interconnectivity with Other Registry System
As described in Question 24 about the SRS and further in response to Question 31, "Technical Overview", when an update is made by a registrar that impacts WHOIS data, a trigger is sent to the WHOIS system by the external notifier layer. The update agent processes these updates, transforms the data if necessary and then uses messaging oriented middleware to publish all updates to each WHOIS slave. The local update agent accepts the update and applies it to the local in-memory database. A separate auditor compares the data in WHOIS and the SRS daily and monthly to ensure accuracy of the published data.
26.7 Frequency of Synchronization between Servers
Updates from the SRS, through the external notifiers, to the constellation of independent WHOIS slaves happens in real-time via an asynchronous publish/subscribe messaging architecture. The updates are guaranteed to be updated in each slave within the required SLA of 95% ≤ 60 minutes. Please note that Neustar's current architecture is built towards the stricter SLAs (95% ≤ 15 minutes) of .BIZ. The vast majority of updates tend to happen within 2-3 minutes.
26.8 Provision for Searchable WHOIS Capabilities
Neustar will create a new web-based service to address the new search features based on requirements specified in Specification 4 Section 1.8. The application will enable users to search the WHOIS directory using any one or more of the following fields:

- Domain name
- Registrar ID
- Contacts and registrant's name
- Contact and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state or province, etc.)
- Name server name and name server IP address
- The system will also allow search using non-Latin character sets which are compliant with IDNA specification.

The user will choose one or more search criteria, combine them by Boolean operators (AND, OR, NOT) and provide partial or exact match regular expressions for each of the criterion name-value pairs. The domain names matching the search criteria will be returned to the user.
Figure 26-2 shows an architectural depiction of the new service.

Potential Forms of Abuse
As recognized by the Terms of Reference for Whois Misuse Studies, http://gnso.icann.org/issues/whois/tor-whois-misuse-studies-25sep09-en.pdf, a number of reported and recorded harmful acts, such as spam, phishing, identity theft, and stalking which Registrants believe were sent using WHOIS contact information. Although these Whois studies are still underway, there is a general belief that public access to Whois data may lead to a measurable degree of misuse – that is, to actions that cause actual harm, are illegal or illegitimate, or otherwise contrary to the stated legitimate purpose. One of the other key focuses of these studies will be to correlate the reported incidents of harmful acts with anti-harvesting measures that some Registrars and Registries apply to WHOIS queries (e.g., rate limiting, CAPTCHA, etc.).

Neustar firmly believes that adding the increased search capabilities, without appropriate controls could exacerbate the potential abuses associated with the Whois service. To mitigate the risk of this powerful search service being abused by unscrupulous data miners, a layer of security will be built around the query engine which will allow the registry to identify rogue activities and then take appropriate measures. Potential abuses include, but are not limited to:

- Data Mining
- Unauthorized Access
- Excessive Querying
- Denial of Service Attacks

To mitigate the abuses noted above, Neustar will implement any or all of these mechanisms as appropriate:

- Username-password based authentication
- Certificate based authentication
- Data encryption
- CAPTCHA mechanism to prevent robo invocation of Web query
- Fee-based advanced query capabilities for premium customers.

The searchable WHOIS application will adhere to all privacy laws and policies of the .TUNES registry.
26.9 Resourcing Plans
As with the SRS, the development, customization, and on-going support of the WHOIS service is the responsibility of a combination of technical and operational teams. The primary groups responsible for managing the service include:

Development/Engineering – 19 employees
Database Administration – 10 employees
Systems Administration – 24 employees
Network Engineering – 5 employees

Additionally, if customization or modifications are required, the Product Management and Quality Assurance teams will also be involved. Finally, the Network Operations and Information Security play an important role in ensuring the systems involved are operating securely and reliably. The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. Neustar's WHOIS implementation is very mature, and has been in production for over 10 years. As such, very little new development will be required to support the implementation of the .TUNES registry. The resources are more than adequate to support the WHOIS needs of all the TLDs operated by Neustar, including the .TUNES registry.

---

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

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

The description of the registration lifecycle should be supplemented by the inclusion of a state diagram, which captures definitions, explanations of trigger points, and transitions from state to state.
If applicable, provide definitions for aspects of the registration lifecycle that are not covered by standard EPP RFCs.
A complete answer is expected to be no more than 5 pages.

27.1 Registration Life Cycle

Introduction

.TUNES will follow the lifecycle and business rules found in the majority of gTLDs today. Our back-end operator, Neustar, has over ten years of experience managing numerous TLDs that utilize standard and unique business rules and lifecycles. This section describes the business rules, registration states, and the overall domain lifecycle that will be used for .TUNES.

Domain Lifecycle - Description

The registry will use the EPP 1.0 standard for provisioning domain names, contacts and hosts. Each domain record is comprised of three registry object types: domain, contacts, and hosts Domains, contacts and hosts may be assigned various EPP defined statuses indicating either a particular state or restriction placed on the object. Some statuses may be applied by the Registrar; other statuses may only be applied by the Registry. Statuses are an integral part of the domain lifecycle and serve the dual purpose of indicating the particular state of the domain and indicating any restrictions placed on the domain. The EPP standard defines 17 statuses, however only 14 of these statuses will be used in the .TUNES registry per the defined .TUNES business rules.

The following is a brief description of each of the statuses. Server statuses may only be applied by the Registry, and client statuses may be applied by the Registrar.

OK – Default status applied by the Registry.

Inactive – Default status applied by the Registry if the domain has less than 2 nameservers.

PendingCreate – Status applied by the Registry upon processing a successful Create command, and indicates further action is pending. This status will not be used in the .TUNES registry.

PendingTransfer – Status applied by the Registry upon processing a successful Transfer request command, and indicates further action is pending.

PendingDelete – Status applied by the Registry upon processing a successful Delete command that does not result in the immediate deletion of the domain, and indicates further action is pending.

PendingRenew – Status applied by the Registry upon processing a successful Renew command that does not result in the immediate renewal of the domain, and indicates further action is pending. This status will not be used in the .TUNES registry.

PendingUpdate – Status applied by the Registry if an additional action is expected to complete the update, and indicates further action is pending. This status will not be used in

the .TUNES registry.

Hold – Removes the domain from the DNS zone.

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

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

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

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

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

Domain may be updated

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

Domain may be renewed at anytime during the term

Domain may be auto-renewed by the Registry

Domain may be transferred to another registrar.

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

27.1.1 Registration States

Domain Lifecycle – Registration States

As described above the .TUNES registry will implement a standard domain lifecycle found in most gTLD registries today. There are five possible domain states:

Active

Inactive

Locked

Pending Transfer

Pending Delete.

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

Active State

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

Inactive State

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

Locked State

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

Pending Transfer State

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

Pending Delete State

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

27.1.2 Typical Registration Lifecycle Activities

Domain Creation Process

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

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

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

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

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

Update Process

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

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

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

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

Renew Process

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

Transfer Process

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

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

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

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

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

Deletion Process

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

27.1.3 Applicable Time Elements

The following section explains the time elements that are involved.

Grace Periods

There are six grace periods:

- Add-Delete Grace Period (AGP)
- Renew-Delete Grace Period
- Transfer-Delete Grace Period
- Auto-Renew-Delete Grace Period
- Auto-Renew Grace Period
- Redemption Grace Period (RGP).

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

The following describes each of these grace periods in detail.

Add-Delete Grace Period

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

Renew-Delete Grace Period

The Renew-Delete Grace Period is associated with the date the Domain was renewed. Domains may

be deleted for credit during the 120 hours after a renewal. The grace period is intended to allow Registrars to correct domains that were mistakenly renewed. It should be noted that domains that are deleted during the renew grace period will be placed into pendingDelete and will enter the RGP (see below).

Transfer-Delete Grace Period

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

Auto-Renew-Delete Grace Period

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

Auto-Renew Grace Period

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

Redemption Grace Period

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

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

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

27.2 State Diagram

Figure 27-1 provides a description of the registration lifecycle.

The different states of the lifecycle are active, inactive, locked, pending transfer, and pending delete. Please refer to section 27.1.1 for detail description of each of these states. The lines between the states represent triggers that transition a domain from one state to another.

The details of each trigger are described below:

Create: Registry receives a create domain EPP command.

WithNS: The domain has met the minimum number of nameservers required by registry policy in order to be published in the DNS zone.

WithOutNS: The domain has not met the minimum number of nameservers required by registry policy. The domain will not be in the DNS zone.

Remove Nameservers: Domain's nameserver(s) is removed as part of an update domain EPP command. The total nameserver is below the minimum number of nameservers required by registry policy in order to be published in the DNS zone.

Add Nameservers: Nameserver(s) has been added to domain as part of an update domain EPP command. The total number of nameservers has met the minimum number of nameservers required by registry policy in order to be published in the DNS zone.

Delete: Registry receives a delete domain EPP command.

DeleteAfterGrace: Domain deletion does not fall within the add grace period.

DeleteWithinAddGrace: Domain deletion falls within add grace period.

Restore: Domain is restored. Domain goes back to its original state prior to the delete command.

Transfer: Transfer request EPP command is received.

Transfer Approve/Cancel/Reject: Transfer requested is approved or cancel or rejected.

TransferProhibited: The domain is in clientTransferProhibited and/or serverTranferProhibited status. This will cause the transfer request to fail. The domain goes back to its original state.

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

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

27.2.1 EPP RFC Consistency

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

27.3 Resources

The registration lifecycle and associated business rules are largely determined by policy and business requirements; as such the Product Management and Policy teams will play a critical

role in working with Amazon EU S.à r.l. to determine the precise rules that meet the requirements of the TLD. Implementation of the lifecycle rules will be the responsibility of Development/Engineering team, with testing performed by the Quality Assurance team.
Neustar's SRS implementation is very flexible and configurable, and in many case development is not required to support business rule changes.
The .TUNES registry will be using standard lifecycle rules, and as such no customization is anticipated. However should modifications be required in the future, the necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:
Development/Engineering – 19 employees
Registry Product Management – 4 employees
These resources are more than adequate to support the development needs of all the TLDs operated by Neustar, including the .TUNES registry.

---

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

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

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

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

deletion requests; and
- Requiring the notification of multiple, unique points of contact when a domain has been updated, transferred, or deleted.

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

28.1 Abuse Prevention and Mitigation

Amazon EU S.à r.l. and its registry service provider, Neustar, recognize that preventing and mitigating abuse and malicious conduct in the <.TLD> registry is an important and significant responsibility. Amazon EU S.à r.l. will leverage Neustar's extensive experience in establishing and implementing registration policies to prevent and mitigate abusive and malicious domain activity within the proposed <.TLD> space.

Amazon will provision <.TLD> domains to third parties in accordance with the TLD registration policy. Opportunities for abusive and malicious domain activity in <.TLD> are therefore very restricted but we will nonetheless abide by our obligations to ICANN. A responsible domain name registry works towards the eradication of abusive domain name registrations and malicious activity, which may include conduct such as:

• Illegal or fraudulent actions
•Spam
• Phishing
• Pharming
• Distribution of malware
• Fast flux hosting
• Botnets
• Malicious hacking
• Distribution of child pornography
• Online sale or distribution of illegal pharmaceuticals.

By taking an active role in researching and monitoring abusive domain name registration and malicious conduct, Neustar has developed the ability to efficiently work with various law enforcement and security communities to mitigate fast flux DNS-using botnets.

Policies and Procedures to Minimize Abusive Registrations

A registry must have the policies, resources, personnel, and expertise in place to combat such abusive registration and malicious conduct. Neustar, Amazon EU S.à r.l.'s registry services provider, has played a leading role in preventing of such abusive practices, and has developed and implemented a "domain takedown" policy. Amazon EU S.à r.l. also believes that combating abusive use of the DNS is important in protecting registrants.

Removing a domain name from the DNS before it can cause harm is often the best preventative measure for thwarting certain malicious conduct such as botnets and malware distribution. Because removing a domain name from the zone will stop all activity associated with the domain name, including websites and e-mail, the decision to remove a domain name from the DNS must follow a documented process, culminating in a determination that the domain name to be removed poses a threat to the security and stability of the Internet or the registry. Amazon EU S.à r.l., via Neustar, has an extensive, defined, and documented process for taking the necessary action of removing a domain from the zone when its presence in the zone poses a threat to the security and stability of the infrastructure of the Internet or the registry.

Abuse Point of Contact

As required by the Registry Agreement, Amazon EU S.à r.l. will establish and publish on its website a single abuse point of contact responsible for addressing inquiries from law enforcement and the public related to malicious and abusive conduct. Amazon EU S.à r.l. will also provide such information to ICANN before delegating any domain names in <.TLD>. This information shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of malicious conduct complaints, and a telephone number and mailing address for the primary contact. Amazon EU S.à r.l. will ensure that this information is accurate and current, and that updates are provided to ICANN if and when changes are made. In addition, the registry services provider for <.TLD>, Neustar, shall continue to have an additional point of contact for requests from registrars related to abusive domain name practices.

28.2 Policies Regarding Abuse Complaints

Amazon EU S.à r.l. will adopt an Acceptable Use Policy that (i) clearly defines the types of activities that will not be permitted in <.TLD>; (ii) reserves Amazon EU S.à r.l.'s right to lock, cancel, transfer or otherwise suspend or take down domain names violating the Acceptable Use Policy; and (iii) identify the circumstances under which Amazon EU S.à r.l. may share information with law enforcement. Amazon EU S.à r.l. will incorporate its <.TLD> Acceptable User Policy into its Registry-Registrar Agreement.
Under the <.TLD> Acceptable Use Policy, which is set forth below, Amazon EU S.à r.l. may lock down the domain name to prevent any changes to the domain name contact and nameserver information, place the domain name "on hold" rendering the domain name non-resolvable, transfer

the domain name to another registrar and/or in cases in which the domain name is associated with an ongoing law enforcement investigation, Amazon EU S.à r.l. will coordinate with law enforcement to assist in the investigation as described in more detail below.

It is Amazon EU S.à r.l.'s intention that all <.TLD> domain names will be registered and used by eligible users and that only ICANN-accredited registrars that have signed a Registry-Registrar Agreement will be permitted to register <.TLD> domain names. Accordingly, the potential for abusive registrations and malicious conduct in the <.TLD> registry is expected to be limited. In the unlikely event that such abuse should occur, Amazon EU S.à r.l. will work with its registry services provider, Neustar, to implement the following policies and processes to prevent and mitigate such activities. Below is initial Acceptable Use Policy for the <.TLD> registry.

<.TLD> Acceptable Use Policy

This Acceptable Use Policy gives the <.TLD> registry the ability to quickly lock, cancel, transfer or take ownership of any <.TLD> domain name, either temporarily or permanently, if the domain name is being used in a manner that appears to threaten the stability, integrity or security of the <.TLD> registry, or any of its registrar partners – and/or that may put the safety and security of any registrant or user at risk. The process also allows the <.TLD> registry to take preventive measures to avoid any such criminal or security threats.

The Acceptable Use Policy may be triggered through a variety of channels, including, among other things, private complaint, public alert, government or enforcement agency outreach, and the on-going monitoring by the <.TLD> registry or its partners. In all cases, the <.TLD> registry or its designees will alert <.TLD> registry's registrar partners about any identified threats and will work closely with them to bring offending sites into compliance.

The following are some (but not all) activities that may be subject to rapid domain compliance:

- Phishing: the attempt to acquire personally identifiable information by masquerading as a website other than <.TLD>'s own.
- Pharming: the redirection of Internet users to websites other than those the user intends to visit, usually through unauthorized changes to the Hosts file on a victim's computer or DNS records in DNS servers.
- Dissemination of Malware: the intentional creation and distribution of "malicious" software designed to infiltrate a computer system without the owner's consent, including, without limitation, computer viruses, worms, key loggers, and Trojans.
- Malicious Fast Flux Hosting: a technique used to shelter Phishing, Pharming and Malware sites and networks from detection and to frustrate methods employed to defend against such practices, whereby the IP address associated with fraudulent websites are changed rapidly so as to make the true location of the sites difficult to find.
- Botnetting: the development and use of a command, agent, motor, service, or software which is implemented: (1) to remotely control the computer or computer system of an Internet user without their knowledge or consent, (2) to generate direct denial of service (DDOS) attacks.
- Malicious Hacking: the attempt to gain unauthorized access (or exceed the level of authorized access) to a computer, information system, user account or profile, database, or security system.
- Child Pornography: the storage, publication, display and/or dissemination of pornographic materials depicting individuals under the age of majority in the relevant jurisdiction.

The <.TLD> registry reserves the right, in its sole discretion, to take any administrative and operational actions necessary, including the use of computer forensics and information security technological services, among other things, in order to implement the Acceptable Use Policy. In addition, the <.TLD> registry reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of the <.TLD> registry as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement, or (5) to correct mistakes made by the <.TLD> registry or any Registrar in connection with a domain name registration. The <.TLD> registry also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

Taking Action Against Abusive and/or Malicious Activity

The <.TLD> registry is committed to acting in a timely manner against those domain names associated with abuse or malicious conduct in violation of the Acceptable Use Policy. After a complaint is received from a trusted source or third-party, or detected by the <.TLD> registry, the registry will use commercially reasonable efforts to verify the information in the complaint. If that information can be verified to the best of the registry's ability, the sponsoring registrar will be notified and have 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. If the registrar has not acted when the 12-hour period ends (i.e., is unresponsive to the request or refuses to take action), the <.TLD> registry will place the domain on "ServerHold". (It is unlikely a registrar will not timely act because Amazon EU S.à r.l. intends to use a registrar contract reflecting these

policies). ServerHold removes the domain name from the <.TLD> zone, but the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

Coordination with Law Enforcement

Amazon EU S.à r.l. will obtain assistance from Neustar to meet its obligations under Section 2.8 of the Registry Agreement to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the <.TLD> registry. The <.TLD> registry will respond to legitimate law enforcement inquiries promptly upon receiving the request.

The response shall include, at a minimum, an acknowledgement of receipt of the request, questions or comments concerning the request, and an outline of the next steps to be taken by Amazon EU S.à r.l. for rapid resolution of the request. If the request involves any of the activities that can be validated by the registry and implicates activity covered by the <.TLD> Acceptable Use Policy, the sponsoring registrar will have 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. The <.TLD> Registry will place the domain on “ServerHold” if the registrar has not acted within the 12-hour period.

Monitoring for Malicious Activity

Neustar, <.TLD>’s registry services provider, has developed and implemented an active “domain takedown” policy in which the registry itself takes down abusive domain names.

Neustar targets domain names verified to be abusive and removes them within 12 hours regardless of whether the domain name registrar cooperated. Neustar has determined that the benefit in removing such threats outweighs any potential damage to the registrar/registrant relationship. Amazon EU S.à r.l.’s registration policies make it unlikely that any <.TLD> domains will be taken down. Moreover, only registrars that contractually agree to cooperate in stemming abusive behaviors will be permitted to register <.TLD> domain names.

Neustar’s active prevention policies stem from the notion that registrants in <.TLD> have a reasonable expectation that they control the data associated with their domains, especially its presence in the DNS zone. Removing a domain name from the DNS before it can cause harm is often the best preventative measure for thwarting certain malicious conduct such as botnets and malware distribution that harms not only the domain name registrant, but also potentially millions of unsuspecting Internet users.

Rapid Takedown Process

Since implementing the program, Neustar has developed two basic variations of the process. The more common process variation is a lightweight process that is triggered by “typical” notices. The less common variation is the full process that is triggered by unusual notices, which generally allege that a domain name is being used to threaten the stability and security of the TLD, or is part of a real-time investigation by law enforcement or security researchers. In these cases, accelerated action by the registry is necessary. These processes are described below.

Lightweight Process

In addition to having an active Information Security group that, on its own initiatives, seeks out abusive practices in the <.TLD> registry, Neustar is an active member in a number of security organizations that have the expertise and experience in receiving and investigating reports of abusive DNS practices, including but not limited to, the Anti-Phishing Working Group, Castle Cops, NSP-SEC, the Registration Infrastructure Safety Group and others. Each of these sources is a well-known security organization that has a reputation for preventing abuse and malicious conduct on the Internet. Aside from these organizations, Neustar also actively participates in privately run security associations that operate based on trust and anonymity, making it much easier to obtain information regarding abusive DNS activity.

Once a complaint is received from a trusted source or third-party, or detected by Neustar’s internal security group, information about the abusive practice is forwarded to an internal mail distribution list that includes members of Neustar’s operations, legal, support, engineering, and security teams for immediate response (“CERT Team”). Although the impacted URL is included in the notification e-mail, the CERT Team is trained not to investigate the URLs themselves because the URLs in question often have scripts, bugs, etc. that can compromise the individual’s own computer and the network safety. Rather, the investigation is conducted by CERT team members who can access the URLs in a laboratory environment to avoid compromising the Neustar network. The lab environment is designed specifically for these types of tests and is scrubbed on a regular basis to ensure that none of Neustar’s internal or external network elements are harmed in any fashion.
Once the complaint has been reviewed and the alleged abusive domain name activity is verified to the best of the ability of the CERT Team, the sponsoring registrar has 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone.
The <.TLD> Registry will place the domain on “ServerHold” if the registrar has not acted within

the 12-hour period.
ServerHold removes the domain name from the <.TLD> zone, but the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement.

Full Process

In the unlikely event that Neustar receives a complaint that claims that a domain name is being used to threaten the stability and security of the <.TLD> registry, or is a part of a real-time investigation by law enforcement or security, Neustar follows a slightly different course of action.
Upon initiation of this process, members of the CERT Team are paged and a teleconference bridge is immediately opened up for the CERT Team to assess whether the activity warrants immediate action. If the CERT Team determines the incident is not an immediate threat to the security and the stability of critical Internet infrastructure, the CERT Team provides documentation to the Neustar Network Operations Center to clearly capture the rationale for the decision and either refers the incident to the Lightweight process set forth above or closes the incident.

However, if the CERT TEAM determines that there is a reasonable likelihood that the incident warrants immediate action, a determination is made to immediately remove the domain from the zone. As such, Customer Support will contact the registrar immediately to communicate that there is a domain involved in a security and stability issue. The registrar is provided only the domain name in question and the broadly stated type of incident.

Coordination with Law Enforcement & Industry Groups

Neustar has a close working relationship with a number of law enforcement agencies, both in the United States and Internationally. For example, in the United States, Neustar is in constant communication with the Federal Bureau of Investigation, US CERT, Homeland Security, the Food and Drug Administration, and the National Center for Missing and Exploited Children.
Neustar also participates in a number of industry groups aimed at sharing information among key industry players about the abusive registration and use of domain names. These groups include the Anti-Phishing Working Group and the Registration Infrastructure Safety Group (where Neustar served for several years on the Board of Directors). Through these organizations and others, Neustar proactively shares information with other registries, registrars, ccTLDs, law enforcement, security professionals, etc. not only on abusive domain name registrations within its own TLDs, but also with respect to information uncovered with respect to domain names in other registries' TLDs. Neustar has often found that rarely are abuses found only in the TLDs for which it manages, but also within other TLDs, such as .com and .info. Neustar routinely provides this information to the other registries so that the relevant registry can take the appropriate action.

With the assistance of Neustar as its registry services provider, Amazon EU S.à r.l. can meet its obligations under Section 2.8 of the Registry Agreement to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its <.TLD> registry. Amazon EU S.à r.l. and/or Neustar will respond to legitimate law enforcement inquiries promptly upon receiving the request. Such response shall include, at a minimum, an acknowledgement of receipt of the request, questions or comments concerning the request, and an outline of the next steps to be taken by Amazon EU S.à r.l. and/or Neustar for rapid resolution of the request.
If the request involves any of the activities that can be validated by the registry and/or Neustar and implicates the type of activity set forth in the Acceptable Use Policy, the sponsoring registrar will have 12 hours to investigate the activity further and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. The <.TLD> registry will place the domain on "ServerHold" if the registrar has not acted within the 12-hour period.

28.3 Measures for Removal of Orphan Glue Records

As the Security and Stability Advisory Committee of ICANN (SSAC) rightly acknowledges, although orphaned glue records may be used for abusive or malicious purposes, the "dominant use of orphaned glue supports the correct and ordinary operation of the DNS." See http://www.icann.org/en/committees/security/sac048.pdf.

While orphan glue often support correct and ordinary operation of the DNS, such glue records can be used maliciously to point to name servers that host domains used in illegal phishing, bot-nets, malware, and other abusive behaviors. Problems occur when the parent domain of the glue record is deleted but its children glue records still remain in DNS. Therefore, when the <.TLD> registry has written evidence of actual abuse of orphaned glue, the <.TLD> registry will act to remove those records from the zone to mitigate such malicious conduct.

Neustar runs a daily audit of entries in its DNS systems and compares those with its provisioning system, which serves as an umbrella protection that items in the DNS zone are valid. Any DNS record that shows up in the DNS zone but not in the provisioning system is flagged for investigation and removed if necessary. This daily DNS audit prevents not only orphaned hosts but also other records that should not be in the zone.
In addition, if either Amazon EU S.à r.l. or Neustar becomes aware of actual abuse on orphaned glue after receiving written notification from a third party through its Abuse Contact or through its customer support, such glue records will be removed from the zone.

28.4 Measures to Promote WHOIS Accuracy

The <.TLD> registry will implement several measures to promote Whois accuracy. Whois service for Amazon EU S.à r.l. will operate as follows. The registry will keep all basic contact details for each domain name in a unique internal system, which facilitates access to the domain information. In addition, Amazon EU S.à r.l. will perform internal monitoring checks and procedures that will only allow accurate Whois information and remove outdated data.

28.4.1. Authentication of Registrant Information

Amazon EU S.à r.l. will guarantee the adequate authentication of registrant data, ensuring the highest levels of accuracy and diligence when dealing with Whois data. In doing so, Amazon EU S.à r.l.'s solid internal system will undertake, but not be limited to the following measures: running checks against Whois internal records and regular verification of all contact details and other relevant registrant information. The registrar will also be charged with regularly checking Whois accuracy.

Amazon EU S.à r.l. will have a well-defined registration policy that will include a requirement that complete and accurate registrant details are provided by the requestor for a domain. These details will be validated by the registrar who will have a contractual duty to comply with Amazon EU S.à r.l.'s registration policy. The full details of every domain requestor will be kept in Amazon EU S.à r.l.'s on-line registry management dashboard which can be accessed by Amazon EU S.à r.l.'s Domain Management Team at any time.

28.4.2. Regular Monitoring of Registration Data

Amazon EU S.à r.l. will comply with ICANN's Whois requirements. Among other measures, Amazon EU S.à r.l. will regularly remind its internal personnel to comply with ICANN's Whois information Policy through regularly checking Whois data against internal records, offering Whois accuracy services, evaluating claims of fraudulent Whois data, and cancelling domain name registrations with outdated Whois details.

28.4.3. Policies and Procedures ensuring compliance

Amazon EU S.à r.l.'s Registry-Registrar Agreement will require a registrar to take steps necessary to ensure Whois data is complete and accurate and to implement the <.TLD> registration policies.

28.5 Resourcing Plans

Responsibility for abuse mitigation rests with a variety of functional groups at Neustar. The Neustar Abuse Monitoring team is primarily responsible for providing analysis and conducting investigations of reports of abuse. The Neustar Customer Service team also plays an important role in assisting with investigations, responding to customers, and notifying registrars of abusive domains. Finally, the Neustar Policy/Legal team is responsible for developing the relevant policies and procedures.

The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:

Customer Support – 12 employees

Policy/Legal – Two employees

The resources are more than adequate to support the abuse mitigation procedures of the <.TLD> registry.

Furthermore, Amazon EU S.à r.l. dedicates significant financial and personnel resources to combating malicious and abusive behavior in the DNS and across the internet. Amazon EU S.à r.l. will extend these resources to designating the unique abuse point of contact, regularly monitoring potential abusive and malicious activities with support from dedicated technical staff, analyzing reported abuse and malicious activity, and acting to address such reported activity.

The designated abuse prevention staff within Neustar and Amazon EU S.à r.l. will be subject to regular evaluations, receive adequate training and work under expert supervision. The abuse prevention resources will comprise both internal staff and external abuse prevention experts who would give extra advice and support when necessary. This external staff includes one legal expert and four operational experts.

Please note that in the above answer the terms "We", "Our" and "Amazon" may refer to either the applicant Amazon EU S.à r.l. or Amazon.com Inc., the ultimate parent, or sometimes NeuStar, the registry services provider.

---

29. Rights Protection Mechanisms: Applicants must describe how their registry will comply with policies

and practices that minimize abusive registrations and other activities that affect the legal rights of others, such as the Uniform Domain Name Dispute Resolution Policy (UDRP), Uniform Rapid Suspension (URS) system, and Trademark Claims and Sunrise services at startup.
A complete answer should include:

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

>To be eligible for a score of 2, answers must also include additional measures specific to rights protection, such as abusive use policies, takedown procedures, registrant pre-verification, or authentication procedures, or other covenants.
A complete answer is expected to be no more than 10 pages.

29.1 Introduction

Amazon is applying for <.TLD> to provide a dedicated platform for stable and secure online communication and interaction. Amazon has several thousand registered intellectual property assets of all types including trademarks, designs, and domain names – we place the protection of our intellectual property as a high priority and we respect the intellectual property of others.

29.1.1 Rights protection in gTLD registry operation is a core objective of Amazon

We will require registrars to work with us on a four-step registration process featuring: (i) Eligibility Confirmation; (ii) Naming Convention Check; (iii) Acceptable Use Review; and (iv) Registration. As stated in our answer to Question 18, all domains in our registry will be subject to eligibility requirements.

We believe that the above registration process will ensure that abusive registrations are prevented, but we will continue to monitor ICANN policy developments, and update our procedures as required.

29.2 Core measures to prevent abusive registrations

To further prevent abusive registration or cybersquatting, we will adopt the following Rights Protection Mechanisms (RPMs) which have been mandated for new gTLD operators by ICANN:

- A 30 day Sunrise process
- A 60 day Trademark Claims process

Generally, these RPMs are targeted at abusive registrations undertaken by third parties. However, domains in our registry will be registered by Amazon and eligible trusted third parties through registrars who will be contractually required to ensure that stated rules covering eligibility and use of a domain are adhered to through a validation process. As a result, abusive registrations should be prevented.

29.2.1 Sunrise Eligibility

Our Sunrise Eligibility Requirements will clearly set out criteria for registration in this TLD. Notice of our Sunrise will be provided to third party holders of validated trademarks in the Trademark Clearinghouse as required by ICANN. Our Sunrise Eligibility Requirements will be published on the website of our registry.

29.2.2 Sunrise Window

As required in the Applicant Guidebook in section 7.1, our Sunrise window will recognize "all word marks: (i) nationally or regionally registered and for which proof of use – which can be a declaration and a single specimen of current use – was submitted to, and validated by, the Trademark
Clearinghouse; or (ii) that have been court-validated; or (iii) that are specifically protected by a statute or treaty currently in effect and that was in effect on or before 26 June 2008".

Our Sunrise window will last for 30 days. Applications received from an ICANN-accredited registrar will be accepted for registration if they are (i) supported by an entry in the Trademark Clearinghouse (TMCH) during our Sunrise window and (ii) satisfy our Sunrise Eligibility Requirements. Once registered, those domain names will normally have a one year term of registration. Any domain names registered will be managed by a registrar.

29.2.3 Sunrise Dispute Resolution Policy

We will devise and publish the rules for our Sunrise Dispute Resolution Policy (SDRP) on our registry website. Our SDRP will allow any party to raise a challenge on the following four grounds as required in the Applicant Guidebook (6.2.4):

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

Complaints can be submitted through our registry website within 30 days following the closure of the Sunrise, and will be initially processed by a registrar which will promptly report to us: (i) the challenger; (ii) the challenged domain name; (iii) the grounds upon which the complaint is based; and (iv) why the challenger believes the grounds are satisfied.

29.2.4 Trademark Claims Service

Our Trademark Claims Service (TMCS) will run for a 60 day period following the closure of our 30 day Sunrise. Our TMCS will be supported by the Trademark Clearinghouse and will provide a notice to third parties interested in filing a character string in our registry of a registered trademark right that matches the character string in the TMCH.

We will honor and recognize in our TMCS the following types of marks as defined in the Applicant Guidebook section 7.1: (i) nationally or regionally registered; (ii) court-validated; or (iii) specifically protected by a statute or treaty in effect at the time the mark is submitted to the Clearinghouse for inclusion.

Once received from the TMCH, with which our registry provider will interface, a claim will be initially processed by a registrar who will provide a report to us on the eligibility of the applicant.

29.2.5 Implementation and Resourcing Plans of core services to prevent abusive registration

Our Sunrise and IP Claims service will be introduced with the following timetable:

Day One: Announcement of Registry Launch and publication of registry website with details of the Sunrise and Trademark Claim Service (“TMCS”)
Day 30: Sunrise opens for 30 days on a first-come, first served basis. Once registrations are approved, they will be entered into the Shared Registry System (SRS) and published in our Thick-Whois database.
Day 60-75: Registry Open, domains applied for in the Sunrise registered and TMCS begins for a minimum of 60 days

Day 120-135: TMCS ends; normal operations continue.

Our Implementation Team will comprise the following:

From Amazon: the Director of IP will lead a team of up to seven experts with experience of domain name management and on-line legal dispute resolution, with access to other teams in Amazon Legal if required.

From NeuStar, registry service provider to Amazon: A Customer Support team of 12, a Product Management Team of four and a Development ⁄ Engineering Team of 19 will be available as required to support the legal team, led by Jeff Neuman. This team has over 10 years’ experience with implementing registry launches including rights protection schemes such as the .biz Sunrise and IP Claims.

In addition, Amazon will be supported externally by two legal specialists, four client managers and six operational staff. The operational staff will undertake the validation checks on registration requests.
The Implementation Team will create a formal Registry Launch plan. This plan will set out the exact process for the launch of each Amazon registry and will define responsibilities and budgets. The Registry website, which is budgeted for in the three year plans provided in our answers to Question 46, will feature Rules of Registration, Rules of Eligibility, Terms & Conditions of Registration, Acceptable Use Policies as well as the Rules of the Sunrise, the Rules of the Sunrise Dispute Resolution Policy and the Rules of the Trademark Claims Service.

Technical implementation between the registry and the Trademark Clearinghouse will be undertaken by the registry service provider as soon as practical after the Trademark Clearinghouse is operational and announces its integration process.

As demonstrated in our answer to question 46, a budget has been set aside to pay fees charged by the Trademark Clearinghouse Operator for this integration.

The contract we have with our registrars (the RRA) will require that registrars use the TMCH, adhere to the Terms & Conditions of the TMCH and will prohibit registrars from filing domains in our registries on their own behalf or utilizing any data from the TMCH except in the provision of their duties as a registrar.

When processing TMCS claims, our registrars will be required to use the specific form of notice provided by ICANN in the Applicant Guidebook.
We will also require our registrars to implement appropriate privacy policies reflecting local requirements. For example, Amazon is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union.

29.3 Mechanisms to identify and address the abusive use of registered domain names on an ongoing basis

To prevent the abusive use of registered domain names on an ongoing basis we will adopt the following Rights Protection Mechanisms (RPMs) which have been mandated by ICANN:

- The Uniform Domain Name Dispute Resolution Policy (UDRP) to address domain names that have been registered and used in bad faith in the TLD.

- The Uniform Rapid Suspension (URS) scheme which is a faster, more efficient alternative to the Uniform Dispute Resolution Policy to deal with clear-cut cases of cybersquatting.

- The Post Delegation Dispute Resolution Procedure (PDDRP).

- Implementation of a Thick WHOIS making it easier for rights holders to identify and locate infringing parties.

The UDRP and the URS are targeted at abusive registrations undertaken by third parties and the PDDRP at so called “Bad Actor” registries.

Abusive behavior by eligible registrants will be prevented by our internal processes, for example the pre-registration validation checks and monitoring of use of our registrars.

We acknowledge that we are subject to the UDRP, the URS and the PDDRP and we will co-operate fully with ICANN and appropriate registries in the unlikely circumstances that complaints are made.

29.3.1 The Uniform Dispute Resolution Policy (UDRP)

The UDRP is an out-of-court dispute resolution mechanism for trademark owners to resolve clear cases of bad faith, abusive registration and use of domain names. The UDRP applies by contract to all domain name registrations in gTLDs. Standing to file a UDRP complaint is limited to trademark owners who must demonstrate their rights. To prevail in a UDRP complaint, the complainant must further demonstrate that the domain name registrant has no rights or legitimate interests in the disputed domain name, and that the disputed domain name has been registered and is being used in bad faith. In the event of a successful claim, the infringing domain name registration is transferred to the complainant’s control.

In the event of a UDRP case ordering transfer of a domain name to a UDRP complainant, any transfer would be subject to the prevailing party meeting the registration eligibility requirements; if such requirements were not met, we may place the domain name that is the subject of the successful complaint on a list that prevents it from being registered again.

29.3.2 The URS

The URS is intended to be a lighter, quicker complement to the UDRP. Like the UDRP, it is intended for clear-cut cases of trademark abuse. Under the URS, the only remedy which a panel may grant is the temporary suspension of a domain name for the duration of the registration period (which may be extended by the prevailing complainant for one year, at commercial rates). URS substantive criteria mirror those of the UDRP but with a higher burden of proof for complainants, and additional registrant defences. Once a determination is rendered, a losing registrant has several appeal possibilities from 30 days up to one year. Either party may file a de novo appeal within 14 days of a decision. There are penalties for filing “abusive complaints” which may result in a ban on future URS filings.

Should a complaint be made, we will respond in a timely fashion, reflecting our contractual responsibility to ICANN as a registry operator.
Should a successful complaint be made, we will suspend the domain name for the duration of the registration period.
We will co-operate with the URS panel providers and panelists as we will co-operate with UDRP panel providers and panelists.

29.3.3 The Post-Delegation Dispute Resolution Procedure (PDDRP)

The PDDRP is an administrative option for trademark owners to file an objection against a registry whose “affirmative conduct” in its operation or use of its gTLD is alleged to cause or materially contribute to trademark abuse. In this way, the PDDRP is intended to act as a higher-level enforcement tool to assist ICANN compliance activities, where rights holders may not be able to continue to turn solely to lower-level multijurisdictional enforcement options in a vastly expanded DNS.

The PDDRP involves a number of procedural layers, such as an administrative compliance review, appointment of a “threshold review panel”, an expert determination as to liability under the procedure (with implementation of any remedies at ICANN’s discretion), a possible de novo appeal and further appeal to arbitration under ICANN’s registry terms. The PDDRP requires specific bad faith conduct including profit from encouraging infringement in addition to “the typical registration fee.”

As set out in the Applicant Guidebook in the appendix summarizing the PDDRP, the grounds for a complaint on a second level registration are that, “(a) there is a substantial pattern or practice of specific bad faith intent by the registry operator to profit from the sale of trademark infringing domain names; and (b) the registry operator’s bad faith intent to profit from the systematic registration of domain names within the gTLD that are identical or confusingly similar to the complainant’s mark, which (i) takes unfair advantage of the distinctive character or the reputation of the complainant’s mark or (ii) impairs the distinctive character or the reputation of the complainant’s mark, or(iii) creates a likelihood of confusion with the complainant’s mark.”

29.3.4 Thick Whois

As required in Specification 4 of the Registry agreement, all Amazon registries will provide Thick Whois. A Thick WHOIS provides a centralized location of registrant information within the control of the registry (as opposed to thin Whois where the data is dispersed across registrars).
Thick Whois will provide rights owners and law enforcement with the ability to review the registration record easily.

We will place a requirement on registrars to ensure that all registrations are filed with accurate Whois details.
Amazon will create and publish a Whois Query email address so that third parties can submit queries about any domains in our registry.

29.3.5 Implementation and Resourcing Plans for mechanisms to identify and address the abusive use of registered domain names on an ongoing basis

Our post-launch rights protection mechanisms will be in place from Day One of the launch of the registry.

To ensure that we are compliant with our obligations as a registry operator, we will develop a section of our registry website to assist third parties involved in UDRP, URS and PDDRP complaints including third parties wishing to make a complaint, ICANN compliance staff and the providers of UDRP and URS panels. This will feature an email address for enquiries relating to disputes or seeking further information on specific domains. We will monitor this address for all of the following: Notice of Complaint, Notice of Default, URS Determination, UDRP Determination, Notice of Appeal and Appeal Panel Findings where appropriate.

As stated in our answer to Question 18, Amazon’s Intellectual Property group will be responsible for the development, maintenance and enforcement of the Domain Management Policy. This will include ensuring that the following implementation targets are met:

- Locking domains that are the subject of URS complaints within 24 hours of receipt of a URS complaint, and ensuring a registrar locks domains that are the subject of UDRP complaints within 24 hours of receipt of a UDRP complaint.

- Confirming the implementation of the lock to the relevant URS provider, and ensure a registrar confirms the implementation of the lock to the relevant UDRP provider.

- Ensuring that a registrar cancels domain names that are the subject of a successful UDRP complaint within 24 hours

- Redirecting servers to a website with the ICANN mandated information following a successful URS within 24 hours

The human resources dedicated to managing post-launch RPM include:

From Amazon: the Director of IP will lead a team of up to seven experts with experience of domain name management and on-line legal dispute resolution, with access to other teams in Amazon Legal if required.

From NeuStar, registry service provider to Amazon: A Customer Support team of 12, a Product

Management Team of four and a Development / Engineering Team of 19 will be available as required to support the legal team, led by Jeff Neuman. This team has over 10 years' experience with implementing registry launches including rights protection schemes including the .biz Sunrise and IP Claims.

In addition, Amazon will be supported externally by two legal specialists, four client managers and six operational staff. The operational staff will undertake the validation checks on registration requests.

We are confident that this staffing is more than adequate for the initial stages of registry operation. Of course, should business goals change requiring more resources, Amazon will closely review any expansion plans, and plan for additional financial, technical, and team-member support to put the Registry in the best position for success.

We will also require registrars to implement appropriate privacy policies reflecting the high standards that we operate. For information on our Privacy Policies, please see: http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496

29.4 Additional Mechanism that exceed requirements

Rights protection is at the core of Amazon's objective in applying for this registry. Therefore we are committed to providing the following additional mechanisms:

29.4.1 Registry Legal Manager

Amazon will appoint a Legal Manager to ensure that we are compliant with ICANN policies. The Legal Manager will also handle all disputes relating to RPMs. This will involve evaluating complaints, working with external legal counsel and law enforcement, and resolving disputes. The Legal Manager will also liaise with external stakeholders including URS and UDRP panel providers, the TMCH operator and trademark holders as needed.

29.4.2 Rights Protection Help Line

Amazon will maintain a Rights Protection Help Line. Calls to this line will be allocated a Case Number and the following details will be recorded: (i) the contact details of the complainant; (ii) the domain name that is the subject of the complaint or query; (iii) the registered right, if any, that is associated with the request; and (iv) an explanation of the concerns.
An initial response to a query or complaint will be made within 24 hours. The Rights Protection Help Line will be in place on Day One of the registry. The cost of the Rights Help Line is reflected in the Projections Templates provided at Question 46 as part of on-going registry maintenance costs.
The aim of the Rights Protection Help Line is to assist third parties in understanding the mission and purpose of our registry and to see if a resolution can be found that is quicker and easier than the filing of a UDRP or URS complaint.

The Legal Manager will oversee the Rights Protection Help Line.

29.4.3 Registrar Accreditation

Amazon may audit the performance of registrars every six months and re-validate our Registry-Registrar Agreements annually. Our audits may include site visits to ensure the security of data etc.

29.4.4 Audits of registration records

Every three months, whichever is the most of 250 or 2% of the total of domain names registered in that period will be reviewed with registrars to ensure accurate registration records and use that is compliant with our Acceptable Use guidelines.

29.4.5 Maintenance of Registry Website

Amazon will create a website for all our registries and we will make it easy for third parties including representatives of law enforcement to contact us by featuring our full contact details (physical, email address and phone number).

29.4.6 Click Wrapping our Terms & Conditions

We may bring to the attention of requestors of domain names the Terms & Conditions of registration and, especially, Acceptable Use terms through Click Wrapping.

29.4.7 Annual Report

Amazon will publish an Annual Report on Rights Protection in our registries on our Registry Website. This will include relevant statistics and it will outline all cases and how they were resolved.

29.4.8 Contacts with WIPO and other DRS providers

Amazon may invite representatives of WIPO and other DRS providers to review our RPMs and to make suggestions on any improvements that we might make after the first full year of

operation.

29.4.9 Registrant Pre-Verification

All requests for registration will be verified by registrars to ensure that they come from eligible applicants. A record of the request will be kept in our on-line domain management console including the requestor's email address and other contact information.

29.4.10 Take down Procedures

Amazon has described Takedown Procedures for domains supporting Abusive Behaviors in Question 28. We will reserve the right to terminate a registration and to take down all associated services after a review by our Legal Manager if a takedown for reasons of rights protection is requested by law enforcement, a representative of a court we recognize etc.

29.4.11 Speed of Response

Wherever possible, as outlined above, Amazon is committed to a response within 24 hours of a complaint being made. This exceeds the guidelines for the UDRP and the URS.

Please note that in the above answer the terms "We", "Our" and "Amazon" may refer to either the applicant Amazon EU S.à r.l. or Amazon.com Inc., the ultimate parent.

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

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

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

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

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

Amazon EU S.à r.l. and our back-end operator, Neustar, recognize the vital need to secure the systems and the integrity of the data in commercial solutions. The .TUNES registry solution will leverage industry-best security practices including the consideration of physical, network, server, and application elements.
Neustar's approach to information security starts with comprehensive information security policies. These are based on the industry best practices for security including SANS (SysAdmin, Audit, Network, Security) Institute, NIST (National Institute of Standards and Technology), and Center for Internet Security (CIS). Policies are reviewed annually by Neustar's information security team.
The following is a summary of the security policies that will be used in the .TUNES registry, including:
1. Summary of the security policies used in the registry operations
2. Description of independent security assessments
3. Description of security features that are appropriate for .TUNES
4. List of commitments made to registrants regarding security levels

All of the security policies and levels described in this section are appropriate for the .TUNES registry.
30.(a).1 Summary of Security Policies

Neustar, Inc. has developed a comprehensive Information Security Program in order to create effective administrative, technical, and physical safeguards for the protection of its information assets, and to comply with Neustar's obligations under applicable law, regulations, and contracts. This Program establishes Neustar's policies for accessing, collecting, storing, using, transmitting, and protecting electronic, paper, and other records containing sensitive information.
The Program defines:

The policies for internal users and our clients to ensure the safe, organized and fair use of information resources.
The rights that can be expected with that use.
The standards that must be met to effectively comply with policy.
The responsibilities of the owners, maintainers, and users of Neustar's information resources.
Rules and principles used at Neustar to approach information security issues

The following policies are included in the Program:

1. Acceptable Use Policy

The Acceptable Use Policy provides the "rules of behavior" covering all Neustar Associates for using Neustar resources or accessing sensitive information.

2. Information Risk Management Policy

The Information Risk Management Policy describes the requirements for the on-going information security risk management program, including defining roles and responsibilities for conducting and evaluating risk assessments, assessments of technologies used to provide information security and monitoring procedures used to measure policy compliance.

3. Data Protection Policy

The Data Protection Policy provides the requirements for creating, storing, transmitting, disclosing, and disposing of sensitive information, including data classification and labeling requirements, the requirements for data retention. Encryption and related technologies such as digital certificates are also covered under this policy.

4. Third Party Policy

The Third Party Policy provides the requirements for handling service provider contracts, including specifically the vetting process, required contract reviews, and on-going monitoring of service providers for policy compliance.

5. Security Awareness and Training Policy

The Security Awareness and Training Policy provide the requirements for managing the on-going awareness and training program at Neustar. This includes awareness and training activities provided to all Neustar Associates.

6. Incident Response Policy

The Incident Response Policy provides the requirements for reacting to reports of potential security policy violations. This policy defines the necessary steps for identifying and reporting security incidents, remediation of problems, and conducting "lessons learned" post-mortem reviews in order to provide feedback on the effectiveness of this Program. Additionally, this policy contains the requirement for reporting data security breaches to the appropriate authorities and to the public, as required by law, contractual requirements, or regulatory bodies.

7. Physical and Environmental Controls Policy

The Physical and Environment Controls Policy provides the requirements for securely storing sensitive information and the supporting information technology equipment and infrastructure. This policy includes details on the storage of paper records as well as access to computer systems and equipment locations by authorized personnel and visitors.

8. Privacy Policy

Neustar supports the right to privacy, including the rights of individuals to control the dissemination and use of personal data that describes them, their personal choices, or life experiences. Neustar supports domestic and international laws and regulations that seek to protect the privacy rights of such individuals.

9. Identity and Access Management Policy

The Identity and Access Management Policy covers user accounts (login ID naming convention, assignment, authoritative source) as well as ID lifecycle (request, approval, creation, use, suspension, deletion, review), including provisions for system/application accounts, shared/group accounts, guest/public accounts, temporary/emergency accounts, administrative access, and remote access. This policy also includes the user password policy requirements.

10. Network Security Policy

The Network Security Policy covers aspects of Neustar network infrastructure and the technical controls in place to prevent and detect security policy violations.

11. Platform Security Policy

The Platform Security Policy covers the requirements for configuration management of servers, shared systems, applications, databases, middle-ware, and desktops and laptops owned or operated by Neustar Associates.

12. Mobile Device Security Policy

The Mobile Device Policy covers the requirements specific to mobile devices with information storage or processing capabilities. This policy includes laptop standards, as well as requirements for PDAs, mobile phones, digital cameras and music players, and any other removable device capable of transmitting, processing or storing information.

13. Vulnerability and Threat Management Policy

The Vulnerability and Threat Management Policy provides the requirements for patch management, vulnerability scanning, penetration testing, threat management (modeling and monitoring) and the appropriate ties to the Risk Management Policy.

14. Monitoring and Audit Policy

The Monitoring and Audit Policy covers the details regarding which types of computer events to record, how to maintain the logs, and the roles and responsibilities for how to review, monitor, and respond to log information. This policy also includes the requirements for backup, archival, reporting, forensics use, and retention of audit logs.

15. Project and System Development and Maintenance Policy

The System Development and Maintenance Policy covers the minimum security requirements for all software, application, and system development performed by or on behalf of Neustar and the minimum security requirements for maintaining information systems.

30. (a).2 Independent Assessment Reports

Neustar IT Operations is subject to yearly Sarbanes-Oxley (SOX), Statement on Auditing Standards #70 (SAS70) and ISO audits. Testing of controls implemented by Neustar management in the areas of access to programs and data, change management and IT Operations are subject to testing by both internal and external SOX and SAS70 audit groups. Audit Findings are communicated to process owners, Quality Management Group and Executive Management. Actions are taken to make process adjustments where required and remediation of issues is monitored by internal audit and QM groups.

External Penetration Test is conducted by a third party on a yearly basis. As authorized by Neustar, the third party performs an external Penetration Test to review potential security weaknesses of network devices and hosts and demonstrate the impact to the environment. The assessment is conducted remotely from the Internet with testing divided into four phases:

A network survey is performed in order to gain a better knowledge of the network that was being tested

Vulnerability scanning is initiated with all the hosts that are discovered in the previous phase

Identification of key systems for further exploitation is conducted

Exploitation of the identified systems is attempted.

Each phase of the audit is supported by detailed documentation of audit procedures and results. Identified vulnerabilities are classified as high, medium and low risk to facilitate management's prioritization of remediation efforts. Tactical and strategic recommendations are provided to management supported by reference to industry best practices.

30.(a).3 Augmented Security Levels and Capabilities

There are no increased security levels specific for .TUNES. However, Neustar will provide the same high level of security provided across all of the registries it manages.

A key to Neustar's Operational success is Neustar's highly structured operations practices. The standards and governance of these processes:

Include annual independent review of information security practices

Include annual external penetration tests by a third party

Conform to the ISO 9001 standard (Part of Neustar's ISO-based Quality Management System)

Are aligned to Information Technology Infrastructure Library (ITIL) and CoBIT best practices

Are aligned with all aspects of ISO IEC 17799

Are in compliance with Sarbanes-Oxley (SOX) requirements (audited annually)

Are focused on continuous process improvement (metrics driven with product scorecards reviewed monthly).

A summary view to Neustar's security policy in alignment with ISO 17799 can be found in section 30.(a).4 below.

30.(a).4 Commitments and Security Levels

The .TUNES registry commits to high security levels that are consistent with the needs of the TLD. These commitments include:

Compliance with High Security Standards

Security procedures and practices that are in alignment with ISO 17799

Annual SOC 2 Audits on all critical registry systems

Annual 3rd Party Penetration Tests

Annual Sarbanes Oxley Audits

Highly Developed and Document Security Policies

Compliance with all provisions described in section 30.(a).4 below and in the attached security policy document.

Resources necessary for providing information security

Fully documented security policies

Annual security training for all operations personnel

High Levels of Registry Security

Multiple redundant data centers

High Availability Design

Architecture that includes multiple layers of security

Diversified firewall and networking hardware vendors

Multi-factor authentication for accessing registry systems

Physical security access controls

A 24x7 manned Network Operations Center that monitors all systems and applications

A 24x7 manned Security Operations Center that monitors and mitigates DDoS attacks

DDoS mitigation using traffic scrubbing technologies

Appendix F

Original Initial Evaluation Scores for Amazon Applications for .MUSIC, .SONG and .TUNES

New gTLD Program
Initial Evaluation Report
Report Date: 21 June 2013

App cat on D:	1-1316-18029
App ed for Str ng:	MUSIC
Pr or ty Number:	838
App cant Name:	Amazon EU S.à r. .

Overall Initial Evaluation Summary

Initial Evaluation Result	**Pass**
Congratu at ons! Based on the rev ew of your app cat on aga nst the re evant cr ter a n the App cant Gu debook (nc ud ng re ated supp ementa notes and adv sor es), your app cat on has passed In t a Eva uat on.	

Background Screening Summary

Background Screening	**Eligible**
Based on rev ew performed to-date, the app cat on s e g b e to proceed to the next step n the Program. ICANN reserves the r ght to perform add t ona background screen ng and research, to seek add t ona nformat on from the app cant, and to reassess and change e g b ty up unt the execut on of the Reg stry Agreement.	

Panel Summary

String Similarity	**Pass - Contention**
The Str ng S m ar ty Pane has determ ned that your app ed-for str ng s v sua y s m ar to another app ed-for gTLD str ng, creat ng a probab ty of user confus on. Based on th s f nd ng and per Sect ons 2.2.1.1 and 2.2.1.2 of the App cant Gu debook, your app cat on was p aced n a str ng content on set.	
DNS Stability	**Pass**
The DNS Stab ty Pane has determ ned that your app cat on s cons stent w th the requ rements n Sect on 2.2.1.3 of the App cant Gu debook.	
Geographic Names	**Not a Geographic Name - Pass**
The Geograph c Names Pane has determ ned that your app cat on does not fa w th n the cr ter a for a geograph c name conta ned n the App cant Gu debook Sect on 2.2.1.4.	
Registry Services	**Pass**
The Reg stry Serv ces Pane has determ ned that the proposed reg stry serv ces do not requ re further rev ew.	
Technical & Operational Capability	**Pass**
The Techn ca & Operat ona Capab ty Pane determ ned that: Your app cat on meets the Techn ca & Operat ona Capab ty cr ter a spec f ed n the App cant Gu debook.	

Quest on	Score
24: SRS	1
25: EPP	1
26: Who s	2
27: Reg strat on L fe Cyc e	1
28: Abuse Prevent on and M t gat on	2
29: R ghts Protect on Mechan sm	2
30: Secur ty Po cy	2
31: Techn ca Overv ew of Reg stry	1
32: Arch tecture	2
33: Database Capab t es	2

34: Geograph c D vers ty	2
35: DNS Serv ce	1
36: IPv6 Reachab ty	1
37: Data Backup Po c es & Procedures	1
38: Data Escrow	1
39: Reg stry Cont nu ty	2
40: Reg stry Trans t on	1
41: Fa over Test ng	1
42: Mon tor ng and Fau t Esca at on	2
43: DNSSEC	1
44: IDNs (Opt ona)	1
Tota	30
M n mum Requ red Tota Score to Pass*	22

**No zero score allowed except on optional Q44*

Financial Capability **Pass**

The F nanc a Capab ty Pane determ ned that:

Your app cat on meets the F nanc a Capab ty cr ter a spec f ed n the App cant Gu debook.

Quest on	Score
45: F nanc a Statements	1
46: Project ons Temp ate	1
47: Costs and Cap ta Expend tures	2
48: Fund ng and Revenue	2
49: Cont ngency P ann ng	2
50: Fund ng Cr t ca Reg stry Funct ons	3
Tota	11
M n mum Requ red Tota Score to Pass**	8

***No zero score allowed on any question*

Disclaimer: P ease note that these In t a Eva uat on resu ts do not necessar y determ ne the f na resu t of the app cat on. In m ted cases the resu ts m ght be subject to change. A app cat ons are subjected to due d gence at contract ng t me, wh ch may nc ude an add t ona rev ew of the Cont nued Operat ons Instrument for conformance to Spec f cat on 8 of the Reg stry Agreement w th ICANN. These resu ts do not const tute a wa ver or amendment of any prov s on of the App cant Gu debook or the Reg stry Agreement. For updated app cat on status and comp ete deta s on the program, p ease refer to the App cant Gu debook and the ICANN New gTLDs m cros te at <newgt ds. cann.org>.

New gTLD Program
Initial Evaluation Report
Report Date: 07 June 2013

App cat on D:	1-1317-53837
App ed for Str ng:	SONG
Pr or ty Number:	628
App cant Name:	Amazon EU S.à r. .

Overall Initial Evaluation Summary

Initial Evaluation Result	**Pass**
Congratu at ons! Based on the rev ew of your app cat on aga nst the re evant cr ter a n the App cant Gu debook (nc ud ng re ated supp ementa notes and adv sor es), your app cat on has passed In t a Eva uat on.	

Background Screening Summary

Background Screening	**Eligible**
Based on rev ew performed to-date, the app cat on s e g b e to proceed to the next step n the Program. ICANN reserves the r ght to perform add t ona background screen ng and research, to seek add t ona nformat on from the app cant, and to reassess and change e g b ty up unt the execut on of the Reg stry Agreement.	

Panel Summary

String Similarity	**Pass - No Contention**
The Str ng S m ar ty Pane has determ ned that your app cat on s cons stent w th the requ rements n Sect ons 2.2.1.1 and 2.2.1.2 of the App cant Gu debook, and your app ed-for str ng s not n content on w th any other app ed-for str ngs.	
DNS Stability	**Pass**
The DNS Stab ty Pane has determ ned that your app cat on s cons stent w th the requ rements n Sect on 2.2.1.3 of the App cant Gu debook.	
Geographic Names	**Not a Geographic Name - Pass**
The Geograph c Names Pane has determ ned that your app cat on does not fa w th n the cr ter a for a geograph c name conta ned n the App cant Gu debook Sect on 2.2.1.4.	
Registry Services	**Pass**
The Reg stry Serv ces Pane has determ ned that the proposed reg stry serv ces do not requ re further rev ew.	
Technical & Operational Capability	**Pass**
The Techn ca & Operat ona Capab ty Pane determ ned that: Your app cat on meets the Techn ca & Operat ona Capab ty cr ter a spec f ed n the App cant Gu debook.	

Quest on	Score
24: SRS	1
25: EPP	1
26: Who s	2
27: Reg strat on L fe Cyc e	1
28: Abuse Prevent on and M t gat on	2
29: R ghts Protect on Mechan sm	2
30: Secur ty Po cy	2
31: Techn ca Overv ew of Reg stry	1
32: Arch tecture	2
33: Database Capab t es	2
34: Geograph c D vers ty	2

35: DNS Serv ce	1
36: IPv6 Reachab ty	1
37: Data Backup Po c es & Procedures	1
38: Data Escrow	1
39: Reg stry Cont nu ty	2
40: Reg stry Trans t on	1
41: Fa over Test ng	1
42: Mon tor ng and Fau t Esca at on	2
43: DNSSEC	1
44: IDNs (Opt ona)	1
Tota	30
M n mum Requ red Tota Score to Pass*	22

**No zero score allowed except on optional Q44*

Financial Capability **Pass**

The F nanc a Capab ty Pane determ ned that:

Your app cat on meets the F nanc a Capab ty cr ter a spec f ed n the App cant Gu debook.

Quest on	Score
45: F nanc a Statements	1
46: Project ons Temp ate	1
47: Costs and Cap ta Expend tures	2
48: Fund ng and Revenue	2
49: Cont ngency P ann ng	2
50: Fund ng Cr t ca Reg stry Funct ons	3
Tota	11
M n mum Requ red Tota Score to Pass**	8

***No zero score allowed on any question*

Disclaimer: P ease note that these In t a Eva uat on resu ts do not necessar y determ ne the f na resu t of the app cat on. In m ted cases the resu ts m ght be subject to change. A app cat ons are subjected to due d gence at contract ng t me, wh ch may nc ude an add t ona rev ew of the Cont nued Operat ons Instrument for conformance to Spec f cat on 8 of the Reg stry Agreement w th ICANN. These resu ts do not const tute a wa ver or amendment of any prov s on of the App cant Gu debook or the Reg stry Agreement. For updated app cat on status and comp ete deta s on the program, p ease refer to the App cant Gu debook and the ICANN New gTLDs m cros te at <newgt ds. cann.org>.

New gTLD Program
Initial Evaluation Report
Report Date: 02 August 2013

App cat on D:	1-1317-30761
App ed for Str ng:	TUNES
Pr or ty Number:	1450
App cant Name:	Amazon EU S.à r. .

Overall Initial Evaluation Summary

Initial Evaluation Result	**Pass**
Congratu at ons! Based on the rev ew of your app cat on aga nst the re evant cr ter a n the App cant Gu debook (nc ud ng re ated supp ementa notes and adv sor es), your app cat on has passed In t a Eva uat on.	

Background Screening Summary

Background Screening	**Eligible**
Based on rev ew performed to-date, the app cat on s e g b e to proceed to the next step n the Program. ICANN reserves the r ght to perform add t ona background screen ng and research, to seek add t ona nformat on from the app cant, and to reassess and change e g b ty up unt the execut on of the Reg stry Agreement.	

Panel Summary

String Similarity	**Pass - No Contention**
The Str ng S m ar ty Pane has determ ned that your app cat on s cons stent w th the requ rements n Sect ons 2.2.1.1 and 2.2.1.2 of the App cant Gu debook, and your app ed-for str ng s not n content on w th any other app ed-for str ngs.	
DNS Stability	**Pass**
The DNS Stab ty Pane has determ ned that your app cat on s cons stent w th the requ rements n Sect on 2.2.1.3 of the App cant Gu debook.	
Geographic Names	**Not a Geographic Name - Pass**
The Geograph c Names Pane has determ ned that your app cat on does not fa w th n the cr ter a for a geograph c name conta ned n the App cant Gu debook Sect on 2.2.1.4.	
Registry Services	**Pass**
The Reg stry Serv ces Pane has determ ned that the proposed reg stry serv ces do not requ re further rev ew.	
Technical & Operational Capability	**Pass**
The Techn ca & Operat ona Capab ty Pane determ ned that: Your app cat on meets the Techn ca & Operat ona Capab ty cr ter a spec f ed n the App cant Gu debook.	

Quest on	Score
24: SRS	1
25: EPP	1
26: Who s	2
27: Reg strat on L fe Cyc e	1
28: Abuse Prevent on and M t gat on	2
29: R ghts Protect on Mechan sm	2
30: Secur ty Po cy	2
31: Techn ca Overv ew of Reg stry	1
32: Arch tecture	2
33: Database Capab t es	2
34: Geograph c D vers ty	2

35: DNS Serv ce	1
36: IPv6 Reachab ty	1
37: Data Backup Po c es & Procedures	1
38: Data Escrow	1
39: Reg stry Cont nu ty	2
40: Reg stry Trans t on	1
41: Fa over Test ng	1
42: Mon tor ng and Fau t Esca at on	2
43: DNSSEC	1
44: IDNs (Opt ona)	1
Tota	30
M n mum Requ red Tota Score to Pass*	22

**No zero score allowed except on optional Q44*

Financial Capability **Pass**

The F nanc a Capab ty Pane determ ned that:

Your app cat on meets the F nanc a Capab ty cr ter a spec f ed n the App cant Gu debook.

Quest on	Score
45: F nanc a Statements	1
46: Project ons Temp ate	1
47: Costs and Cap ta Expend tures	2
48: Fund ng and Revenue	2
49: Cont ngency P ann ng	2
50: Fund ng Cr t ca Reg stry Funct ons	3
Tota	11
M n mum Requ red Tota Score to Pass**	8

***No zero score allowed on any question*

Disclaimer: P ease note that these In t a Eva uat on resu ts do not necessar y determ ne the f na resu t of the app cat on. In m ted cases the resu ts m ght be subject to change. A app cat ons are subjected to due d gence at contract ng t me, wh ch may nc ude an add t ona rev ew of the Cont nued Operat ons Instrument for conformance to Spec f cat on 8 of the Reg stry Agreement w th ICANN. These resu ts do not const tute a wa ver or amendment of any prov s on of the App cant Gu debook or the Reg stry Agreement. For updated app cat on status and comp ete deta s on the program, p ease refer to the App cant Gu debook and the ICANN New gTLDs m cros te at <newgt ds. cann.org>.

Appendix G

Public Comments filed against ICANN-Approved Material Change Requests for Amazon's .MUSIC, .SONG and .TUNES Applications

APPLICATION COMMENT DETAILS

Comment ID: pwkgxamk

Name: Constantine Roussos

Affiliation: .MUSIC (DotMusic Limited)

Applicant: Amazon EU S.à r.l.

String: MUSIC

Application ID: 1-1316-18029

Panel/Objection Ground: Community Objection Ground

Subject: Objection to Approved Change Request 1/4

Comment Submission Date: 26 May 2014 at 19:31:47 UTC

Comment:

Amazon submitted wholesale deletion and addition of key language across all of its sensitive Intellectual Property (IP) related strings (such as music-themed .MUSIC/.SONG/.TUNES). These material changes negatively impact the public and other Applicants.

AGB Section 1.2.7 requires ICANN to balance the following 7 factors in deciding whether to accept the change requests:

1. Explanation – Is a reasonable explanation provided? Answer: It can reasonably be deduced that Amazon's sweeping changes were in response to strong condemnation of Applicant's stated goals to run an exclusive access registry and control critical intellectual property sectors worldwide.

2. Evidence that original submission was in error – Are there indicia to support an assertion that the change merely corrects an error? Answer: NO. There is no "indicia" of error based on Amazon's published defense of its "exclusive access" position in response to Community Objections.

3. Other third parties affected – Does the change affect other third parties materially? Answer: YES - Such changes affect the public, Community Applicants and Objectors, and others in the contention set. Some have spent significant time and expense arguing against Applicant's policies.

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? Answer: These unprecedented massive changes were made without public notice and address Applicant's control of critical IP sectors. Such changes should not be done in secret without debate, evaluation or explanation. Other Applicants have not been permitted to make such sweeping changes. The size of Applicant, the strings

affected and the potential impact on the public warrants further examination.

5. Fairness to applicants – Would allowing the change be construed as fair to the general community? Would disallowing the change be construed as unfair? Answer: All Applicants are bound by the AGB regardless of size, power or influence. Other Applicants appear to be subject to different standards and have had their change requests rejected. Such a massive set of changes for a single powerful applicant without transparency is unfair. Disallowing the changes would not be construed as unfair because this Applicant knowingly filed Applications and took a strong position in defense of its desire to control sensitive IP-focused strings for its sole benefit. Such position was made knowingly and defended at great cost to others. It would not be "unfair" to deny the requested changes or require re-evaluation or submission in a future round. Moreover, merely allowing this Applicant to "fix" its defective Applications is unfair to others who are not able to fix or improve their Applications.

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? Answer: YES – Per Part 2 of these Comments such changes are indisputably material.

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.) Answer: YES

APPLICATION COMMENT DETAILS

Comment ID: 53-vavb4

Name: Constantine Roussos

Affiliation: .MUSIC (DotMusic Limited)

Applicant: Amazon EU S.à r.l.

String: MUSIC

Application ID: 1-1316-18029

Panel/Objection Ground: Community Objection Ground

Subject: Objection to Approved Change Request 2/4

Comment Submission Date: 26 May 2014 at 19:23:40 UTC

Comment:

Amazon EU S.à.r.l.'s changes are a wholesale deletion and addition of key language across all of its Applications for sensitive IP related strings. Applicant has submitted "Material Changes" that may negatively impact the public and other Applicants.

ICANN should not have approved material change requests for Amazon's exclusive access Applications for .MUSIC, .SONG and .TUNES. By approving the change requests ICANN allowed Amazon to make significant material changes to these Applications. Amazon materially altered their mission statement (Question 18) by deleting all exclusive access language. Other changes can be found in: Questions 22, 28, 29, 46, 47, 48, 49, and 50. It should be noted that Questions 28 (Abuse Prevention and Mitigation), 29 (Rights Protection Mechanism), 46 (Projections Template), 47 (Costs and Capital Expenditures), 48 (Funding and Revenue), 49 (Contingency Planning) and 50 (Funding Critical Registry Functions) are scored points. Applicant's massive and sweeping change requests would change its Initial Evaluation scores.

These changes are indisputably "Material" because they represent an intention to dramatically change the Applicant's original position from "exclusive access" to a seemingly more "open" registry. These changes would require a change in Applicant's business plan to account for changes in domain name registration projections and registration policies, a change in registry financials, and the submission of a new LOC to address the proposed changes. Such changes effect both graded and ungraded portions of the Application.

Amazon's changes essentially revolve around deletion of the following objectionable exclusive access language where Applicant originally applied to run each registry to:

"Provide Amazon with additional controls over its technical architecture, offering…"

"Provide Amazon a platform for innovation…"

"Enable Amazon to protect its intellectual property rights…"

Amazon also applied and was graded on its original Applications that unequivably stated that:

"All domains in the [.MUSIC/.SONG/.TUNES] registry will remain the property of Amazon;" and

"[.MUSIC/.SONG/.TUNES] domains may not be delegated or assigned to any third party organizations, institutions, or individuals."

The above-referenced "exclusive access" language positioned Amazon to run sensitive registries for its sole benefit and restrict registration of domain names at its sole discretion. It was Amazon's original desire to control the dissemination of music online through .MUSIC, SONG, and .TUNES. The deletion of this language represents an attempt to make a complete reversal in Applicant's position.

After spending months arguing against such changes, many Community Objectors and others were forced to expend significant resources challenging Amazon's "exclusive access" language, Amazon now quietly seeks to pass through sweeping changes to its Applications. These changes are indisputably "material" and, on their face, represent Applicant's desire to shift position from "exclusive" access to something more "open." GAC Advice, NGPC Resolutions and the .POLO and .MOBILE Expert Determinations prove that "exclusive access language" is material to an Application.

Amazon's changes go to the core of the Applicant's policies. Accordingly, Amazon's change request is material.

APPLICATION COMMENT DETAILS

Make a Comment | View Comments

Comment ID: yzp05x2o

Name: Constantine Roussos

Affiliation: .MUSIC (DotMusic Limited)

Applicant: Amazon EU S.à r.l.

String: MUSIC

Application ID: 1-1316-18029

Panel/Objection Ground: Community Objection Ground

Subject: Objection to Approved Change Request 3/4

Comment Submission Date: 26 May 2014 at 19:18:54 UTC

Comment:

Other third-parties affected – Does the .MUSIC change request approval affect other third parties materially?

Answer:

YES - Such changes affect the public interest, and Community Objectors, who have spent significant time and expense arguing against Applicant's original policies, as well as others in the contention set.

Public Interest:

The referenced "exclusive access" language essentially positioned Amazon to run sensitive registries for its sole benefit and restrict registration of domain names at its sole discretion. It was Amazon's original desire to control these important IP sectors. The deletion of this language represents an attempt to make a complete reversal in Applicant's position. The GAC has articulated the public interest concerns and the sensitive nature of these important IP related strings. Accordingly, any sweeping changes made by Applicant at this stage must be closely scrutinized to determine if, in fact, the public interest is now being met or whether Amazon's changes are insufficient to protect the public.

Because Amazon is not a Community Applicant and it does not hold a trademark for any of the sensitive generic strings its "New Application" should be closely examined. Query whether it is in the public interest to have Amazon controlling all generic strings related to IP (e.g Music) with insufficiently articulated policies and safeguards. It is respectfully submitted that Amazon's purported material changes significantly impacts the public interest and the future of an open Internet.

Community Interest and Community Objectors:

The Music Community has long been concerned about Amazon's lack of appropriate treatment of these sensitive IP strings. Protection of IP rights is central to the Community and both Community Applications for .MUSIC. Moreover, significant resources and costs were spent by Community Objectors in their cases against Amazon's .MUSIC, .SONG, .TUNES, .BOOK, and .MOBILE Applications. In response to the Objections and GAC Advice, Applicant defended the statements presented in its original Applications. Objectors challenged the exact exclusive access language that has been now been deleted.

These material changes (at least in the case of the music themed strings) prove that Amazon mislead Objection Panelists and ICANN with false and misleading information to circumvent the Objection process. Amazon has successfully accomplished circumventing the Objections without any accountability for their new updated changes. Such exclusive language was indeed detrimental and harmful thus vindicating the Objectors' position.

Community Objectors spent hundreds of thousands of dollars seeking to challenge Amazon on this very issue, whether Amazon should be permitted to run an "exclusive access" non-community based registry for sensitive IP strings. Such action by Amazon to remove material language from their .MUSIC, .SONG and .TUNES Applications proves that Amazon was providing misleading and false information to Panelists and highlights the inappropriateness and material harm their Applications posed to the Objectors consistent with the position of the Objectors.

As set forth in Part 4 of the Comments these changes harm other Applicants in the Contention Set as well as other Applicants that have been unable to "fix" update or amend their Applications in response to developments in the new gTLD program.

APPLICATION COMMENT DETAILS

Comment ID: ojuv9nyo

Name: Constantine Roussos

Affiliation: .MUSIC (DotMusic Limited)

Applicant: Amazon EU S.à r.l.

String: MUSIC

Application ID: 1-1316-18029

Panel/Objection Ground: Community Objection Ground

Subject: Objection to Approved Change Request 4/4

Comment Submission Date: 26 May 2014 at 19:13:03 UTC

Comment:

Fairness to applicants – Would allowing the .MUSIC change request be construed as fair to the general community? Would disallowing the change be construed as unfair?

Answer:

All Applicants are bound by the AGB regardless of size, power, or influence. Other Applicants appear to be subject to different standards and have had their change requests rejected. Applicant knowingly filed Applications and took a very strong position in defense of its desire to control key IP related strings for its sole benefit. Such position was made knowingly and defended at great cost but now is treated as an error. It would be "fair" to deny the requested changes or require re-evaluation or submission in a future round. Moreover, allowing this Applicant to "fix" its defective Applications is unfair to others that are not able to fix or improve their Applications.

These material changes were approved despite the preponderance of evidence and knowledge that such deletion of notable exclusive access language would ultimately affect and change scored sections of these Applications, including financial components such as Projections Template (Q.46), Costs and Capital Expenditures (Q.47), Funding and Revenue (Q.48), Contingency Planning (Q.49) and Funding Critical Registry Functions (Q.50).

Allowing such policy-related material changes in an application is unfair to applicants and the general community. If important policy changes are allowed for this Applicant then other Applicants should also be able to request a similar policy changes or updates.

If ICANN agrees to re-evaluate and re-score such material policy changes for Amazon then it should also allow other applicants – such as Community Applicants to do the same if they do not receive a satisfactory CPE score and would like to update their Application to fix

certain sections and ask for a re-evaluation of their Application, including re-scoring their CPE score. Should not other Applicants be able to make wholesale changes to their Applications in response to GAC Advice or other developments in the new gTLD program?

It is clear that the original Applications differ materially with the new Applications and such a change was not made in error. Amazon's conflicting position changes were made to "survive" both Objections processes and GAC Advice and subsequent NGPC Resolutions prohibiting exclusive access language for generic strings.

Notably, 12 applicants responded that the TLD would be operated as an exclusive access registry. 12 Applicants applied for .BROKER, .CRUISE, .DATA, .DVR, .GROCERY, .MOBILE, .PHONE, .STORE, .THEATER, .THEATRE and .TIRES. These Applicants consistently defended their position to keep the exclusive access language in their Applications by providing an explanation of how the proposed exclusive registry access serves a public interest goal without changing their positions or being misleading. The overarching question remains: Why did Amazon change the position they took in their Objection response and original Applications and not defend their Applications with ICANN like these 12 Applicants?

Amazon could have proceeded with its original language but chose to file these change requests. By allowing such changes so late in the process without scrutiny and transparent evaluation ICANN is harming other Applicants and giving Amazon preferential treatment.

APPLICATION COMMENT DETAILS

Comment ID: tl4uv0ai

Name: Constantine Roussos

Affiliation: .MUSIC (DotMusic Limited)

Applicant: Amazon EU S.à r.l.

String: SONG

Application ID: 1-1317-53837

Panel/Objection Ground: Community Objection Ground

Subject: Objection to Approved Change Request 1/4

Comment Submission Date: 26 May 2014 at 19:37:30 UTC

Comment:

Amazon submitted wholesale deletion and addition of key language across all of its sensitive Intellectual Property (IP) related strings (such as music-themed .MUSIC/.SONG/.TUNES). These material changes negatively impact the public and other Applicants.

AGB Section 1.2.7 requires ICANN to balance the following 7 factors in deciding whether to accept the change requests:

1. Explanation – Is a reasonable explanation provided? Answer: It can reasonably be deduced that Amazon's sweeping changes were in response to strong condemnation of Applicant's stated goals to run an exclusive access registry and control critical intellectual property sectors worldwide.

2. Evidence that original submission was in error – Are there indicia to support an assertion that the change merely corrects an error? Answer: NO. There is no "indicia" of error based on Amazon's published defense of its "exclusive access" position in response to Community Objections.

3. Other third parties affected – Does the change affect other third parties materially? Answer: YES - Such changes affect the public, Community Applicants and Objectors, and others in the contention set. Some have spent significant time and expense arguing against Applicant's policies.

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? Answer: These unprecedented massive changes were made without public notice and address Applicant's control of critical IP sectors. Such changes should not be done in secret without debate, evaluation or explanation. Other Applicants have not been permitted to make such sweeping changes. The size of Applicant, the strings

affected and the potential impact on the public warrants further examination.

5. Fairness to applicants – Would allowing the change be construed as fair to the general community? Would disallowing the change be construed as unfair? Answer: All Applicants are bound by the AGB regardless of size, power or influence. Other Applicants appear to be subject to different standards and have had their change requests rejected. Such a massive set of changes for a single powerful applicant without transparency is unfair. Disallowing the changes would not be construed as unfair because this Applicant knowingly filed Applications and took a strong position in defense of its desire to control sensitive IP-focused strings for its sole benefit. Such position was made knowingly and defended at great cost to others. It would not be "unfair" to deny the requested changes or require re-evaluation or submission in a future round. Moreover, merely allowing this Applicant to "fix" its defective Applications is unfair to others who are not able to fix or improve their Applications.

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? Answer: YES – Per Part 2 of these Comments such changes are indisputably material.

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.) Answer: YES

APPLICATION COMMENT DETAILS

Make a Comment View Comments

Comment ID: zuazqs8f

Name: Constantine Roussos

Affiliation: .MUSIC (DotMusic Limited)

Applicant: Amazon EU S.à r.l.

String: SONG

Application ID: 1-1317-53837

Panel/Objection Ground: Community Objection Ground

Subject: Objection to Approved Change Request 2/4

Comment Submission Date: 26 May 2014 at 19:36:21 UTC

Comment:

Amazon EU S.à.r.l.'s changes are a wholesale deletion and addition of key language across all of its Applications for sensitive IP related strings. Applicant has submitted "Material Changes" that may negatively impact the public and other Applicants.

ICANN should not have approved material change requests for Amazon's exclusive access Applications for .MUSIC, .SONG and .TUNES. By approving the change requests ICANN allowed Amazon to make significant material changes to these Applications. Amazon materially altered their mission statement (Question 18) by deleting all exclusive access language. Other changes can be found in: Questions 22, 28, 29, 46, 47, 48, 49, and 50. It should be noted that Questions 28 (Abuse Prevention and Mitigation), 29 (Rights Protection Mechanism), 46 (Projections Template), 47 (Costs and Capital Expenditures), 48 (Funding and Revenue), 49 (Contingency Planning) and 50 (Funding Critical Registry Functions) are scored points. Applicant's massive and sweeping change requests would change its Initial Evaluation scores.

These changes are indisputably "Material" because they represent an intention to dramatically change the Applicant's original position from "exclusive access" to a seemingly more "open" registry. These changes would require a change in Applicant's business plan to account for changes in domain name registration projections and registration policies, a change in registry financials, and the submission of a new LOC to address the proposed changes. Such changes effect both graded and ungraded portions of the Application.

Amazon's changes essentially revolve around deletion of the following objectionable exclusive access language where Applicant originally applied to run each registry to:

"Provide Amazon with additional controls over its technical architecture, offering…"

"Provide Amazon a platform for innovation…"

"Enable Amazon to protect its intellectual property rights…"

Amazon also applied and was graded on its original Applications that unequivably stated that:

"All domains in the [.MUSIC/.SONG/.TUNES] registry will remain the property of Amazon;" and

"[.MUSIC/.SONG/.TUNES] domains may not be delegated or assigned to any third party organizations, institutions, or individuals."

The above-referenced "exclusive access" language positioned Amazon to run sensitive registries for its sole benefit and restrict registration of domain names at its sole discretion. It was Amazon's original desire to control the dissemination of music online through .MUSIC, SONG, and .TUNES. The deletion of this language represents an attempt to make a complete reversal in Applicant's position.

After spending months arguing against such changes, many Community Objectors and others were forced to expend significant resources challenging Amazon's "exclusive access" language, Amazon now quietly seeks to pass through sweeping changes to its Applications. These changes are indisputably "material" and, on their face, represent Applicant's desire to shift position from "exclusive" access to something more "open." GAC Advice, NGPC Resolutions and the .POLO and .MOBILE Expert Determinations prove that "exclusive access language" is material to an Application.

Amazon's changes go to the core of the Applicant's policies. Accordingly, Amazon's change request is material.

APPLICATION COMMENT DETAILS

Make a Comment | View Comments

Comment ID: dh5f72fz

Name: Constantine Roussos

Affiliation: .MUSIC (DotMusic Limited)

Applicant: Amazon EU S.à r.l.

String: SONG

Application ID: 1-1317-53837

Panel/Objection Ground: Community Objection Ground

Subject: Objection to Approved Change Request 3/4

Comment Submission Date: 26 May 2014 at 19:35:00 UTC

Comment:

Other third-parties affected – Does the .SONG change request approval affect other third parties materially?

Answer:

YES - Such changes affect the public interest, and Community Objectors, who have spent significant time and expense arguing against Applicant's original policies, as well as others in the contention set.

Public Interest:

The referenced "exclusive access" language essentially positioned Amazon to run sensitive registries for its sole benefit and restrict registration of domain names at its sole discretion. It was Amazon's original desire to control these important IP sectors. The deletion of this language represents an attempt to make a complete reversal in Applicant's position. The GAC has articulated the public interest concerns and the sensitive nature of these important IP related strings. Accordingly, any sweeping changes made by Applicant at this stage must be closely scrutinized to determine if, in fact, the public interest is now being met or whether Amazon's changes are insufficient to protect the public.

Because Amazon is not a Community Applicant and it does not hold a trademark for any of the sensitive generic strings its "New Application" should be closely examined. Query whether it is in the public interest to have Amazon controlling all generic strings related to IP (e.g Music) with insufficiently articulated policies and safeguards. It is respectfully submitted that Amazon's purported material changes significantly impacts the public interest and the future of an open Internet.

Community Interest and Community Objectors:

The Music Community has long been concerned about Amazon's lack of appropriate treatment of these sensitive IP strings. Protection of IP rights is central to the Community and both Community Applications for .MUSIC. Moreover, significant resources and costs were spent by Community Objectors in their cases against Amazon's .MUSIC, .SONG, .TUNES, .BOOK, and .MOBILE Applications. In response to the Objections and GAC Advice, Applicant defended the statements presented in its original Applications. Objectors challenged the exact exclusive access language that has been now been deleted.

These material changes (at least in the case of the music themed strings) prove that Amazon mislead Objection Panelists and ICANN with false and misleading information to circumvent the Objection process. Amazon has successfully accomplished circumventing the Objections without any accountability for their new updated changes. Such exclusive language was indeed detrimental and harmful thus vindicating the Objectors' position.

Community Objectors spent hundreds of thousands of dollars seeking to challenge Amazon on this very issue, whether Amazon should be permitted to run an "exclusive access" non-community based registry for sensitive IP strings. Such action by Amazon to remove material language from their .MUSIC, .SONG and .TUNES Applications proves that Amazon was providing misleading and false information to Panelists and highlights the inappropriateness and material harm their Applications posed to the Objectors consistent with the position of the Objectors.

As set forth in Part 4 of the Comments these changes harm other Applicants in the Contention Set as well as other Applicants that have been unable to "fix" update or amend their Applications in response to developments in the new gTLD program.

APPLICATION COMMENT DETAILS

Comment ID: e2a1w6hd

Name: Constantine Roussos

Affiliation: .MUSIC (DotMusic Limited)

Applicant: Amazon EU S.à r.l.

String: SONG

Application ID: 1-1317-53837

Panel/Objection Ground: Community Objection Ground

Subject: Objection to Approved Change Request 4/4

Comment Submission Date: 26 May 2014 at 19:33:23 UTC

Comment:

Fairness to applicants – Would allowing the .SONG change request be construed as fair to the general community? Would disallowing the change be construed as unfair?

Answer:

All Applicants are bound by the AGB regardless of size, power, or influence. Other Applicants appear to be subject to different standards and have had their change requests rejected. Applicant knowingly filed Applications and took a very strong position in defense of its desire to control key IP related strings for its sole benefit. Such position was made knowingly and defended at great cost but now is treated as an error. It would be "fair" to deny the requested changes or require re-evaluation or submission in a future round. Moreover, allowing this Applicant to "fix" its defective Applications is unfair to others that are not able to fix or improve their Applications.

These material changes were approved despite the preponderance of evidence and knowledge that such deletion of notable exclusive access language would ultimately affect and change scored sections of these Applications, including financial components such as Projections Template (Q.46), Costs and Capital Expenditures (Q.47), Funding and Revenue (Q.48), Contingency Planning (Q.49) and Funding Critical Registry Functions (Q.50).

Allowing such policy-related material changes in an application is unfair to applicants and the general community. If important policy changes are allowed for this Applicant then other Applicants should also be able to request a similar policy changes or updates.

If ICANN agrees to re-evaluate and re-score such material policy changes for Amazon then it should also allow other applicants – such as Community Applicants to do the same if they do not receive a satisfactory CPE score and would like to update their Application to fix

certain sections and ask for a re-evaluation of their Application, including re-scoring their CPE score. Should not other Applicants be able to make wholesale changes to their Applications in response to GAC Advice or other developments in the new gTLD program?

It is clear that the original Applications differ materially with the new Applications and such a change was not made in error. Amazon's conflicting position changes were made to "survive" both Objections processes and GAC Advice and subsequent NGPC Resolutions prohibiting exclusive access language for generic strings.

Notably, 12 applicants responded that the TLD would be operated as an exclusive access registry. 12 Applicants applied for .BROKER, .CRUISE, .DATA, .DVR, .GROCERY, .MOBILE, .PHONE, .STORE, .THEATER, .THEATRE and .TIRES. These Applicants consistently defended their position to keep the exclusive access language in their Applications by providing an explanation of how the proposed exclusive registry access serves a public interest goal without changing their positions or being misleading. The overarching question remains: Why did Amazon change the position they took in their Objection response and original Applications and not defend their Applications with ICANN like these 12 Applicants?

Amazon could have proceeded with its original language but chose to file these change requests. By allowing such changes so late in the process without scrutiny and transparent evaluation ICANN is harming other Applicants and giving Amazon preferential treatment.

APPLICATION COMMENT DETAILS

Make a Comment View Comments

Comment ID: f0dzs9ay

Name: Constantine Roussos

Affiliation: .MUSIC (DotMusic Limited)

Applicant: Amazon EU S.à r.l.

String: TUNES

Application ID: 1-1317-30761

Panel/Objection Ground: Community Objection Ground

Subject: Objection to Approved Change Request 1/4

Comment Submission Date: 26 May 2014 at 19:42:55 UTC

Comment:

Amazon submitted wholesale deletion and addition of key language across all of its sensitive Intellectual Property (IP) related strings (such as music-themed .MUSIC/.SONG/.TUNES). These material changes negatively impact the public and other Applicants.

AGB Section 1.2.7 requires ICANN to balance the following 7 factors in deciding whether to accept the change requests:

1. Explanation – Is a reasonable explanation provided? Answer: It can reasonably be deduced that Amazon's sweeping changes were in response to strong condemnation of Applicant's stated goals to run an exclusive access registry and control critical intellectual property sectors worldwide.

2. Evidence that original submission was in error – Are there indicia to support an assertion that the change merely corrects an error? Answer: NO. There is no "indicia" of error based on Amazon's published defense of its "exclusive access" position in response to Community Objections.

3. Other third parties affected – Does the change affect other third parties materially? Answer: YES - Such changes affect the public, Community Applicants and Objectors, and others in the contention set. Some have spent significant time and expense arguing against Applicant's policies.

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? Answer: These unprecedented massive changes were made without public notice and address Applicant's control of critical IP sectors. Such changes should not be done in secret without debate, evaluation or explanation. Other Applicants have not been permitted to make such sweeping changes. The size of Applicant, the strings

affected and the potential impact on the public warrants further examination.

5. Fairness to applicants – Would allowing the change be construed as fair to the general community? Would disallowing the change be construed as unfair? Answer: All Applicants are bound by the AGB regardless of size, power or influence. Other Applicants appear to be subject to different standards and have had their change requests rejected. Such a massive set of changes for a single powerful applicant without transparency is unfair. Disallowing the changes would not be construed as unfair because this Applicant knowingly filed Applications and took a strong position in defense of its desire to control sensitive IP-focused strings for its sole benefit. Such position was made knowingly and defended at great cost to others. It would not be "unfair" to deny the requested changes or require re-evaluation or submission in a future round. Moreover, merely allowing this Applicant to "fix" its defective Applications is unfair to others who are not able to fix or improve their Applications.

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? Answer: YES – Per Part 2 of these Comments such changes are indisputably material.

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) Answer: YES

APPLICATION COMMENT DETAILS

Comment ID: g9ry7urc

Name: Constantine Roussos

Affiliation: .MUSIC (DotMusic Limited)

Applicant: Amazon EU S.à r.l.

String: TUNES

Application ID: 1-1317-30761

Panel/Objection Ground: Community Objection Ground

Subject: Objection to Approved Change Request 2/4

Comment Submission Date: 26 May 2014 at 19:41:27 UTC

Comment:

Amazon EU S.à.r.l.'s changes are a wholesale deletion and addition of key language across all of its Applications for sensitive IP related strings. Applicant has submitted "Material Changes" that may negatively impact the public and other Applicants.

ICANN should not have approved material change requests for Amazon's exclusive access Applications for .MUSIC, .SONG and .TUNES. By approving the change requests ICANN allowed Amazon to make significant material changes to these Applications. Amazon materially altered their mission statement (Question 18) by deleting all exclusive access language. Other changes can be found in: Questions 22, 28, 29, 46, 47, 48, 49, and 50. It should be noted that Questions 28 (Abuse Prevention and Mitigation), 29 (Rights Protection Mechanism), 46 (Projections Template), 47 (Costs and Capital Expenditures), 48 (Funding and Revenue), 49 (Contingency Planning) and 50 (Funding Critical Registry Functions) are scored points. Applicant's massive and sweeping change requests would change its Initial Evaluation scores.

These changes are indisputably "Material" because they represent an intention to dramatically change the Applicant's original position from "exclusive access" to a seemingly more "open" registry. These changes would require a change in Applicant's business plan to account for changes in domain name registration projections and registration policies, a change in registry financials, and the submission of a new LOC to address the proposed changes. Such changes effect both graded and ungraded portions of the Application.

Amazon's changes essentially revolve around deletion of the following objectionable exclusive access language where Applicant originally applied to run each registry to:

"Provide Amazon with additional controls over its technical architecture, offering…"

"Provide Amazon a platform for innovation…"

"Enable Amazon to protect its intellectual property rights…"

Amazon also applied and was graded on its original Applications that unequivably stated that:

"All domains in the [.MUSIC/.SONG/.TUNES] registry will remain the property of Amazon;" and

"[.MUSIC/.SONG/.TUNES] domains may not be delegated or assigned to any third party organizations, institutions, or individuals."

The above-referenced "exclusive access" language positioned Amazon to run sensitive registries for its sole benefit and restrict registration of domain names at its sole discretion. It was Amazon's original desire to control the dissemination of music online through .MUSIC, SONG, and .TUNES. The deletion of this language represents an attempt to make a complete reversal in Applicant's position.

After spending months arguing against such changes, many Community Objectors and others were forced to expend significant resources challenging Amazon's "exclusive access" language, Amazon now quietly seeks to pass through sweeping changes to its Applications. These changes are indisputably "material" and, on their face, represent Applicant's desire to shift position from "exclusive" access to something more "open." GAC Advice, NGPC Resolutions and the .POLO and .MOBILE Expert Determinations prove that "exclusive access language" is material to an Application.

Amazon's changes go to the core of the Applicant's policies. Accordingly, Amazon's change request is material.

APPLICATION COMMENT DETAILS

Make a Comment | View Comments

Comment ID: amukn5c6

Name: Constantine Roussos

Affiliation: .MUSIC (DotMusic Limited)

Applicant: Amazon EU S.à r.l.

String: TUNES

Application ID: 1-1317-30761

Panel/Objection Ground: Community Objection Ground

Subject: Objection to Approved Change Request 3/4

Comment Submission Date: 26 May 2014 at 19:40:41 UTC

Comment:

Other third-parties affected – Does the .TUNES change request approval affect other third parties materially?

Answer:

YES - Such changes affect the public interest, and Community Objectors, who have spent significant time and expense arguing against Applicant's original policies, as well as others in the contention set.

Public Interest:

The referenced "exclusive access" language essentially positioned Amazon to run sensitive registries for its sole benefit and restrict registration of domain names at its sole discretion. It was Amazon's original desire to control these important IP sectors. The deletion of this language represents an attempt to make a complete reversal in Applicant's position. The GAC has articulated the public interest concerns and the sensitive nature of these important IP related strings. Accordingly, any sweeping changes made by Applicant at this stage must be closely scrutinized to determine if, in fact, the public interest is now being met or whether Amazon's changes are insufficient to protect the public.

Because Amazon is not a Community Applicant and it does not hold a trademark for any of the sensitive generic strings its "New Application" should be closely examined. Query whether it is in the public interest to have Amazon controlling all generic strings related to IP (e.g Music) with insufficiently articulated policies and safeguards. It is respectfully submitted that Amazon's purported material changes significantly impacts the public interest and the future of an open Internet.

Community Interest and Community Objectors:

The Music Community has long been concerned about Amazon's lack of appropriate treatment of these sensitive IP strings. Protection of IP rights is central to the Community and both Community Applications for .MUSIC. Moreover, significant resources and costs were spent by Community Objectors in their cases against Amazon's .MUSIC, .SONG, .TUNES, .BOOK, and .MOBILE Applications. In response to the Objections and GAC Advice, Applicant defended the statements presented in its original Applications. Objectors challenged the exact exclusive access language that has been now been deleted.

These material changes (at least in the case of the music themed strings) prove that Amazon mislead Objection Panelists and ICANN with false and misleading information to circumvent the Objection process. Amazon has successfully accomplished circumventing the Objections without any accountability for their new updated changes. Such exclusive language was indeed detrimental and harmful thus vindicating the Objectors' position.

Community Objectors spent hundreds of thousands of dollars seeking to challenge Amazon on this very issue, whether Amazon should be permitted to run an "exclusive access" non-community based registry for sensitive IP strings. Such action by Amazon to remove material language from their .MUSIC, .SONG and .TUNES Applications proves that Amazon was providing misleading and false information to Panelists and highlights the inappropriateness and material harm their Applications posed to the Objectors consistent with the position of the Objectors.

As set forth in Part 4 of the Comments these changes harm other Applicants in the Contention Set as well as other Applicants that have been unable to "fix" update or amend their Applications in response to developments in the new gTLD program.

APPLICATION COMMENT DETAILS

Comment ID: bpbspwym

Name: Constantine Roussos

Affiliation: .MUSIC (DotMusic Limited)

Applicant: Amazon EU S.à r.l.

String: TUNES

Application ID: 1-1317-30761

Panel/Objection Ground: Community Objection Ground

Subject: Objection to Approved Change Request 4/4

Comment Submission Date: 26 May 2014 at 19:39:11 UTC

Comment:

Fairness to applicants – Would allowing the .TUNES change request be construed as fair to the general community? Would disallowing the change be construed as unfair?

Answer:

All Applicants are bound by the AGB regardless of size, power, or influence. Other Applicants appear to be subject to different standards and have had their change requests rejected. Applicant knowingly filed Applications and took a very strong position in defense of its desire to control key IP related strings for its sole benefit. Such position was made knowingly and defended at great cost but now is treated as an error. It would be "fair" to deny the requested changes or require re-evaluation or submission in a future round. Moreover, allowing this Applicant to "fix" its defective Applications is unfair to others that are not able to fix or improve their Applications.

These material changes were approved despite the preponderance of evidence and knowledge that such deletion of notable exclusive access language would ultimately affect and change scored sections of these Applications, including financial components such as Projections Template (Q.46), Costs and Capital Expenditures (Q.47), Funding and Revenue (Q.48), Contingency Planning (Q.49) and Funding Critical Registry Functions (Q.50).

Allowing such policy-related material changes in an application is unfair to applicants and the general community. If important policy changes are allowed for this Applicant then other Applicants should also be able to request a similar policy changes or updates.

If ICANN agrees to re-evaluate and re-score such material policy changes for Amazon then it should also allow other applicants – such as Community Applicants to do the same if they do not receive a satisfactory CPE score and would like to update their Application to fix

certain sections and ask for a re-evaluation of their Application, including re-scoring their CPE score. Should not other Applicants be able to make wholesale changes to their Applications in response to GAC Advice or other developments in the new gTLD program?

It is clear that the original Applications differ materially with the new Applications and such a change was not made in error. Amazon's conflicting position changes were made to "survive" both Objections processes and GAC Advice and subsequent NGPC Resolutions prohibiting exclusive access language for generic strings.

Notably, 12 applicants responded that the TLD would be operated as an exclusive access registry. 12 Applicants applied for .BROKER, .CRUISE, .DATA, .DVR, .GROCERY, .MOBILE, .PHONE, .STORE, .THEATER, .THEATRE and .TIRES. These Applicants consistently defended their position to keep the exclusive access language in their Applications by providing an explanation of how the proposed exclusive registry access serves a public interest goal without changing their positions or being misleading. The overarching question remains: Why did Amazon change the position they took in their Objection response and original Applications and not defend their Applications with ICANN like these 12 Applicants?

Amazon could have proceeded with its original language but chose to file these change requests. By allowing such changes so late in the process without scrutiny and transparent evaluation ICANN is harming other Applicants and giving Amazon preferential treatment.