EXHIBIT JJN-1

New gTLD Application Submitted to ICANN by: NU DOT CO LLC

String: WEB

Originally Posted: 13 June 2012

Application ID: 1-1296-36138

Applicant Information

1. Full legal name

NU DOT CO LLC

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact Information Redacted

4. Fax number

Contact Information Redacted

5. If applicable, website or URL

Primary Contact

6(a). Name

Jose Ignacio Rasco

6(b). Title

Manager

6(c). Address

6(d). Phone Number

Contact Information Redacted

6(e). Fax Number

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Mr. Nicolai Bezsonoff

7(b). Title

Manager

7(c). Address

7(d). Phone Number

Contact Information Redacted

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Limited liability company

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

NU DOTCO LLC is a UNITED STATES entity, registered in the STATE of DELAWARE as a limited liability company.

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

Attachments are not displayed on this form.

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

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

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

Applicant Background

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

Jose Ignacio Rasco III	Manager
Juan Diego Calle	Manager
Nicolai Bezsonoff	Manager

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

Jose Ignacio Rasco III	CFO
Juan Diego Calle	CEO
Nicolai Bezsonoff	COO

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

Domain Marketing Holdings, LLC	Not Applicable
NUCO LP, LLC	Not Applicable

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

Applied-for gTLD string

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

WEB

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

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

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

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

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

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

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

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

Attachments are not displayed on this form.

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

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

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

NU DOTCO, LLC (“NU.CO”) foresees no known rendering issues in connection with the proposed .LAW TLD which it is seeking to apply for as a gTLD. This answer is based upon consultation with NU.CO’s backend provider, Neustar, which has successfully launched a number of new gTLDs over the last decade. In reaching this determination, the following data points were analyzed:

- ICANN's Security Stability Advisory Committee (SSAC) entitled Alternative TLD Name Systems and Roots: Conflict, Control and Consequences (SAC009);
- IAB - RFC3696 "Application Techniques for Checking and Transformation of Names"
- Known software issues which Neustar has encountered during the last decade launching new gTLDs;
- Character type and length;
- ICANN supplemental notes to Question 16; and
- ICANN's presentation during its Costa Rica regional meeting on TLD Universal Acceptance;

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

Mission/Purpose

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

18.1 Mission/purpose of .WEB
The mission of .WEB is to provide the internet community at-large with an alternative "home domain" for their online presence. We envision that through strategic marketing campaigns designed to brand the domain, it will become a premium online namespace for a variety of businesses and websites. This general domain will provide new registrants with better, more relevant alternatives to the limited options remaining for current commercial TLD names.

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

18.2 How will .WEB benefit registrants, Internet users, and others?
.WEB seeks to offer registrants and the broader internet community, with a reliable, trusted, and secure top level domain (TLD). Congestion in the current availability of commercial TLD names fundamentally advantages older incumbent players. Providing access to additional high-value second level domain names (i.e. shorter and more memorable) will provide an opportunity for new entrants to compete effectively for internet users' finite attention. The domain's coherent and consistent branding will assist registrants in developing meaningful emotional connection with users, allowing them to further differentiate themselves as premium destinations. These marketing efforts along with the initial adoption of key industry players, should reinforce the implicit attribution of "cutting-edge" and "innovativeness" upon its registrants. Prospective users benefit from the long-term commitment of a proven executive team that has a track-record of building and successfully marketing affinity TLD's (e.g., .CO targeting innovative businesses and entrepreneurs).

The demand for having an online presence continues to grow worldwide, especially as more people and businesses become active internet users, enjoying the increases in productivity and promotional effectiveness that the internet offers. A clear example of this is the number of worldwide internet users, which has grown at an average18% annual rate over the past decade, and domain registrations which have experienced similar adoption rates having grown from approximately 25mm in 2000 to over 225mm today.

In particular for small businesses and entrepreneurs, the Internet offers an incredibly useful way to promote themselves to a wider audience, both locally and globally. Moreover, it allows them to cost-effective offer their products and services directly to consumers, leveling the playing field with larger and more established competitors. A number of new and innovative business models have been established that were not possible prior to the Internet, creating substantial value for society.

However, until a few years ago it was difficult and costly for individuals and small businesses to establish an internet presence. This has changed as prices decreased dramatically and offerings became more accessible and intuitive. This is the result of having many retailers (i.e. registrars or resellers) that compete amongst each other on price, along with product and service differentiation. Differentiation has mainly centered around higher value-add services ancillary to the domain registration itself, such as hosting, web-site builders, SSL, e-mail, etc. The basic product (a domain) has not changed much, and until now, there have been few feasible alternatives to the commercial TLDs. The proposed new TLDs will provide users with more relevant and customized options. Just as ICANN opened up the market for the distribution and registration of domains and created the Registrar industry, which ultimately benefitted hundreds of millions of people and businesses worldwide, we expect that the introduction of new TLDs will yield similar benefits.

The experienced team behind this application initially launched and currently operates the .CO ccTLD. The intention is for .WEB to be added to .CO's product portfolio, where it can benefit from economies of scale along with the firm's experience and expertise in marketing and branding TLD properties. Their successful track record proves that properly branded affinity domains can help sites form deeper emotional connections with their users, providing significant value-add. The .CO re-launch is a great illustration of how a new option in TLDs can address the unmet needs an affinity group (e.g., small businesses and start-ups), and we continue to firmly believe that the new .WEB domain will provide better, more relevant solutions for registrants .

Since its launch, .CO's marketing has primarily focused on developing a worldwide ecosystem of innovative small businesses and entrepreneurs. To date, the .CO registry, .CO Internet S.A.S, has reached close to 1.3 million domains under management, with more than one million individual new Registrations in the first year alone and a renewal rate for domains purchased during launch of nearly 70% and a current average renewal rate of 65%. The renewal rate is one of the highest amongst the industry and especially high considering it has not yet reached the multiple year expiration dates, where it's expected to climb even higher. In addition, .CO has become the standard secondary option to .COM for the leading global registrars, having the most conversions when presented with a non-.COM option. Further, .CO has secured a strong position with the tech startup community by securing such high profile users as Twitter (t.co), Google (g.co), tech influencers like Angel list (angel.co) and 500 Startups (500.co), and entrepreneurship organizations like Startup America (s.co).

.CO has differentiated itself from other existing TLDs by combining innovative branding with the highest standards in trademark protection, unprecedented marketing campaigns, and pro-active security monitoring. We plan to implement a very similar strategy for .WEB in its launch, operation, promotion and growth.

We plan to target a similar community of entrepreneurs, startups, and progressive corporate entities that are looking for an online presence with a suitable domain name. We anticipate the addressable community will continue to grow as traditional businesses choose to launch an online presence for their pre-existing operations and as entrepreneurs launch new start-ups. The domain's marketing strategy will utilize a 3 pillar framework, similar to that used with .CO:

- Awareness: We plan to launch marketing campaigns to both the small businesses and entrepreneurs promoting .WEB via a combination of:
o Media placements online and offline
o Social media campaigns
o Events
o Sponsorships
o Endorsements
o PR efforts
o Direct marketing
o Channel marketing

- Usage: We plan to foster the community of users of .WEB via a combination community engagement and outreach, use-case development and direct marketing to base.

- Distribution: The distribution will be done through the existing ICANN accredited registrar channel and will include marketing at the point of sale, packages and bundles, campaigns, etc.

The marketing plans will evolve depending on market conditions, but using .CO as an example, we implemented an awareness and branding strategy that included the creation of a brand identity and logo; mass media placements including 2 super-bowl commercials with one of our partners plus many TV

placements; billboards and other outdoors campaigns; several online media campaigns including networks, re-targeting and videos; ongoing Twitter, Facebook engagements; sponsorship and presence in a variety of events for TMs (INTA), Tech startups (SxSW, Web 2.0, Internetweek, etc.), Startups (Task Rabbit TR.co), Community (ICANN, LACTLD, etc.), etc. We also implemented for .CO a strong usage promotion of the domain by creating and fostering a community of .CO users and case studies. We achieved this through a combination of events, sponsorships, and partnerships with different entities like Angel.co, 500.co, Startup America (s.co), founders institute (fi.co), etc. We also cultivated many case studies of successful .CO users, remaining in close contact with them. Finally, we implemented a rigorous channel marketing and sales plan that included marketing placements at the point of purchase plus co-marketing and community outreach.

While we do plan to follow a similar strategy to achieve widespread awareness, usage and distribution, the budget and actual placements for promoting .WEB will be scaled down accordingly, as neither its volume of registrations or revenues is expected to be in line with that of .CO.

By launching the .WEB domain we expect to provide more descriptive/ relevant options for end-users, including access to desirable second level domain names which are unavailable or occupied by current general TLD's. As illustrated with .CO, the rapid growth to 1.3 million domains is evidence of pent up demand in the marketplace for good, descriptive domain names. We expect that our marketing strategies will result in a new branded and available option that will emotionally connect with potential users and allow them to differentiate themselves through the use of a branded premium domain.

We will also follow the same ICANN rules and distribution methods of major gTLDs thereby ensuring Registrars and Resellers do not have to change their systems to distribute the .WEB domain. As our systems are already integrated with largest registrars in the world and we have implemented industry best practices, the transition to delegation and launch should be seamless to the registrar channel as well as consumers.

We will also implement a thick whois and adopt any ICANN recommendations or requirements in the future. In order to protect the privacy of our users, we will allow the use of Privacy or Proxy registrations by reputable registrars that comply with applicable policies specified by ICANN. We find this service is highly valuable for registrants that want to ensure their information is not available online and would like to maintain a higher level privacy.

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

18.3 .WEB operating rules to benefit consumers
We plan to follow all ICANN policies, including the best practices and recommendations for gTLDs. This will allow us to ensure end-users, have an easy way to register/purchase, administer, and use their domains. Adopting these policies will also prevent malicious behavior by third parties and ensure a smooth operation of the domain. The plans for the launch will be similar to the launch process used in .CO, which included:

- Gradual Offering Plan: The .CO launch included a very comprehensive gradual opening plan that both protected trademarks and provided transparency to end users. The launch was lauded by ICANN for its comprehensiveness and management. For the launch of .WEB we will follow ICANN's policies especially as it relates to the Trademark Clearinghouse which was similar to the process we used for .CO:
-
o Sunrise: Provide a period of a few weeks to allow the TM and IP community to register their .WEB domains prior to the opening to the public. Trademark validations will be done by the Trademark Clearinghouse or as specified by ICANN in their policies. If there are multiple validated applications, these would go to auction and allocated based on these results.
o Landrush: Provide a period of a few weeks to allow domain investors and others that are interested in premium domains to apply for these domains. Once the period of the Landrush phase is over, a process to check the applications will determine if these were unique or if there were multiple applicants. If single applicants, then the domain is awarded at that time. If multiple applicants then the domain would go to an auction in which all applicants would be able to participate. For .CO this process included close to 30,000 applications and the resulting auctions were managed by Pool.com. The process was very successful managing to allocate very efficiently domains according to their perceived value by applicants and bidders at the resulting auctions.

- General Availability: For .CO we had 100k registrations in the first 10 minutes and we didn’t have a single issue nor service degradation through the launch or afterwards. We achieved this through a combination of strong planning between our partners, especially Neustar our back-end provider; communication with our Registrars prior and during the launch in a very structured way; strong infrastructure planning and provisioning; and effective load, contingency, and disaster recovery planning. We plan to use similar methods for the launch of .WEB.
o First come first serve during GA and afterwards, which we believe is the best mechanism to ensure a fair allocation of domains once the domain has been launched.
o Use of UDRP and any other best-practices in rights protection mechanisms
o Highly managed General Availability launch
- Premium Domains: We will keep some domains for premium sales and these will be restricted prior to the Gradual Offering Plan begins, but can be applied for during the Sunrise phase. These premium domains will be brokered or sold via auction directly or through an accredited 3rd party. With .CO we used this mechanism as a way to allocate high value domains and also to promote the usage of the domain by high profile companies including Twitter with t.co, Google with g.co, Startup America with s.co, as well as a myriad of smaller startups and other endorsements.

Community-based Designation

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

No

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

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

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

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

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

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

Attachments are not displayed on this form.

Geographic Names

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

No

Protection of Geographic Names

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

In preparation for answering this question, NU DOTCO, LLC (NU.CO) reviewed the following relevant background material regarding the protection of geographic names in the DNS, including:

- ICANN Board Resolution 01-92 regarding the methodology developed for the reservation and release of country names in the .INFO top-level domain (see http://www.icann.org/en/minutes/minutes-10sep01.htm);

- ICANN's Proposed Action Plan on .INFO Country Names (see http://www.icann.org/en/meetings/montevideo/action-plan-country-names-09oct01.htm);

- "Report of the Second WIPO Internet Domain Name Process: The Recognition and Rights and the Use of Names in the Internet Domain Name System," Section 6, Geographical Identifiers (see http://www.wipo.int/amc/en/processes/process²/report/html/report.html);

- ICANN's Governmental Advisory Committee (GAC) Principles Regarding New gTLDs, (see https://gacweb.icann.org/download/attachments/₁₅₄₀₁₂₈/gTLD_principles_0.pdf?version=1&modificationDate=1312358178000); and

- ICANN's Generic Names Supporting Organization (GNSO) Reserved Names Working Group – Final Report (see http://gnso.icann.org/issues/new-gtlds/final-report-rn-wg-23may07.htm).

Initial Reservation of Country and Territory Names

NU.CO is committed to initially reserving the country and territory names contained in the internationally recognized lists described in Article 5 of Specification 5 attached to the New gTLD Applicant Guidebook at the second level and at all other levels within the .WEB gTLD at which domain name registrations will be provided. Specifically, NU.CO will reserve:

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

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

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

Potential Future Release of Two Character Names

While NU.CO foresees no immediate need for plans to make use of these initially reserved country names at the second level within the .WEB namespace, NU.CO recognizes that there has been several successful and non-misleading use of country names by new gTLD operators as evidenced below:

AUSTRALIA.COOP – Is operated by Co-operatives Australia the national body for State Co-operative Federations and provides a valuable resource about cooperatives within Australia.

UK.COOP – Is operated by Co-operatives UK the national trade body that campaigns for co-operation and works to promote, develop and unite co-operative enterprises within the United Kingdom.

NZ.COOP – Is operated by the New Zealand Cooperatives Association which brings together the country's cooperative mutual business in a not-for-profit incorporated society.

USA.JOBS - Is operated by DirectEmployers Association (DE). While Employ Media the registry operator of the .JOBS gTLD is currently in a dispute with ICANN regarding the allocation of this and other domain names. Direct Employers has a series of partnerships and programs with the United States Department of Labor, the National Association of State Workforce Agencies and Facebook to help unemployed workers find jobs.

MALDIVIAN.AERO - Is the dominant domestic air carrier in Maldives, and provides a range of commercial and leisure air transport services.

The more likely request by NU.CO will come in connection with the un-reservation and allocation of two-letter .WEB domain names, e.g. US.WEB, UK.WEB, etc. If NU.CO should decide in the future to attempt and allocate these domain names, it would submit the proper Registry Service Evaluation Processes (RSEP) with ICANN. In evaluating similar RSEP requests that have been submitted to ICANN by other gTLD registry operators, NU.CO believes that its request would be favorably granted.

Creation and Updating the Policies

NU.CO is committed to continually reviewing and updating when necessary its policies in this area. Consistent with this commitment, NU.CO intends to remain an active participant in any ongoing ICANN policy discussion regarding the protection of geographic names within the DNS.

Registry Services

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

23.1 Introduction

NU DOTCO LLC has elected to partner with NeuStar, Inc ("Neustar") to provide back-end services for the .WEB registry. In making this decision, NU DOTCO LLC recognized that Neustar already possesses a production-proven registry system that can be quickly deployed and smoothly operated over its robust, flexible, and scalable world-class infrastructure. The existing registry services will be leveraged for the .WEB registry. The following section describes the registry services to be provided.

23.2 Standard Technical and Business Components

Neustar will provide the highest level of service while delivering a secure, stable and comprehensive

registry platform. NU DOTCO LLC will use Neustar's Registry Services platform to deploy the .WEB registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to .WEB):

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

The following is a description of each of the services.

23.2.1 SRS

Neustar's secure and stable SRS is a production-proven, standards-based, highly reliable, and high-performance domain name registration and management system. The SRS includes an EPP interface for receiving data from registrars for the purpose of provisioning and managing domain names and name servers. The response to Question 24 provides specific SRS information.

23.2.2 EPP

The .WEB registry will use the Extensible Provisioning Protocol (EPP) for the provisioning of domain names. The EPP implementation will be fully compliant with all RFCs. Registrars are provided with access via an EPP API and an EPP based Web GUI. With more than 10 gTLD, ccTLD, and private TLDs implementations, Neustar has extensive experience building EPP-based registries. Additional discussion on the EPP approach is presented in the response to Question 25.

23.2.3 DNS

NU DOTCO LLC will leverage Neustar's world-class DNS network of geographically distributed nameserver sites to provide the highest level of DNS service. The service utilizes "Anycast" routing technology, and supports both IPv4 and IPv6. The DNS network is highly proven, and currently provides service to over 20 TLDs and thousands of enterprise companies. Additional information on the DNS solution is presented in the response to Questions 35.

23.2.4 WHOIS

Neustar's existing standard WHOIS solution will be used for the .WEB. The service provides supports for near real-time dynamic updates. The design and construction is agnostic with regard to data display policy is flexible enough to accommodate any data model. In addition, a searchable WHOIS service that complies with all ICANN requirements will be provided. The following WHOIS options will be provided:

Standard WHOIS (Port 43)
Standard WHOIS (Web)
Searchable WHOIS (Web)

23.2.5 DNSSEC

An RFC compliant DNSSEC implementation will be provided using existing DNSSEC capabilities. Neustar is an experienced provider of DNSSEC services, and currently manages signed zones for three large top level domains: .biz, .us, and .co. Registrars are provided with the ability to submit and manage DS records using EPP, or through a web GUI. Additional information on DNSSEC, including the management of security extensions is found in the response to Question 43.

23.2.6 Data Escrow

Data escrow will be performed in compliance with all ICANN requirements in conjunction with an

approved data escrow provider. The data escrow service will:

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

Additional information on the Data Escrow service is provided in the response to Question 38.

23.2.7 Dissemination of Zone Files using Dynamic Updates

Dissemination of zone files will be provided through a dynamic, near real-time process. Updates will be performed within the specified performance levels. The proven technology ensures that updates pushed to all nodes within a few minutes of the changes being received by the SRS. Additional information on the DNS updates may be found in the response to Question 35.

23.2.8 Access to Bulk Zone Files

NU DOTCO LLC will provide third party access to the bulk zone file in accordance with specification 4, Section 2 of the Registry Agreement. Credentialing and dissemination of the zone files will be facilitated through the Central Zone Data Access Provider.

23.2.9 Dynamic WHOIS Updates

Updates to records in the WHOIS database will be provided via dynamic, near real-time updates. Guaranteed delivery message oriented middleware is used to ensure each individual WHOIS server is refreshed with dynamic updates. This component ensures that all WHOIS servers are kept current as changes occur in the SRS, while also decoupling WHOIS from the SRS. Additional information on WHOIS updates is presented in response to Question 26.

23.2.10 IPv6 Support

The .WEB registry will provide IPv6 support in the following registry services: SRS, WHOIS, and DNS/DNSSEC. In addition, the registry supports the provisioning of IPv6 AAAA records. A detailed description on IPv6 is presented in the response to Question 36.

23.2.11 Required Rights Protection Mechanisms

NU DOTCO LLC, will provide all ICANN required Rights Mechanisms, including:

-Trademark Claims Service
-Trademark Post-Delegation Dispute Resolution Procedure (PDDRP)
-Registration Restriction Dispute Resolution Procedure (RRDRP)
-UDRP
-URS
-Sunrise service.
More information is presented in the response to Question 29.

23.2.12 Internationalized Domain Names (IDN)

IDN registrations are provided in full compliance with the IDNA protocol. Neustar possesses extensive experience offering IDN registrations in numerous TLDs, and its IDN implementation uses advanced technology to accommodate the unique bundling needs of certain languages. Character mappings are easily constructed to block out characters that may be deemed as confusing to users. A detailed description of the IDN implementation is presented in response to Question 44.

23.3 Unique Services

NU DOTCO LLC will not be offering services that are unique to .WEB.

23.4 Security or Stability Concerns

All services offered are standard registry services that have no known security or stability

concerns. Neustar has demonstrated a strong track record of security and stability within the industry.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

24.1 Introduction

NU DOTCO LLC has partnered with NeuStar, Inc (”Neustar”), an experienced TLD registry operator, for the operation of the .WEB Registry. The applicant is confident that the plan in place for the operation of a robust and reliable Shared Registration System (SRS) as currently provided by Neustar will satisfy the criterion established by ICANN.

Neustar built its SRS from the ground up as an EPP based platform and has been operating it reliably and at scale since 2001. The software currently provides registry services to five TLDs (.BIZ, .US, TEL, .CO and .TRAVEL) and is used to provide gateway services to the .CN and .TW registries. Neustar’s state of the art registry has a proven track record of being secure, stable, and robust. It manages more than 6 million domains, and has over 300 registrars connected today.
The following describes a detailed plan for a robust and reliable SRS that meets all ICANN requirements including compliance with Specifications 6 and 10.

24.2 The Plan for Operation of a Robust and Reliable SRS

24.2.1 High-level SRS System Description

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

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

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

24.2.2 SRS Systems, Software, Hardware, and Interoperability

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

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

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

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

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

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

24.2.3 SRS Design

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

-Protocol Layer
-Business Policy Layer
-Database.

Each of the layers is described below.

24.2.4 Protocol Layer

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

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

-The registrar’s host exchanges keys to initiates a TLS handshake session with the EPP server.
-The registrar’s host must provide credentials to determine proper access levels.
-The registrar’s IP address must be preregistered in the network firewalls and traffic-shapers.

24.2.5 Business Policy Layer

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

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

The SRS today processes over 30 million EPP transactions daily.

24.2.6 Database

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

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

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

24.2.7 Number of Servers

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

24.2.8 Description of Interconnectivity with Other Registry Systems

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

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

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

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

24.2.9 WHOIS External Notifier

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

24.2.10 DNS External Notifier

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

24.2.11 Billing External Notifier

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

24.2.12 Data Warehouse

The data warehouse is responsible for managing reporting services, including registrar reports, business intelligence dashboards, and the processing of data escrow files. The Reporting Database is used to create both internal and external reports, primarily to support registrar billing and contractual reporting requirement. The data warehouse databases are updated on a daily basis with full copies of the production SRS data.

24.2.13 Frequency of Synchronization between Servers

The external notifiers discussed above perform updates in near real-time, well within the prescribed service level requirements. As transactions from registrars update the core SRS, update notifications are pushed to the external systems such as DNS and WHOIS. These updates are typically live in the external system within 2-3 minutes.

24.2.14 Synchronization Scheme (e.g., hot standby, cold standby)

Neustar operates two hot databases within the data center that is operating in primary mode. These two databases are kept in sync via synchronous replication. Additionally, there are two databases in the secondary data center. These databases are updated real time through asynchronous replication. This model allows for high performance while also ensuring protection of data. See response to Question 33 for greater detail.

24.2.15 Compliance with Specification 6 Section 1.2

The SRS implementation for .WEB is fully compliant with Specification 6, including section 1.2. EPP Standards are described and embodied in a number of IETF RFCs, ICANN contracts and practices, and registry-registrar agreements. Extensible Provisioning Protocol or EPP is defined by a core set of RFCs that standardize the interface that make up the registry-registrar model. The SRS interface supports EPP 1.0 as defined in the following RFCs shown in Table 24-1 attached.

Additional information on the EPP implementation and compliance with RFCs can be found in the response to Question 25.

24.2.16 Compliance with Specification 10

Specification 10 of the New TLD Agreement defines the performance specifications of the TLD, including service level requirements related to DNS, RDDS (WHOIS), and EPP. The requirements include both availability and transaction response time measurements. As an experienced registry operator, Neustar has a long and verifiable track record of providing registry services that consistently exceed the performance specifications stipulated in ICANN agreements. This same high level of service will be provided for the .WEB Registry. The following section describes Neustar’s experience and its capabilities to meet the requirements in the new agreement.

To properly measure the technical performance and progress of TLDs, Neustar collects data on key essential operating metrics. These measurements are key indicators of the performance and health of the registry. Neustar’s current .biz SLA commitments are among the most stringent in the industry today, and exceed the requirements for new TLDs. Table 24-2 compares the current SRS performance levels compared to the requirements for new TLDs, and clearly demonstrates the ability of the SRS to exceed those requirements.

Their ability to commit and meet such high performance standards is a direct result of their philosophy towards operational excellence. See response to Question 31 for a full description of their philosophy for building and managing for performance.

24.3 Resourcing Plans

The development, customization, and on-going support of the SRS are the responsibility of a combination of technical and operational teams, including:

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

Additionally, if customization or modifications are required, the Product Management and Quality Assurance teams will be involved in the design and testing. Finally, the Network Operations and Information Security play an important role in ensuring the systems involved are operating securely and reliably.

The necessary resources will be pulled from the pool of operational resources described in detail in the response to Question 31. Neustar's SRS implementation is very mature, and has been in production for over 10 years. As such, very little new development related to the SRS will be required for the implementation of the .WEB registry. The following resources are available from those teams:

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

The resources are more than adequate to support the SRS needs of all the TLDs operated by Neustar, including the .WEB registry.

25. Extensible Provisioning Protocol (EPP)

25.1 Introduction

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

25.2 EPP Interface

Registrars are provided with two different interfaces for interacting with the registry. Both are EPP based, and both contain all the functionality necessary to provision and manage domain names. The primary mechanism is an EPP interface to connect directly with the registry. This is the interface registrars will use for most of their interactions with the registry.

However, an alternative web GUI (Registry Administration Tool) that can also be used to perform EPP transactions will be provided. The primary use of the Registry Administration Tool is for performing administrative or customer support tasks.
The main features of the EPP implementation are:

-Standards Compliance: The EPP XML interface is compliant to the EPP RFCs. As future EPP RFCs are published or existing RFCs are updated, Neustar makes changes to the implementation keeping in mind of any backward compatibility issues.

-Scalability: The system is deployed keeping in mind that it may be required to grow and shrink the footprint of the Registry system for a particular TLD.

-Fault-tolerance: The EPP servers are deployed in two geographically separate data centers to provide for quick failover capability in case of a major outage in a particular data center. The EPP servers adhere to strict availability requirements defined in the SLAs.

-Configurability: The EPP extensions are built in a way that they can be easily configured to turn on or off for a particular TLD.

-Extensibility: The software is built ground up using object oriented design. This allows for easy extensibility of the software without risking the possibility of the change rippling through the whole application.

-Auditable: The system stores detailed information about EPP transactions from provisioning to DNS

and WHOIS publishing. In case of a dispute regarding a name registration, the Registry can provide comprehensive audit information on EPP transactions.

-Security: The system provides IP address based access control, client credential-based authorization test, digital certificate exchange, and connection limiting to the protocol layer.

25.3 Compliance with RFCs and Specifications

The registry-registrar model is described and embodied in a number of IETF RFCs, ICANN contracts and practices, and registry-registrar agreements. As shown in Table 25-1 attached, EPP is defined by the core set of RFCs that standardize the interface that registrars use to provision domains with the SRS. As a core component of the SRS architecture, the implementation is fully compliant with all EPP RFCs.

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

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

25.3.1 EPP Toolkits

Toolkits, under open source licensing, are freely provided to registrars for interfacing with the SRS. Both Java and C++ toolkits will be provided, along with the accompanying documentation. The Registrar Tool Kit (RTK) is a software development kit (SDK) that supports the development of a registrar software system for registering domain names in the registry using EPP. The SDK consists of software and documentation as described below.

The software consists of working Java and C++ EPP common APIs and samples that implement the EPP core functions and EPP extensions used to communicate between the registry and registrar. The RTK illustrates how XML requests (registration events) can be assembled and forwarded to the registry for processing. The software provides the registrar with the basis for a reference implementation that conforms to the EPP registry-registrar protocol. The software component of the SDK also includes XML schema definition files for all Registry EPP objects and EPP object extensions. The RTK also includes a “dummy” server to aid in the testing of EPP clients.

The accompanying documentation describes the EPP software package hierarchy, the object data model, and the defined objects and methods (including calling parameter lists and expected response behavior). New versions of the RTK are made available from time to time to provide support for additional features as they become available and support for other platforms and languages.

25.4 Proprietary EPP Extensions

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

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

25.5 Resourcing Plans

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

specific extensions.

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

-Development/Engineering – 19 employees
-Quality Assurance - 7 employees.

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

26. Whois

26.1 Introduction

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

Some of the key features of .WEB's solution include:

-Fully compliant with all relevant RFCs including 3912

-Production proven, highly flexible, and scalable with a track record of 100% availability over the past 10 years

-Exceeds current and proposed performance specifications

-Supports dynamic updates with the capability of doing bulk updates

-Geographically distributed sites to provide greater stability and performance

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

26.2 Software Components

The WHOIS architecture comprises the following components:

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

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

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

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

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

-Scalable architecture: The WHOIS system is scalable and has a very small footprint. Depending on the

query volume, the deployment size can grow and shrink quickly.

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

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

26.3 Compliance with RFC and Specifications 4 and 10

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

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

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

26.4 High-level WHOIS System Description

26.4.1 WHOIS Service (port 43)

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

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

26.4.2 Web Page for WHOIS queries

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

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

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

1. Redemption Grace Period calculation: Based on the registry’s policy, domains in pendingDelete can be restorable or scheduled for release depending on the date/time the domain went into pendingDelete. For these domains, the web based WHOIS displays “Restorable” or “Scheduled for Release” to clearly show this additional status to the user.

2. Extensive support for international domain names (IDN)

3. Ability to perform WHOIS lookups on the actual Unicode IDN

4. Display of the actual Unicode IDN in addition to the ACE-encoded name

5. A Unicode to Punycode and Punycode to Unicode translator

6. An extensive FAQ

7. A list of upcoming domain deletions

26.5 IT and Infrastructure Resources

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

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

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

26.6 Interconnectivity with Other Registry System

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

26.7 Frequency of Synchronization between Servers

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

26.8 Provision for Searchable WHOIS Capabilities

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

-Domain name

-Registrar ID

-Contacts and registrant's name

-Contact and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state or province, etc.)

-Name server name and name server IP address

-The system will also allow search using non-Latin character sets which are compliant with IDNA specification.
The user will choose one or more search criteria, combine them by Boolean operators (AND, OR, NOT) and provide partial or exact match regular expressions for each of the criterion name-value pairs. The domain names matching the search criteria will be returned to the user.

Figure 26-2 attached shows an architectural depiction of the new service.

To mitigate the risk of this powerful search service being abused by unscrupulous data miners, a layer of security will be built around the query engine which will allow the registry to identify rogue activities and then take appropriate measures. Potential abuses include, but are not limited to:

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

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

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

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

26.9 Resourcing Plans

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

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

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

27. Registration Life Cycle

27.1 Registration Life Cycle

27.1.1 Introduction

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

27.1.2 Domain Lifecycle - Description

The registry will use the EPP 1.0 standard for provisioning domain names, contacts and hosts. Each domain record is comprised of three registry object types: domain, contacts, and hosts.

Domains, contacts and hosts may be assigned various EPP defined statuses indicating either a particular state or restriction placed on the object. Some statuses may be applied by the Registrar; other statuses may only be applied by the Registry. Statuses are an integral part of the domain lifecycle and serve the dual purpose of indicating the particular state of the domain and indicating any restrictions placed on the domain. The EPP standard defines 17 statuses, however only 14 of these

statuses will be used in the .WEB registry per the defined .WEB business rules.

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

-OK – Default status applied by the Registry.
-Inactive – Default status applied by the Registry if the domain has less than 2 nameservers.
-PendingCreate – Status applied by the Registry upon processing a successful Create command, and indicates further action is pending. This status will not be used in the .WEB registry.
-PendingTransfer – Status applied by the Registry upon processing a successful Transfer request command, and indicates further action is pending.
-PendingDelete – Status applied by the Registry upon processing a successful Delete command that does not result in the immediate deletion of the domain, and indicates further action is pending.
-PendingRenew – Status applied by the Registry upon processing a successful Renew command that does not result in the immediate renewal of the domain, and indicates further action is pending. This status will not be used in the .WEB registry.
-PendingUpdate – Status applied by the Registry if an additional action is expected to complete the update, and indicates further action is pending. This status will not be used in the .WEB registry.
-Hold – Removes the domain from the DNS zone.
-UpdateProhibted – Prevents the object from being modified by an Update command.
-TransferProhibted – Prevents the object from being transferred to another Registrar by the Transfer command.
-RenewProhibted – Prevents a domain from being renewed by a Renew command.
-DeleteProhibted – Prevents the object from being deleted by a Delete command.

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

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

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

27.2 Registration States

27.2.1 Domain Lifecycle – Registration States

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

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

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

27.2.2 Active State

The active state is the normal state of a domain and indicates that delegation data has been provided

and the delegation information is published in the zone. A domain in an Active state may also be in the Locked or Pending Transfer states.

27.2.3 Inactive State

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

27.2.4 Locked State

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

27.2.5 Pending Transfer State

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

27.2.6 Pending Delete State

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

27.3 Typical Registration Lifecycle Activities

27.3.1 Domain Creation Process

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

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

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

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

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

27.3.2 Update Process

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

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

-Domain statuses
-Registrant ID

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

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

27.3.4 Renew Process

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

27.3.5 Transfer Process

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

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

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

1. The gaining (new) Registrar submits a Transfer command, which includes the AuthInfo code of the domain name.

2. If the AuthInfo code is valid and the domain is not in a status that does not allow transfers the domain is placed into pendingTransfer status

3. A poll message notifying the losing Registrar of the pending transfer is sent to the Registrar’s message queue

4. The domain remains in pendingTransfer status for up to 120 hours, or until the losing (current) Registrar Acks (approves) or Nack (rejects) the transfer request

5. If the losing Registrar has not Acked or Nacked the transfer request within the 120 hour timeframe, the Registry auto-approves the transfer

6. The requesting Registrar may cancel the original request up until the transfer has been completed.

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

27.3.6 Deletion Process

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

27.4 Applicable Time Elements

The following section explains the time elements that are involved.

27.4.1 Grace Periods

There are six grace periods:

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

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

27.4.2 Add-Delete Grace Period

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

27.4.3 Renew-Delete Grace Period

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

27.4.4 Transfer-Delete Grace Period

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

27.4.5 Auto-Renew-Delete Grace Period

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

27.4.6 Auto-Renew Grace Period

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

27.4.7 Redemption Grace Period

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

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

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

27.5 State Diagram

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

The different states of the lifecycle are active, inactive, locked, pending transfer, and pending delete. Please refer to section 27.2 for detailed descriptions of each of these states. The lines between the states represent triggers that transition a domain from one state to another.

The details of each trigger are described below:

-Create: Registry receives a create domain EPP command.
-WithNS: The domain has met the minimum number of nameservers required by registry policy in order to be published in the DNS zone.
-WithOutNS: The domain has not met the minimum number of nameservers required by registry policy. The domain will not be in the DNS zone.
-Remove Nameservers: Domain's nameserver(s) is removed as part of an update domain EPP command. The total nameserver is below the minimum number of nameservers required by registry policy in order to be published in the DNS zone.
-Add Nameservers: Nameserver(s) has been added to domain as part of an update domain EPP command. The total number of nameservers has met the minimum number of nameservers required by registry policy in order to be published in the DNS zone.
-Delete: Registry receives a delete domain EPP command.
-DeleteAfterGrace: Domain deletion does not fall within the add grace period.
-DeleteWithinAddGrace: Domain deletion falls within add grace period.
-Restore: Domain is restored. Domain goes back to its original state prior to the delete command.
-Transfer: Transfer request EPP command is received.
-Transfer Approve/Cancel/Reject: Transfer requested is approved or cancel or rejected.
-TransferProhibited: The domain is in clientTransferProhibited and/or serverTranferProhibited status. This will cause the transfer request to fail. The domain goes back to its original state.
-DeleteProhibited: The domain is in clientDeleteProhibited and/or serverDeleteProhibited status. This will cause the delete command to fail. The domain goes back to its original state.

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

27.5.1 EPP RFC Consistency

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

27.6 Resources

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

The .WEB registry will be using standard lifecycle rules, and as such no customization is anticipated. However should modifications be required in the future, the necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The

following resources are available from those teams:

-Development/Engineering – 19 employees
-Registry Product Management – 4 employees

These resources are more than adequate to support the development needs of all the TLDs operated by Neustar, including the .WEB registry.

28. Abuse Prevention and Mitigation

28.1 Abuse Prevention and Mitigation

Strong abuse prevention of a new gTLD is an important benefit to the internet community. .WEB and its registry operator and back-end registry services provider, Neustar agree that a registry must not only aim for the highest standards of technical and operational competence, but also needs to act as a steward of the space on behalf of the Internet community and ICANN in promoting the public interest. Neustar brings extensive experience establishing and implementing registration policies. This experience will be leveraged to help .WEB combat abusive and malicious domain activity within the new gTLD space.

One of those public interest functions for a responsible domain name registry includes working towards the eradication of abusive domain name registrations, including but not limited to those resulting from:

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

More specifically, although traditionally botnets have used Internet Relay Chat (IRC) servers to control registry and the compromised PCs, or bots, for DDoS attacks and the theft of personal information, an increasingly popular technique, known as fast-flux DNS, allows botnets to use a multitude of servers to hide a key host or to create a highly-available control network. This ability to shift the attacker’s infrastructure over a multitude of servers in various countries creates an obstacle for law enforcement and security researchers to mitigate the effects of these botnets. But a point of weakness in this scheme is its dependence on DNS for its translation services. By taking an active role in researching and monitoring these sorts of botnets, NU DOTCO LLC’s partner, Neustar has developed the ability to efficiently work with various law enforcement and security communities to begin a new phase of mitigation of these types of threats.

28.1.1 Policies and Procedures to Minimize Abusive Registrations

A Registry must have the policies, resources, personnel, and expertise in place to combat such abusive DNS practices. As .WEB’s registry provider, Neustar is at the forefront of the prevention of such abusive practices and is one of the few registry operators to have actually developed and implemented an active “domain takedown” policy. We also believe that a strong program is essential given that registrants have a reasonable expectation that they are in control of the data associated with their domains, especially its presence in the DNS zone. Because domain names are sometimes used as a mechanism to enable various illegitimate activities on the Internet often the best preventative measure to thwart these attacks is to remove the names completely from the DNS before they can impart harm, not only to the domain name registrant, but also to millions of unsuspecting Internet users.

Removing the domain name from the zone has the effect of shutting down all activity associated with the domain name, including the use of all websites and e-mail. The use of this technique should not be entered into lightly. .WEB has an extensive, defined, and documented process for taking the necessary action of removing a domain from the zone when its presence in the zone poses a threat to the security and stability of the infrastructure of the Internet or the registry.

28.1.2 Abuse Point of Contact

As required by the Registry Agreement, .WEB will establish and publish on its website a single abuse point of contact responsible for addressing inquiries from law enforcement and the public related to malicious and abusive conduct. .WEB will also provide such information to ICANN prior to the delegation of any domain names in the TLD. This information shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of malicious conduct complaints, and a telephone number and mailing address for the primary contact. We will ensure that this information will be kept accurate and up to date and will be provided to ICANN if and when changes are made. In addition, with respect to inquiries from ICANN-Accredited registrars, our registry services provider, Neustar shall have an additional point of contact, as it does today, handling requests by registrars related to abusive domain name practices.

28.2 Policies Regarding Abuse Complaints

One of the key policies each new gTLD registry will need to have is an Acceptable Use Policy that clearly delineates the types of activities that constitute “abuse” and the repercussions associated with an abusive domain name registration. In addition, the policy will be incorporated into the applicable Registry-Registrar Agreement and reserve the right for the registry to take the appropriate actions based on the type of abuse. This will include locking down the domain name preventing any changes to the contact and nameserver information associated with the domain name, placing the domain name “on hold” rendering the domain name non-resolvable, transferring to the domain name to another registrar, and/or in cases in which the domain name is associated with an existing law enforcement investigation, substituting name servers to collect information about the DNS queries to assist the investigation.

.WEB will adopt an Acceptable Use Policy that clearly defines the types of activities that will not be permitted in the TLD and reserves the right of NU DOTCO LLC to lock, cancel, transfer or otherwise suspend or take down domain names violating the Acceptable Use Policy and allow the Registry where and when appropriate to share information with law enforcement. Each ICANN-Accredited Registrar must agree to pass through the Acceptable Use Policy to its Resellers (if applicable) and ultimately to the TLD registrants. Below is the Registry’s initial Acceptable Use Policy that we will use in connection with .WEB.

28.2.1 .WEB Acceptable Use Policy

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

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

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

-Phishing: the attempt to acquire personally identifiable information by masquerading as a website other than .WEB’s own.
-Pharming: the redirection of Internet users to websites other than those the user intends to visit, usually through unauthorized changes to the Hosts file on a victim’s computer or DNS records in DNS servers.
-Dissemination of Malware: the intentional creation and distribution of ”malicious” software designed to infiltrate a computer system without the owner’s consent, including, without limitation, computer viruses, worms, key loggers, and Trojans.
-Fast Flux Hosting: a technique used to shelter Phishing, Pharming and Malware sites and networks from detection and to frustrate methods employed to defend against such practices, whereby the IP address associated with fraudulent websites are changed rapidly so as to make the true location of the sites difficult to find.
-Botnetting: the development and use of a command, agent, motor, service, or software which is

implemented: (1) to remotely control the computer or computer system of an Internet user without their knowledge or consent, (2) to generate direct denial of service (DDOS) attacks.
-Malicious Hacking: the attempt to gain unauthorized access (or exceed the level of authorized access) to a computer, information system, user account or profile, database, or security system.
-Child Pornography: the storage, publication, display and/or dissemination of pornographic materials depicting individuals under the age of majority in the relevant jurisdiction.

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

28.2.2 Taking Action Against Abusive and/or Malicious Activity
The Registry is committed to ensuring that those domain names associated with abuse or malicious conduct in violation of the Acceptable Use Policy are dealt with in a timely and decisive manner. These include taking action against those domain names that are being used to threaten the stability and security of the TLD, or is part of a real-time investigation by law enforcement.

Once a complaint is received from a trusted source, third-party, or detected by the Registry, the Registry will use commercially reasonable efforts to verify the information in the complaint. If that information can be verified to the best of the ability of the Registry, the sponsoring registrar will be notified and be given 12 hours to investigate the activity and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety or providing a compelling argument to the Registry to keep the name in the zone. If the registrar has not taken the requested action after the 12-hour period (i.e., is unresponsive to the request or refuses to take action), the Registry will place the domain on “ServerHold”. Although this action removes the domain name from the TLD zone, the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

28.2.2.1 Coordination with Law Enforcement

With the assistance of Neustar as its back-end registry services provider, .WEB can meet its obligations under Section 2.8 of the Registry Agreement where required to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its TLD. The Registry will respond to legitimate law enforcement inquiries within one business day from receiving the request. Such response shall include, at a minimum, an acknowledgement of receipt of the request, Questions or comments concerning the request, and an outline of the next steps to be taken by .WEB for rapid resolution of the request.

In the event such request involves any of the activities which can be validated by the Registry and involves the type of activity set forth in the Acceptable Use Policy, the sponsoring registrar is then given 12 hours to investigate the activity further and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety or providing a compelling argument to the registry to keep the name in the zone. If the registrar has not taken the requested action after the 12-hour period (i.e., is unresponsive to the request or refuses to take action), the Registry will place the domain on “serverHold”.

28.2.3 Monitoring for Malicious Activity

.WEB’s partner, Neustar is at the forefront of the prevention of abusive DNS practices. Neustar is one of only a few registry operators to have actually developed and implemented an active “domain takedown” policy in which the registry itself takes down abusive domain names.

Neustar’s approach is quite different from a number of other gTLD Registries and the results have been unmatched. Neustar targets verified abusive domain names and removes them within 12 hours regardless of whether or not there is cooperation from the domain name registrar. This is because

Neustar has determined that the interest in removing such threats from the consumer outweighs any potential damage to the registrar/registrant relationship.

Neustar's active prevention policies stem from the notion that registrants in the TLD have a reasonable expectation that they are in control of the data associated with their domains, especially its presence in the DNS zone. Because domain names are sometimes used as a mechanism to enable various illegitimate activities on the Internet, including malware, bot command and control, pharming, and phishing, the best preventative measure to thwart these attacks is often to remove the names completely from the DNS before they can impart harm, not only to the domain name registrant, but also to millions of unsuspecting Internet users.

28.2.3.1 Rapid Takedown Process

Since implementing the program, Neustar has developed two basic variations of the process. The more common process variation is a light-weight process that is triggered by "typical" notices. The less-common variation is the full process that is triggered by unusual notices. These notices tend to involve the need for accelerated action by the registry in the event that a complaint is received by Neustar which alleges that a domain name is being used to threaten the stability and security of the TLD, or is part of a real-time investigation by law enforcement or security researchers. These processes are described below:

28.2.3.2 Lightweight Process

In addition to having an active Information Security group that, on its own initiatives, seeks out abusive practices in the TLD, Neustar is an active member in a number of security organizations that have the expertise and experience in receiving and investigating reports of abusive DNS practices, including but not limited to, the Anti-Phishing Working Group, Castle Cops, NSP-SEC, the Registration Infrastructure Safety Group and others. Each of these sources are well-known security organizations that have developed a reputation for the prevention of harmful agents affecting the Internet. Aside from these organizations, Neustar also actively participates in privately run security associations whose basis of trust and anonymity makes it much easier to obtain information regarding abusive DNS activity.

Once a complaint is received from a trusted source, third-party, or detected by Neustar's internal security group, information about the abusive practice is forwarded to an internal mail distribution list that includes members of the operations, legal, support, engineering, and security teams for immediate response ("CERT Team"). Although the impacted URL is included in the notification e-mail, the CERT Team is trained not to investigate the URLs themselves since often times the URLs in Question have scripts, bugs, etc. that can compromise the individual's own computer and the network safety. Rather, the investigation is done by a few members of the CERT team that are able to access the URLs in a laboratory environment so as to not compromise the Neustar network. The lab environment is designed specifically for these types of tests and is scrubbed on a regular basis to ensure that none of Neustar's internal or external network elements are harmed in any fashion.

Once the complaint has been reviewed and the alleged abusive domain name activity is verified to the best of the ability of the CERT Team, the sponsoring registrar is given 12 hours to investigate the activity and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety or providing a compelling argument to the registry to keep the name in the zone.

If the registrar has not taken the requested action after the 12-hNeustar's period (i.e., is unresponsive to the request or refuses to take action), Neustar places the domain on "ServerHold". Although this action removes the domain name from the TLD zone, the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

28.2.3.3 Full Process

In the event that Neustar receives a complaint which claims that a domain name is being used to threaten the stability and security of the TLD or is a part of a real-time investigation by law enforcement or security researchers, Neustar follows a slightly different course of action.

Upon initiation of this process, members of the CERT Team are paged and a teleconference bridge is immediately opened up for the CERT Team to assess whether the activity warrants immediate action. If the CERT Team determines the incident is not an immediate threat to the security and the stability of

critical internet infrastructure, they provide documentation to the Neustar Network Operations Center to clearly capture the rationale for the decision and either refers the incident to the Lightweight process set forth above. If no abusive practice is discovered, the incident is closed.

However, if the CERT TEAM determines there is a reasonable likelihood that the incident warrants immediate action as described above, a determination is made to immediately remove the domain from the zone. As such, Customer Support contacts the responsible registrar immediately to communicate that there is a domain involved in a security and stability issue. The registrar is provided only the domain name in Question and the broadly stated type of incident. Given the sensitivity of the associated security concerns, it may be important that the registrar not be given explicit or descriptive information in regards to data that has been collected (evidence) or the source of the complaint. The need for security is to fully protect the chain of custody for evidence and the source of the data that originated the complaint.

28.2.3.3.1 Coordination with Law Enforcement & Industry Groups

One of the reasons for which Neustar was selected to serve as the back-end registry services provider by .WEB is Neustar's extensive experience with its industry-leading abusive domain name and malicious monitoring program and its close working relationship with a number of law enforcement agencies, both in the United States and internationally. For example, in the United States, Neustar is in constant communication with the Federal Bureau of Investigation, US CERT, Homeland Security, the Food and Drug Administration, and the National Center for Missing and Exploited Children.

Neustar is also a participant in a number of industry groups aimed at sharing information amongst key industry players about the abusive registration and use of domain names. These groups include the Anti-Phishing Working Group and the Registration Infrastructure Safety Group (where Neustar served for several years as on the Board of Directors). Through these organizations and others, Neustar shares information with other registries, registrars, ccTLDs, law enforcement, security professionals, etc. not only on abusive domain name registrations within its own TLDs, but also provides information uncovered with respect to domain names in other registries' TLDs. Neustar has often found that rarely are abuses found only in the TLDs for which it manages, but also within other TLDs, such as .com and .info. Neustar routinely provides this information to the other registries so that it can take the appropriate action.

With the assistance of Neustar as its back-end registry services provider, .WEB can meet its obligations under Section 2.8 of the Registry Agreement where required to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its TLD. .WEB and/or Neustar will respond to legitimate law enforcement inquiries within one business day from receiving the request. Such response shall include, at a minimum, an acknowledgement of receipt of the request, Questions or comments concerning the request, and an outline of the next steps to be taken by .WEB and/or Neustar for rapid resolution of the request.

In the event such request involves any of the activities which can be validated by .WEB and/or Neustar and involves the type of activity set forth in the Acceptable Use Policy, the sponsoring registrar is then given 12 hours to investigate the activity further and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety or providing a compelling argument to the registry to keep the name in the zone. If the registrar has not taken the requested action after the 12-hour period (i.e., is unresponsive to the request or refuses to take action), Neustar places the domain on "serverHold".

28.3 Measures for Removal of Orphan Glue Records

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

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

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

In addition, if either .WEB or Neustar become aware of actual abuse on orphaned glue after receiving written notification by a third party through its Abuse Contact or through its customer support, such glue records will be removed from the zone.

28.4 Measures to Promote WHOIS Accuracy

.WEB acknowledges that ICANN has developed a number of mechanisms over the past decade that are intended to address the issue of inaccurate WHOIS information. Such measures alone have not proven to be sufficient and therefore .WEBwill put forth additional efforts to address this by undertaking the following measures:

1) A mechanism a procedures to address domain names with inaccurate or incomplete WHOIS data
2) Policies and Procedures to ensure compliance including include audits

- Mechanism to address with inaccurate WHOIS data: a procedure whereby third parties can submit complaints directly to the Applicant (as opposed to ICANN or the sponsoring Registrar) about inaccurate or incomplete WHOIS data. Such information shall be forwarded to the sponsoring Registrar, who shall be required to address those complaints with their registrants. Thirty days after forwarding the complaint to the registrar, .WEB will examine the current WHOIS data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or there was some other disposition. If the Registrar has failed to take any action, or it is clear that the Registrant was either unwilling or unable to correct the inaccuracies, Applicant reserves the right to suspend the applicable domain name(s) until such time as the Registrant is able to cure the deficiencies.

- Policies and Procedures to ensure compliance: .WEB shall on its own initiative, no less than twice per year, perform a manual review of a random sampling of .WEB domain names to test the accuracy of the WHOIS information. Although this will not include verifying the actual information in the WHOIS record, .WEB will be examining the WHOIS data for prima facie evidence of inaccuracies. In the event that such evidence exists, it shall be forwarded to the sponsoring Registrar, who shall be required to address those complaints with their registrants. Thirty days after forwarding the complaint to the registrar, the Applicant will examine the current WHOIS data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or there was some other disposition. If the Registrar has failed to take any action, or it is clear that the Registrant was either unwilling or unable to correct the inaccuracies, .WEB reserves the right to suspend the applicable domain name(s) until such time as the Registrant is able to cure the deficiencies.

28.5 Resourcing Plans

Responsibility for abuse mitigation rests with a variety of functional groups. The Abuse Monitoring team is primarily responsible for providing analysis and conducting investigations of reports of abuse. The customer service team also plays an important role in assisting with the investigations, responded to customers, and notifying registrars of abusive domains. Finally, the Policy/Legal team is responsible for developing the relevant policies and procedures.
The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:

-Customer Support – 12 employees
-Policy/Legal – 2 employees

The resources are more than adequate to support the abuse mitigation procedures of the .WEB registry.

29. Rights Protection Mechanisms

29.1 Rights Protection Mechanisms

NU DOTCO LLC is firmly committed to the protection of Intellectual Property rights and to implementing the mandatory rights protection mechanisms contained in the Applicant Guidebook and detailed in Specification 7 of the Registry Agreement. .WEB recognizes that although the New gTLD program includes significant protections beyond those that were mandatory for a number of the current TLDs, a key motivator for .WEB's selection of Neustar as its registry services provider is Neustar's experience in successfully launching a number of TLDs with diverse rights protection mechanisms, including many the ones required in the Applicant Guidebook. More specifically, .WEB will implement the following rights protection mechanisms in accordance with the Applicant Guidebook as further described below:

-Trademark Clearinghouse: a one-stop shop so that trademark holders can protect their trademarks with a single registration.
-Sunrise and Trademark Claims processes for the TLD.
-Implementation of the Uniform Dispute Resolution Policy to address domain names that have been registered and used in bad faith in the TLD.
-Uniform Rapid Suspension: A quicker, more efficient and cheaper alternative to the Uniform Dispute Resolution Policy to deal with clear cut cases of cybersquatting.
-Implementation of a Thick WHOIS making it easier for rights holders to identify and locate infringing parties

29.1.1 Trademark Clearinghouse Including Sunrise and Trademark Claims

The first mandatory rights protection mechanism ("RPM") required to be implemented by each new gTLD Registry is support for, and interaction with, the trademark clearinghouse. The trademark clearinghouse is intended to serve as a central repository for information to be authenticated, stored and disseminated pertaining to the rights of trademark holders. The data maintained in the clearinghouse will support and facilitate other RPMs, including the mandatory Sunrise Period and Trademark Claims service. Although many of the details of how the trademark clearinghouse will interact with each registry operator and registrars, .WEB is actively monitoring the developments of the Implementation Assistance Group ("IAG") designed to assist ICANN staff in firming up the rules and procedures associated with the policies and technical requirements for the trademark clearinghouse. In addition, .WEB's back-end registry services provider is actively participating in the IAG to ensure that the protections afforded by the clearinghouse and associated RPMs are feasible and implementable.

Utilizing the trademark clearinghouse, all operators of new gTLDs must offer: (i) a sunrise registration service for at least 30 days during the pre-launch phase giving eligible trademark owners an early opportunity to register second-level domains in new gTLDs; and (ii) a trademark claims service for at least the first 60 days that second-level registrations are open. The trademark claim service is intended to provide clear notice" to a potential registrant of the rights of a trademark owner whose trademark is registered in the clearinghouse.

.WEB's registry service provider, Neustar, has already implemented Sunrise and/or Trademark Claims programs for numerous TLDs including .biz, .us, .travel, .tel and .co and will implement the both of these services on behalf of .WEB.

29.1.1.1 Neustar's Experience in Implementing Sunrise and Trademark Claims Processes

In early 2002, Neustar became the first registry operator to launch a successful authenticated Sunrise process. This process permitted qualified trademark owners to pre-register their trademarks as domain names in the .us TLD space prior to the opening of the space to the general public. Unlike any other "Sunrise" plans implemented (or proposed before that time), Neustar validated the authenticity of Trademark applications and registrations with the United States Patent and Trademark Office (USPTO).

Subsequently, as the back-end registry operator for the .tel gTLD and the .co ccTLD, Neustar launched validated Sunrise programs employing processes. These programs are very similar to those that are to be employed by the Trademark Clearinghouse for new gTLDs.

Below is a high level overview of the implementation of the .co Sunrise period that demonstrates Neustar's experience and ability to provide a Sunrise service and an overview of Neustar's experience in implementing a Trademark Claims program to trademark owners for the launch of .BIZ. Neustar's experience in each of these rights protection mechanisms will enable it to seamlessly provide these

services on behalf of .WEB as required by ICANN.

a) Sunrise and .co

The Sunrise process for .co was divided into two sub-phases:

-Local Sunrise giving holders of eligible trademarks that have obtained registered status from the Colombian trademark office the opportunity apply for the .CO domain names corresponding with their marks
-Global Sunrise program giving holders of eligible registered trademarks of national effect, that have obtained a registered status in any country of the world the opportunity apply for the .CO domain names corresponding with their marks for a period of time before registration is open to the public at large.

Like the new gTLD process set forth in the Applicant Guidebook, trademark owners had to have their rights validated by a Clearinghouse provider prior to the registration being accepted by the Registry. The Clearinghouse used a defined process for checking the eligibility of the legal rights claimed as the basis of each Sunrise application using official national trademark databases and submitted documentary evidence.

Applicants and/or their designated agents had the option of interacting directly with the Clearinghouse to ensure their applications were accurate and complete prior to submitting them to the Registry pursuant to an optional “Pre-validation Process”. Whether or not an applicant was “pre-validated”, the applicant had to submit its corresponding domain name application through an accredited registrar. When the Applicant was pre-validated through the Clearinghouse, each was given an associated approval number that it had to supply the registry. If they were not pre-validated, applicants were required to submit the required trademark information through their registrar to the Registry.
As the registry level, Neustar, subsequently either delivered the:

-Approval number and domain name registration information to the Clearinghouse
-When there was no approval number, trademark information and the domain name registration information was provided to the
Clearinghouse through EPP (as is currently required under the Applicant Guidebook).

Information was then used by the Clearinghouse as either further validation of those pre-validated applications, or initial validation of those that did not go through pre-validation. If the applicant was validated and their trademark matched the domain name applied-for, the Clearinghouse communicated that fact to the Registry via EPP.

When there was only one validated sunrise application, the application proceeded to registration when the .co launched. If there were multiple validated applications (recognizing that there could be multiple trademark owners sharing the same trademark), those were included in the .co Sunrise auction process. Neustar tracked all of the information it received and the status of each application and posted that status on a secure Website to enable trademark owners to view the status of its Sunrise application.

Although the exact process for the Sunrise program and its interaction between the trademark owner, Registry, Registrar, and IP Clearinghouse is not completely defined in the Applicant Guidebook and is dependent on the current RFI issued by ICANN in its selection of a Trademark Clearinghouse provider, Neustar’s expertise in launching multiple Sunrise processes and its established software will implement a smooth and compliant Sunrise process for the new gTLDs.

b) Trademark Claims Service Experience

With Neustar’s biz TLD launched in 2001, Neustar became the first TLD with a Trademark Claims service. Neustar developed the Trademark Claim Service by enabling companies to stake claims to domain names prior to the commencement of live .biz domain registrations.

During the Trademark Claim process, Neustar received over 80,000 Trademark Claims from entities around the world. Recognizing that multiple intellectual property owners could have trademark rights in a particular mark, multiple Trademark Claims for the same string were accepted. All applications were logged into a Trademark Claims database managed by Neustar.
The Trademark Claimant was required to provide various information about their trademark rights, including the:

-Particular trademark or service mark relied on for the trademark Claim
-Date a trademark application on the mark was filed, if any, on the string of the domain name
-Country where the mark was filed, if applicable
-Registration date, if applicable
-Class or classes of goods and services for which the trademark or service mark was registered
-Name of a contact person with whom to discuss the claimed trademark rights.

Once all Trademark Claims and domain name applications were collected, Neustar then compared the claims contained within the Trademark Claims database with its database of collected domain name applications (DNAs). In the event of a match between a Trademark Claim and a domain name application, an e-mail message was sent to the domain name applicant notifying the applicant of the existing Trademark Claim. The e-mail also stressed that if the applicant chose to continue the application process and was ultimately selected as the registrant, the applicant would be subject to Neustar's dispute proceedings if challenged by the Trademark Claimant for that particular domain name.

The domain name applicant had the option to proceed with the application or cancel the application. Proceeding on an application meant that the applicant wanted to go forward and have the application proceed to registration despite having been notified of an existing Trademark Claim. By choosing to "cancel," the applicant made a decision in light of an existing Trademark Claim notification to not proceed.

If the applicant did not respond to the e-mail notification from Neustar, or elected to cancel the application, the application was not processed. This resulted in making the applicant ineligible to register the actual domain name. If the applicant affirmatively elected to continue the application process after being notified of the claimant's (or claimants') alleged trademark rights to the desired domain name, Neustar processed the application.

This process is very similar to the one ultimately adopted by ICANN and incorporated in the latest version of the Applicant Guidebook. Although the collection of Trademark Claims for new gTLDs will be by the Trademark Clearinghouse, many of the aspects of Neustar's Trademark Claims process in 2001 are similar to those in the Applicant Guidebook. This makes Neustar uniquely qualified to implement the new gTLD Trademark Claims process.

29.1.2 Uniform Dispute Resolution Policy (UDRP) and Uniform Rapid Suspension (URS)

29.1.2.1 UDRP

Prior to joining Neustar, Mr. Neuman was a key contributor to the development of the Uniform Dispute Resolution Policy ("UDRP") in 1998. This became the first "Consensus Policy" of ICANN and has been required to be implemented by all domain name registries since that time. The UDRP is intended as an alternative dispute resolution process to transfer domain names from those that have registered and used domain names in bad faith. Although there is not much of an active role that the domain name registry plays in the implementation of the UDRP, Neustar has closely monitored UDRP decisions that have involved the TLDs for which it supports and ensures that the decisions are implemented by the registrars supporting its TLDs. When alerted by trademark owners of failures to implement UDRP decisions by its registrars, Neustar either proactively implements the decisions itself or reminds the offending registrar of its obligations to implement the decision.

29.1.2.2 URS

In response to complaints by trademark owners that the UDRP was too cost prohibitive and slow, and the fact that more than 70 percent of UDRP cases were "clear cut" cases of cybersquatting, ICANN adopted the IRT's recommendation that all new gTLD registries be required, pursuant to their contracts with ICANN, to take part in a Uniform Rapid Suspension System ("URS"). The purpose of the URS is to provide a more cost effective and timely mechanism for brand owners than the UDRP to protect their trademarks and to promote consumer protection on the Internet.

The URS is not meant to address Questionable cases of alleged infringement (e.g., use of terms in a generic sense) or for anti-competitive purposes or denial of free speech, but rather for those cases in which there is no genuine contestable issue as to the infringement and abuse that is taking place.

Unlike the UDRP which requires little involvement of gTLD registries, the URS envisages much more of an active role at the registry-level. For example, rather than requiring the registrar to lock down a domain name subject to a UDRP dispute, it is the registry under the URS that must lock the domain

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

In addition, in the event of a determination in favor of the complainant, the registry is required to suspend the domain name. This suspension remains for the balance of the registration period and would not resolve the original website. Rather, the nameservers would be redirected to an informational web page provided by the URS Provider about the URS.
Additionally, the WHOIS reflects that the domain name will not be able to be transferred, deleted, or modified for the life of the registration. Finally, there is an option for a successful complainant to extend the registration period for one additional year at commercial rates.

.WEB is fully aware of each of these requirements and will have the capability to implement these requirements for new gTLDs. In fact, during the IRT's development of f the URS, Neustar began examining the implications of the URS on its registry operations and provided the IRT with feedback on whether the recommendations from the IRT would be feasible for registries to implement.

Although there have been a few changes to the URS since the IRT recommendations, Neustar continued to participate in the development of the URS by providing comments to ICANN, many of which were adopted. As a result, Neustar is committed to supporting the URS for all of the registries that it provides back-end registry services.

29.1.3 Implementation of Thick WHOIS

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

29.1.4 Policies Handling Complaints Regarding Abuse

In addition the Rights Protection mechanisms addressed above, NU DOTCO LLC will implement a number of measures to handle complaints regarding the abusive registration of domain names in its TLD as described in .WEB's response to Question 28.

29.1.4.1 Registry Acceptable Use Policy

One of the key policies each new gTLD registry is the need to have is an Acceptable Use Policy that clearly delineates the types of activities that constitute "abuse" and the repercussions associated with an abusive domain name registration. The policy must be incorporated into the applicable Registry-Registrar Agreement and reserve the right for the registry to take the appropriate actions based on the type of abuse. This may include locking down the domain name preventing any changes to the contact and nameserver information associated with the domain name, placing the domain name "on hold" rendering the domain name non-resolvable, transferring to the domain name to another registrar, and/or in cases in which the domain name is associated with an existing law enforcement investigation, substituting name servers to collect information about the DNS queries to assist the investigation. .WEB's Acceptable Use Policy, set forth in our response to Question 28, will include prohibitions on phishing, pharming, dissemination of malware, fast flux hosting, hacking, and child pornography. In addition, the policy will include the right of the registry to take action necessary to deny, cancel, suspend, lock, or transfer any registration in violation of the policy.

29.1.4.2 Monitoring for Malicious Activity

.WEB is committed to ensuring that those domain names associated with abuse or malicious conduct in violation of the Acceptable Use Policy are dealt with in a timely and decisive manner. These include taking action against those domain names that are being used to threaten the stability and security of the TLD, or is part of a real-time investigation by law enforcement.

Once a complaint is received from a trusted source, third-party, or detected by the Registry, the Registry will use commercially reasonable efforts to verify the information in the complaint. If that information can be verified to the best of the ability of the Registry, the sponsoring registrar will be notified and be given 12 hours to investigate the activity and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety or providing a compelling argument to the Registry to keep the name in the zone. If the registrar has not taken the requested action after the 12-hour period (i.e., is unresponsive to the request or refuses to take action), the Registry will place the domain on "ServerHold". Although this action removes the domain

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

29.3 Resourcing Plans

The rights protection mechanisms described in the response above involve a wide range of tasks, procedures, and systems. The responsibility for each mechanism varies based on the specific requirements. In general the development of applications such as sunrise and IP claims is the responsibility of the Engineering team, with guidance from the Product Management team. Customer Support and Legal play a critical role in enforcing certain policies such as the rapid suspension process. These teams have years of experience implementing these or similar processes.

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

-Development/Engineering – 19 employees
-Product Management- 4 employees
-Customer Support – 12 employees

The resources are more than adequate to support the rights protection mechanisms of the .WEB registry.

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

30.(a).1 Security Policies

NU DOTCO LLC and our back-end operator, Neustar recognize the vital need to secure the systems and the integrity of the data in commercial solutions. The .WEB registry solution will leverage industry-best security practices including the consideration of physical, network, server, and application elements.
Neustar's approach to information security starts with comprehensive information security policies. These are based on the industry best practices for security including SANS (SysAdmin, Audit, Network, Security) Institute, NIST (National Institute of Standards and Technology), and CIS (Center for Internet Security). Policies are reviewed annually by Neustar's information security team.

The following is a summary of the security policies that will be used in the .WEB registry, including:

1. Summary of the security policies used in the registry operations
2. Description of independent security assessments
3. Description of security features that are appropriate for .WEB
4. List of commitments made to registrants regarding security levels

All of the security policies and levels described in this section are appropriate for the .WEB registry.

30.(a).2 Summary of Security Policies

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

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

The following policies are included in the Program:

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

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

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

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

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

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

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

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

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

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

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

12. Mobile Device Security Policy
The Mobile Device Policy covers the requirements specific to mobile devices with information storage

or processing capabilities. This policy includes laptop standards, as well as requirements for PDAs, mobile phones, digital cameras and music players, and any other removable device capable of transmitting, processing or storing information.

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

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

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

30.(a).3 Independent Assessment Reports

Neustar IT Operations is subject to yearly Sarbanes-Oxley (SOX), Statement on Auditing Standards #70 (SAS70) and ISO audits. Testing of controls implemented by Neustar management in the areas of access to programs and data, change management and IT Operations are subject to testing by both internal and external SOX and SAS70 audit groups. Audit Findings are communicated to process owners, Quality Management Group and Executive Management. Actions are taken to make process adjustments where required and remediation of issues is monitored by internal audit and QM groups.
External Penetration Test is conducted by a third party on a yearly basis. As authorized by Neustar, the third party performs an external Penetration Test to review potential security weaknesses of network devices and hosts and demonstrate the impact to the environment. The assessment is conducted remotely from the Internet with testing divided into four phases:

-A network survey is performed in order to gain a better knowledge of the network that was being tested
-Vulnerability scanning is initiated with all the hosts that are discovered in the previous phase
-Identification of key systems for further exploitation is conducted
-Exploitation of the identified systems is attempted.

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

30.(a).4 Augmented Security Levels and Capabilities

There are no increased security levels specific for .WEB. However, Neustar will provide the same high level of security provided across all of the registries it manages.
A key to Neustar’s Operational success is Neustar’s highly structured operations practices. The standards and governance of these processes:

-Include annual independent review of information security practices
-Include annual external penetration tests by a third party
-Conform to the ISO 9001 standard (Part of Neustar’s ISO-based Quality Management System)
-Are aligned to Information Technology Infrastructure Library (ITIL) and CoBIT best practices
-Are aligned with all aspects of ISO IEC 17799
-Are in compliance with Sarbanes-Oxley (SOX) requirements (audited annually)
-Are focused on continuous process improvement (metrics driven with product scorecards reviewed monthly).

A summary view to Neustar’s security policy in alignment with ISO 17799 can be found in section 30.(a).5 below.

30.(a).5 Commitments and Security Levels

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

Compliance with High Security Standards

-Security procedures and practices that are in alignment with ISO 17799
-Annual SOC 2 Audits on all critical registry systems
-Annual 3rd Party Penetration Tests
-Annual Sarbanes Oxley Audits

Highly Developed and Document Security Policies

-Compliance with all provisions described in section 30.(b) and in the attached security policy document.
-Resources necessary for providing information security
-Fully documented security policies
-Annual security training for all operations personnel

High Levels of Registry Security

-Multiple redundant data centers
-High Availability Design
-Architecture that includes multiple layers of security
-Diversified firewall and networking hardware vendors
-Multi-factor authentication for accessing registry systems
-Physical security access controls
-A 24x7 manned Network Operations Center that monitors all systems and applications
-A 24x7 manned Security Operations Center that monitors and mitigates DDoS attacks
-DDoS mitigation using traffic scrubbing technologies

© Internet Corporation For Assigned Names and Numbers.

EXHIBIT JJN-2

New gTLD Application Submitted to ICANN by: VeriSign Sarl

String: קום

Originally Posted: 13 June 2012

Application ID: 1-1254-29622

Applicant Information

1. Full legal name

VeriSign Sarl

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact Information Redacted

4. Fax number

Contact Information Redacted

5. If applicable, website or URL

http://www.verisigninc.com/en_CH/index.xhtml?loc=en_CH#/site_owners

Primary Contact

6(a). Name

Ms. Sarah Elizabeth Langstone

6(b). Title

Director, Product Management

6(c). Address

6(d). Phone Number

Contact Information Redacted

6(e). Fax Number

Contact Information Redacted

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Mr. Joe Alton Waldron

7(b). Title

Director, Product Management

7(c). Address

7(d). Phone Number

Contact Information Redacted

7(e). Fax Number

Contact Information Redacted

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Société à Responsabilité Limitée (Sàrl)

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

Switzerland

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.

VeriSign Switzerland SA

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

Not applicable.

Applicant Background

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

Daniel Blättler	Gérant (Manager)
Romain Jean-Pierre Cholat	Gérant (Manager) & President

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

Daniel Blättler	Gérant (Manager)
Romain Jean-Pierre Cholat	Gérant (Manager) & President

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

VeriSign Switzerland SA	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.

קום

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

xn--9dbq2a

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

Transliteration of com

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

Hebrew

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

he

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

Hebrew

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

Hebr

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

U+05E7 U+05D5 U+05DD

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

Attachments are not displayed on this form.

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

Verisign will leverage its mature shared registration system to provide services for the HEBREW_TRANSLITERATION_OF_COM gTLD. Verisign's registration software is in compliance with all current IDN standards, including ICANN's IDN Guidelines, as well as The Internationalized Domain Names in Applications (IDNA 2008) specification, published by the IETF as RFC 5891.

The IDN tables provided herein represent Unicode characters allowed for registration by Verisign's software. The data in these tables come from three categories of source material.

1. Openly available language standards, published in RFC and other formats, by appropriate authorities.
2. The Unicode Standard, specifically definitions of written scripts as defined by this well-known specification.
3. ICANN's own IDN Implementation Guidelines, which provide some special rules for domain registration, especially code points not appropriate for the DNS.

Attached IDN Tables

Per ICANN's requirement, "IDN tables should be submitted in a machine-readable format. The model format described in Section 5 of RFC 4290 would be ideal." Of the formats that the TAS tool accepts, there are no machine readable formats available for upload. The best format for machine readable, RFC 4290 compliant, text would be the open standard ASCII text format of .txt. Upon inquiring with ICANN applicants were told to submit the IDN tables in an .xls or .pdf format. All of the IDN tables attached to this application are available in the machine readable open standard ASCII text format of .txt. In order to meet the 5 attachment per question limit and the 5MB size per file, we have divided the Language and Script files into five files that accommodate the size of the tables. As such we have attached 4 .pdf files, and one .xls file. The single Excel file contains the one script file for Han which far exceeded the 5MB limit in .pdf but is offered here in .xls format. Again, all IDN tables are available for ICANN's review in the required RFC 4290 compliant machine readable open standard ASCII text format of .txt outlined in the application; however, due to limitations in the TAS tool accommodations have been made.

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

N/A

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.

Having successfully operated TLDs for more than 16 years and having used IDNs in our registries since 2000, Verisign has deep knowledge and understanding of potential operational or rendering problems associated with TLDs and IDN strings.

Verisign operates the HEBREW_TRANSLITERATION_OF_COM gTLD in compliance with the most recently approved versions of the ICANN IDN Guidelines and RFC application protocol, currently RFC 5891, Internationalized Domain Names in Applications (IDNA 2008).

Bi-directional rules for impacted scripts, outlined in RFC 5893 (Right-to-Left Scripts for IDNA), specify the relevant rules for the HEBREW_TRANSLITERATION_OF_COM gTLD.

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

ˈkoʊm

Mission/Purpose

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

1 MISSION AND PURPOSE OF PROPOSED GTLD

The primary mission of the HEBREW_TRANSLITERATION_OF_.COM gTLD is to improve the user experience by offering a fully internationalized domain name (IDN) that includes a transliteration of .com. This gTLD is intended to serve users whose primary language is based in Hebrew script. For the first time in the history of the Domain Name System (DNS), internationalized generic top-level domains (gTLDs) create the capability for speakers of non-Latin-based languages to access the DNS entirely in their native script. Offering HEBREW_TRANSLITERATION_OF_.COM represents a critical step toward implementing that functionality. Verisign's vision is to improve usability of domain names for users of major scripts around the world. Registrants and Internet users will be able to use their native script, if desired, to take advantage of their domain name's functionality, ubiquity, and stability.

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

2 BENEFIT TO REGISTRANTS, INTERNET USERS, AND OTHERS

As of this writing, more than 800,000 internationalized second-level domain names are registered in .com, including approximately 12,000 in Hebrew. The HEBREW_TRANSLITERATION_OF_.COM gTLD, along with the other proposed IDN transliterations of .com, provide an immediate benefit to registrants of those names by giving them the opportunity to register IDN second-level domain names as "IDN.IDN" domain names. That is, registrants can use their preferred script in both the second-level domain name and the gTLD name. Doing so improves these domain names' functionality and accessibility to speakers of non-Latin-based languages.

We anticipate that the availability of the HEBREW_TRANSLITERATION_OF_.COM will greatly increase the appeal and value of internationalized addresses in Israel. Expanding the accessibility and functionality of these domain names to users worldwide is the primary benefit of all internationalized transliterations of .com.

Finally, we anticipate that HEBREW_TRANSLITERATION_OF_.COM will increase choice and competition in Israel and elsewhere by giving local users the option of registering their domain name with an established, trusted gTLD in their own language. Potential registrants in Israel currently have limited choices if they want to register an IDN.IDN domain name in a gTLD that is recognized across Hebrew-speaking regions. The HEBREW_TRANSLITERATION_OF_.COM gTLD creates an attractive new option for these users.

More specifically, the HEBREW_TRANSLITERATION_OF_.COM gTLD benefits the following groups:

Registrants: As discussed above, current .com registrants with second-level .com IDNs in

Hebrew can greatly expand the functionality and reach of their existing registered addresses by the availability of IDN.IDN domain names entirely in Hebrew script. In addition, new registrants, whether Israel or elsewhere, who seek entirely Hebrew addresses, have the option of registering their IDN.IDN domain names in a globally recognized domain.

Internet Users: The HEBREW_TRANSLITERATION_OF_.COM gTLD significantly increases the ubiquity and functionality of .com for users around the world, particularly those in Israel. For the first time, Hebrew speakers could access a transliteration of .com addresses entirely in their native script. Verisign is committed to ensuring that the domain name experience remains consistent to all users, in every major script, everywhere in the world. This commitment supports the vision of “One World. One Internet.” that infuses ICANN’s global efforts.

2.1 Business Goals

Our goal is for HEBREW_TRANSLITERATION_OF_.COM to operate as a best-in-class IDN registry. Although the HEBREW_TRANSLITERATION_OF_.COM gTLD is distinct from the .com gTLD in the DNS, we plan to provide a similar high quality of service that users of .com have come to expect.

The first step in this process is to ensure that, like .com, HEBREW_TRANSLITERATION_OF_.COM operates at the highest level of availability, stability, and security. The HEBREW_TRANSLITERATION_OF_.COM gTLD is rooted in the same world-class infrastructure that supports .com and .net at the highest level of operational excellence. Users and registrants have extremely high expectations of .com, and we leverage the full capability of our infrastructure and operational expertise to ensure that HEBREW_TRANSLITERATION_OF_.COM meets these expectations from the moment of its launch.

The initial target audience for HEBREW_TRANSLITERATION_OF_.COM is the registrants of the approximately 12,000 IDN second-level addresses in .com. These registrants will have the opportunity to register their IDN.com addresses as IDN. HEBREW_TRANSLITERATION_OF_.COM addresses.

The secondary target market for HEBREW_TRANSLITERATION_OF_.COM is the current registrants of ASCII domain name addresses who may be doing business in Israel or other regions with a high number of Hebrew speakers. The HEBREW_TRANSLITERATION_OF_.COM gTLD provides these registrants a ready-made solution to localize their online identity while still maintaining the continuity of their .com addresses.

Finally, we are committed to working with registrars to perform outreach in Israel and elsewhere to reach potential new registrants who are interested in establishing a new HEBREW_TRANSLITERATION_OF_.COM domain name.

2.2. Competition, Differentiation, and Innovation Goals

Hebrew speakers currently have limited options for registering IDN.IDN domain names. The HEBREW_TRANSLITERATION_OF_.COM gTLD introduces competition and choice for registrants in Israel by providing them with an option that—while new—also carries the trust, reliability, and accessibility of an established global brand.

What differentiates HEBREW_TRANSLITERATION_OF_.COM from other potential market entrants for Hebrew IDN gTLDs is that it represents a localized representation of a domain that many users already know and trust, .com. In addition, HEBREW_TRANSLITERATION_OF_.COM is the best available phonetic representation of “.com” in Hebrew. The IDN’s brand is the brand of a globally recognized domain, operated by a globally recognized provider.

2.3 User Experience Goals

Verisign’s goal for HEBREW_TRANSLITERATION_OF_.COM is to deliver a user experience as similar to the current experience of .com as possible. Verisign operates the HEBREW_TRANSLITERATION_OF_.COM gTLD at the same high level of security, stability, and

availability as .com, allowing registrars to enjoy the same high service levels that Verisign provides for all of the domains we operate.

We helped organize and are deeply involved in the IDN Software Developers Consortium (IDNSDC), which is committed to improving the functionality and accessibility of IDNs to users. We continue to engage significantly in the IDNSDC to complement the IDN initiatives being driven by ICANN and to help drive adoption of IDN capabilities in standard client software.

2.4 Registration Policies

The registration policies for HEBREW_TRANSLITERATION_OF_.COM follow closely the existing IDN registration policies for .com. The Verisign Shared Registration System (SRS) allows the creation of IDNs that contain Unicode supported non-ASCII scripts. We have developed a policy for IDN registrations specifying permissible and prohibited code points. The policy is implemented in the following five rules. IDNs that adhere to these five rules are considered valid registrations.

2.4.1. Internet Engineering Task Force (IETF) Standards

The IDNA2008 specification defines rules and algorithms that permit/prohibit Unicode points in IDN registrations. We comply with all of the RFC documents that comprise the IDNA2008 standard.

2.4.2. Restrictions on Specific Languages

All IDN registrations require a three-letter Language Tag. HEB, for instance, is for the Hebrew language. If the Language Tag associated with the registration is in our Language Tag Table, we have a List of Included Characters for that language. The requested IDN must be entirely contained within this List of Included Characters. If even one code point from the IDN is not a valid character for this language, the registration is rejected.

2.4.3. Restriction on Commingling of Scripts

If the Language Tag specified in the IDN registration is not in the approved list of Language Tags located on our website, and so does not have a List of Included Characters, then we apply an alternate restriction to prevent commingling of different scripts in a single domain.

The Unicode Standard defines a set of Unicode Scripts (http://www.unicode.org/Public/6.0.0/ucd/Scripts.txt) by assigning each code point exactly one Unicode script value. As a rule, Verisign rejects the commingling of code points from different Unicode scripts. That is, if an IDN contains code points from two or more Unicode scripts, then that IDN registration is rejected. For example, a character from the Latin script cannot be used in the same IDN with any Cyrillic character. All code points within an IDN must come from the same Unicode script. This is done to prevent confusable code points from appearing in the same IDN.

Again, this rule only applies to languages for which there is not a strictly defined List of Included Characters. For example, the FRE Language Tag, indicating the French language, does not have a strict List of Included Characters, and so the commingling rule applies. All code points in a French domain must come from a single script.

2.4.4. The Verisign SRS also adheres to ICANN’s Guidelines for the Implementation of Internationalized Domain Names. Section 5 of the document outlines characters that are allowed by the IETF standard, but should be prohibited for IDN registration.

2.4.5. Special Characters

There are two (Unicode characters whose latest definitions are not backward compatible with previous versions of the IDNA Standard. The Latin Sharp S and Greek Final Sigma were previously mapped to alternate characters. Clients and registries that comply with the older standard would, for instance, map a Latin Sharp S into two lowercase Latin letter S characters. This mapping is irreversible. The latest version of the IDNA standard does not apply this mapping. So, whereas the Latin Sharp S was previously prohibited (mapped into other characters), the latest standard allows registries to accept this character at their own discretion.

Because these changes are not backward compatible, Verisign has elected to continue to

disallow these two characters until a clear and fair approach to their registration has been reached and communicated.
Additional information about our registration policies and approach to rights protection is available in our response to Question 29, Rights Protection Mechanisms.

2.5 Measures to Protect Privacy and Confidentiality

We limit information collection from registrants to ICANN mandated data points required in the registration of a domain name, and use this data solely for the purpose of publishing to the publicly available Whois service. Whois Terms of Use are available on our website.

2.6 Outreach and Communications

Registrar Outreach

Many of our registrars have marketed and supported IDNs at the second-level of the .com TLD for more than ten years. Well-established registrars have provided IDN communications and customer service in markets where IDNs provide the highest level of benefit. We have sought advice from registrars and actively communicated the planned approach for launching IDNs at the top-level in regular meetings with the registrar channel. We continue to work closely with registrars not only to prepare for the Sunrise, Trademark Claims service, and general launch periods, but also to reach existing and prospective registrants who are interested in realizing the benefits of IDNs.

Registrant and End-User Outreach

We augment our existing IDN web content with launch planning information and additional online resources for the IDN.IDN transliterations of .com. This web content includes details on the benefits of IDNs, and our approach to protect intellectual property and enhance end-user ubiquity. The full launch plan addresses Sunrise and Trademark Claims services, general launch through the registrar channel, and localized content for the initial launch markets.
The IDN Software Developer’s Consortium (IDNSDC)

To complement the IDN initiatives being driven by ICANN, we have organized a consortium to facilitate adoption of IDN capabilities in standard client software. The IDNSDC works with domain name industry stakeholders and application developers to bring greater awareness to existing client-side application challenges so that registrars in communication with their domain name registrants may fully understand usability issues.

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

3 OPERATING RULES TO MINIMIZE SOCIAL COSTS

Verisign follows the standards and procedures in the Applicant Guidebook to ensure the stable, secure, and successful launch and operation of the HEBREW_TRANSLITERATION_OF_.COM gTLD. The registration policies described in Section 2.4 ensure that all HEBREW_TRANSLITERATION_OF_.COM addresses comply with Internet standards, and ensure ICANN guidelines are put in place to reduce end-user confusion and security-related issues.

Our implementation of Language Tags and the restrictions on script commingling are intended to minimize the risk of misuse of IDN domain names for activities such as phishing.

3.1 Resolution of Multiple Applications

During the Sunrise phase of the HEBREW_TRANSLITERATION_OF_.COM launch, the registry accepts only applications with a valid identifier from the Trademark Clearinghouse. If multiple applications are received for the same domain name, the registry uses a first-come/first-served

policy to determine the registrant.
During the general availability of the domain name, we continue to employ a first-come/first-served policy. Therefore, multiple requests for the same domain name result in a successful registration for the first request while subsequent requests will return a Not Available status.

3.2 Cost Benefits for Registrants

The introduction of IDN gTLDs, including HEBREW_TRANSLITERATION_OF_.COM, introduces competition and choice to registrants interested in localizing their online identities to better reach
non-English speaking end users.

3.3 Contractual Commitments Regarding Price Escalation

We provide to registrars at least six months’ written notice of any increase to domain name registration fees.

4 OTHER STEPS TO MINIMIZE NEGATIVE CONSEQUENCES/COSTS IMPOSED UPON CONSUMERS

We have implemented extensive abuse prevention and rights protection mechanisms, as outlined in the response to Question 28, Abuse Prevention and Mitigation, and Question 29, Rights Protection Mechanisms.

Community-based Designation

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

No

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

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

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

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

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

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

Attachments are not displayed on this form.

Geographic Names

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

No

Protection of Geographic Names

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

The Verisign registry solution provides a mechanism for reserving second-level domain names that prevents them from being registered. This functionality includes a list of strings that the system will not allow to be registered. Strings can be added and removed from this list as needed.

For the protection of geographic names for the HEBREW_TRANSLITERATION_OF_COM gTLD, the country and territory names contained in the following internationally recognized lists shall be blocked initially:

* The short form (in English) of all country and territory names, including the European Union, contained on the International Organization for Standardization (ISO) 3166-1 list:

http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166-1_decoding_table.htm#EU

* The United Nations Group of Experts on Geographical Names (UNGEGN), Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World:

http://unstats.un.org/unsd/geoinfo/UNGEGN/publications.html

* The list of United Nations member states, in six official United Nations languages, prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names. The most recent list of country names approved by the Working Group was submitted on behalf of UNGEGN for the Ninth UN Conference on the Standardization of Geographical Names in August

2007: E/CONF.98/89 Add.1 (http://unstats.un.org/unsd/geoinfo/ungegn/docs/9th-uncsgn-docs/econf/9th_UNCSGN_e-conf-98-89-add1.pdf)

As new versions of these three internationally recognized lists are published, Verisign will update the list of names reserved by the Verisign registry system to reflect any changes.

In addition to providing protection for geographic names, this reserved name functionality will be used to reserve other names specifically ineligible for delegation. For example, Section 2.2.1.2.3 of the Applicant Guidebook lists strings associated with the International Olympic Committee and the International Red Cross and Red Crescent organizations to be prohibited from delegation per the Government Advisory Committee (GAC) request.

All the strings on these lists as well as any others put forth by the GAC and approved by ICANN will be included in the list of reserved names.

There are no plans at this time to release any of the reserved names. If, however, Verisign intends to release any of the names at a future date, we will follow the appropriate procedures, outlined in Section 5 of Specification 5, on the release of reserved names.

Registry Services

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

1 CUSTOMARY REGISTRY SERVICES

Verisign provides a comprehensive system and physical security solution that is designed to ensure a TLD is protected from unauthorized disclosure, alteration, insertion, or destruction of registry data. Our system addresses all areas of security including information and policies, security procedures, the systems development lifecycle, physical security, system hacks, break-ins, data tampering, and other disruptions to operations. Our operational environments not only meet the security criteria specified in our customer contractual agreements, thereby preventing unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with applicable standards, but also are subject to multiple independent assessments as detailed in the response to Question 30, Security Policy. Our physical and system security methodology follows a mature, ongoing lifecycle that was developed and implemented many years before the development of the industry standards with which we currently comply. Please see the response to Question 30, Security Policy, for details of the security features of our registry services.

Verisign’s registry services comply with relevant standards and best current practice RFCs published by the Internet Engineering Task Force (IETF), including all successor standards, modifications, or additions relating to the DNS and name server operations including without limitation RFCs 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 3901, 4343, and 4472. Moreover, our Shared Registration System (SRS) supports the following IETF Extensible Provisioning Protocol (EPP) specifications, where the Extensible Markup Language (XML) templates and XML schemas are defined in RFC 3915, 5730, 5731, 5732, 5733, and 5734. By strictly adhering to these RFCs, we help ensure our registry services do not create a condition that adversely affects the throughput, response time, consistency, or coherence of responses to Internet servers or end systems. Besides our leadership in authoring RFCs for EPP, Domain Name System Security Extensions (DNSSEC), and other DNS services, we have created and contributed to several now well-established IETF standards and are a regular and long-standing participant in key Internet standards forums.

Figure 23-1 (see Attachment VRSN_.comHebrew_Q23 Figures for all figures in this response) summarizes the technical and business components of those registry services, customarily offered by a registry operator (i.e., Verisign), that support this application. These services are currently operational and support both large and small Verisign-managed registries. We provide customary registry services in the same manner as we provide these services for our existing gTLD.

Through these established registry services, we have proven our ability to operate a reliable and low-risk registry that supports millions of transactions per day. We are unaware of any potential security or stability concern related to any of these services.

Registry services defined by this application are not intended to be offered in a manner unique to the new generic top-level domain (gTLD) nor are any proposed services unique to this application's registry.

As further evidence of Verisign's compliance with ICANN mandated security and stability requirements, we allocate the applicable RFCs to each of the five customary registry services (items A – E above). For each registry service, we also provide evidence in Figure 23-2 of our RFC compliance and include relevant ICANN prior-service approval actions.

1.1 Critical Operations of the Registry

I. Receipt of Data from Registrars Concerning Registration of Domain Names and Name Servers

See Item A in Figure 23-1 and Figure 23-2.

ii. Provision to Registrars Status Information Relating to the Zone Servers

Verisign registry services provisions to registrars status information relating to zone servers for the TLD. The services also allow a domain name to be updated with client Hold, server Hold status, which removes the domain name server details from zone files. This ensures that DNS queries of the domain name are not resolved temporarily. When these hold statuses are removed, the name server details are written back to zone files and DNS queries are again resolved. Figure 23-3 describes the domain name status information and zone insertion indicator provided to registrars. The zone insertion indicator determines whether the name server details of the domain name exist in the zone file for a given domain name status. Verisign also has the capability to withdraw domain names from the zone file in near-real time by changing the domain name statuses upon request by customers, courts, or legal authorities as required.

iii. Dissemination of TLD Zone Files

See Item B in Figure 23-1 and Figure 23-2.

iv. Operation of the Registry Zone Servers

As a company, Verisign operates zone servers and serves DNS resolution from 76 geographically distributed resolution sites located in North America, South America, Africa, Europe, Asia, and Australia. Currently, 17 DNS locations are designated primary sites, offering greater capacity than smaller sites comprising the remainder of the Verisign constellation. We also use Any cast techniques and regional Internet resolution sites to expand coverage, accommodate emergency or surge capacity, and support system availability during maintenance procedures. We operate the gTLD from a minimum of eight of our primary sites (two on the East Coast of the United States, two on the West Coast of the United States, two in Europe, and two in Asia) and expand resolution sites based on traffic volume and patterns. Further details of the geographic diversity of our zone servers are provided in the response to Question 34, Geographic Diversity. Moreover, additional details of our zone servers are provided in the response to Question 32, Architecture and the response to Question 35, DNS Service.

v. Dissemination of Contact and Other Information Concerning Domain Name Server Registrations

See Item C in Figure 23-1 and Figure 23-2.

2 OTHER PRODUCTS OR SERVICES THE REGISTRY OPERATOR IS REQUIRED TO PROVIDE BECAUSE OF THE ESTABLISHMENT OF A CONSENSUS POLICY

Verisign is a proven supporter of ICANN's consensus-driven, bottom-up policy development process whereby community members identify a problem, initiate policy discussions, and generate a solution that produces effective and sustained results. Verisign currently provides all of the products or services (collectively referred to as services) that the registry operator is required to provide because of the establishment of a Consensus Policy. For the HEBREW_TRANSLITERATION_OF_.COM gTLD, we implement these services using the same proven processes and procedures currently in-place for all registries under our management. Furthermore, we execute these services on computing platforms comparable to those of other registries under our management. Our extensive experience with consensus policy required services and our proven processes to implement these services greatly minimize any potential risk to Internet security or stability. Details of these services are provided in the following subsections. It shall be noted that consensus policy services required of registrars (e.g., Whois Reminder, Expired Domain) are not included in this response. This exclusion is in accordance with the direction provided in the question's Notes column to address registry operator services.

2.1 Inter-Registrar Transfer Policy (IRTP)

Technical Component
In compliance with the IRTP consensus policy, we have designed our registration systems to systematically restrict the transfer of domain names within 60 days of the initial create date. In addition, we have implemented EPP and "AuthInfo" code functionality, which is used to further authenticate transfer requests. The registration system has been designed to enable compliance with the five-day Transfer grace period and includes the following functionality:

* Allows the losing registrar to proactively 'ACK' or acknowledge a transfer prior to the expiration of the five-day Transfer grace period
* Allows the losing registrar to proactively 'NACK' or not acknowledge a transfer prior to the expiration of the five-day Transfer grace period
* Allows the system to automatically ACK the transfer request once the five-day Transfer grace period has passed if the losing registrar has not proactively ACK'd or NACK'd the transfer request.

Business Component
All requests to transfer a domain name to a new registrar are handled according to the procedures detailed in the IRTP. Dispute proceedings arising from a registrar's alleged failure to abide by this policy may be initiated by any ICANN-accredited registrar under the Transfer Dispute Resolution Policy. Our compliance office serves as the first-level dispute resolution provider pursuant to the associated Transfer Dispute Resolution Policy. As needed Verisign is available to offer policy guidance as issues arise.

Security and Stability Concerns
We are unaware of any impact, caused by the service, on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems. By implementing the IRTP in accordance with ICANN policy, security is enhanced as all transfer commands are authenticated using the AuthInfo code prior to processing.

ICANN Prior Approval
We have been in compliance with the IRTP since November 2004.

Unique to the TLD
This service is not provided in a manner unique to the HEBREW_TRANSLITERATION_OF_.COM gTLD.

2.2 Add Grace Period (AGP) Limits Policy

Technical Component
Our registry system monitors registrars' Add grace period deletion activity and provides reporting that permits us to assess registration fees upon registrars that have exceeded the AGP thresholds stipulated in the AGP Limits Policy. Further, we accept and evaluate all exemption requests received from registrars and determine whether the exemption request

meets the exemption criteria. We maintain all AGP Limits Policy exemption request activity so that this material may be included within our Monthly Registry Operator Report to ICANN.

Registrars that exceed the limits established by the policy may submit exemption requests to us for consideration. Our compliance office reviews these exemption requests in accordance with the AGP Limits Policy and renders a decision. Upon request, we submit associated reporting on exemption request activity to support reporting in accordance with established ICANN requirements.

Business Component
The Add grace period (AGP) is restricted for any gTLD operator that has implemented an AGP. Specifically, for each operator:

* During any given month, an operator may not offer any refund to an ICANN-accredited registrar for any domain names deleted during the AGP that exceed (i) 10% of that registrar's net new registrations (calculated as the total number of net adds of one-year through ten-year registrations as defined in the monthly reporting requirement of Operator Agreements) in that month, or (ii) fifty (50) domain names, whichever is greater, unless an exemption has been granted by an operator.
* Upon the documented demonstration of extraordinary circumstances, a registrar may seek from an operator an exemption from such restrictions in a specific month. The registrar must confirm in writing to the operator how, at the time the names were deleted, these extraordinary circumstances were not known, reasonably could not have been known, and were outside the registrar's control. Acceptance of any exemption will be at the sole and reasonable discretion of the operator; however "extraordinary circumstances" that reoccur regularly for the same registrar will not be deemed extraordinary.

In addition to all other reporting requirements to ICANN, we identify each registrar that has sought an exemption, along with a brief description of the type of extraordinary circumstance and the action, approval, or denial that the operator took.

Security and Stability Concerns
We are unaware of any impact, caused by the policy, on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems.

ICANN Prior Approval
We have had experience with this policy since its implementation in April 2009.

Unique to the TLD
This service is not provided in a manner unique to the HEBREW_TRANSLITERATION_OF_.COM gTLD.

2.3 Registry Services Evaluation Policy (RSEP)

Technical Component
We adhere to all RSEP submission requirements. We have followed the process many times and are fully aware of the submission procedures, the type of documentation required, and the evaluation process that ICANN adheres to.

Business Component
In accordance with ICANN procedures detailed on the ICANN RSEP website (http://www.icann.org/en/registries/rsep/), all gTLD registry operators are required to follow this policy when submitting a request for new registry services.

Security and Stability Concerns
As part of the RSEP submission process, we identify any potential security and stability concerns in accordance with RSEP stability and security requirements. We never launch services without satisfactory completion of the RSEP process and resulting approval.

ICANN Prior Approval
Not applicable.

Unique to the TLD
gTLD RSEP procedures are not implemented in a manner unique to the

HEBREW_TRANSLITERATION_OF_.COM gTLD.

3 PRODUCTS OR SERVICES ONLY A REGISTRY OPERATOR IS CAPABLE OF PROVIDING BY REASON OF ITS DESIGNATION AS THE REGISTRY OPERATOR

We have developed a Registry-Registrar Two-Factor Authentication Service that complements traditional registration and resolution registry services. In accordance with direction provided in Question 23, Verisign details below the technical and business components of the service, identifies any potential threat to registry security or stability, and lists previous interactions with
ICANN to approve the operation of the service. The Two-Factor Authentication Service is currently operational, supporting multiple registries under ICANN's purview.

We are unaware of any competition issue that may require the registry service(s) listed in this response to be referred to the appropriate governmental competition authority or authorities with applicable jurisdiction. ICANN previously approved the service(s), at which time it was determined that either the service(s) raised no competitive concerns or any applicable concerns related to competition were satisfactorily addressed.

3.1 Two-Factor Authentication Service

Technical Component
The Registry-Registrar Two-Factor Authentication Service is designed to improve domain name security and assist registrars in protecting the accounts they manage. As part of the service, dynamic one-time passwords (OTPs) augment the user names and passwords currently used to process update, transfer, and/or deletion requests. These one-time passwords enable transaction processing to be based on requests that are validated both by "what users know" (i.e., their user name and password) and "what users have" (i.e., a two-factor authentication credential with a one-time-password).

Registrars can use the OTP when communicating directly with Verisign's Customer Service department as well as when using the registrar portal to make manual updates, transfers, and/or deletion transactions. The Two-Factor Authentication Service is an optional service offered to registrars that execute the Registry-Registrar Two-Factor Authentication Service Agreement.

Business Component
There is no charge for the Registry-Registrar Two-Factor Authentication Service. It is enabled only for registrars that wish to take advantage of the added security provided by the service.

Security and Stability Concerns
We are unaware of any impact, caused by the service, on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems. The service is intended to enhance domain name security, resulting in increased confidence and trust by registrants.

ICANN Prior Approval
ICANN approved the same Two-Factor Authentication Service for Verisign's use on .com and .net on 10 July 2009 (RSEP Proposal 2009004) and for .name on 16 February 2011 (RSEP Proposal 2011001).

Unique to the TLD
This service is not provided in a manner unique to the HEBREW_TRANSLITERATION_OF_.COM gTLD.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

1 ROBUST PLAN FOR OPERATING A RELIABLE SRS

1.1 High-Level Shared Registration System (SRS) System Description

Verisign provides and operates a robust and reliable SRS that enables multiple registrars to provide domain name registration services in the top-level domain (TLD). Our proven reliable SRS serves approximately 915 registrars, and as a company, we have averaged more than 140 million registration transactions per day. The SRS provides a scalable, fault-tolerant platform for the delivery of gTLDs through the use of a central customer database, a web interface, a standard provisioning protocol (i.e., Extensible Provisioning Protocol, EPP), and a transport protocol (i.e., Secure Sockets Layer, SSL).

The SRS components include:

* Web Interface: Allows customers to access the authoritative database for accounts, contacts, users, authorization groups, product catalog, product subscriptions, and customer notification messages.

* EPP Interface: Provides an interface to the SRS that enables registrars to use EPP to register and manage domains, hosts, and contacts.

* Authentication Provider: A Verisign-developed application, specific to the SRS, that authenticates a user based on a login name, password, and the SSL certificate common name and client IP address.

The SRS is designed to be scalable and fault tolerant by incorporating clustering in multiple tiers of the platform. New nodes can be added to a cluster within a single tier to scale a specific tier, and if one node fails within a single tier, the services will still be available. The SRS allows registrars to manage the HEBREW_TRANSLITERATION_OF_.COM gTLD domain names in a single architecture.

To flexibly accommodate the scale of our transaction volumes, as well as new technologies, we employ the following design practices:

* Scale for Growth: Scale to handle current volumes and projected growth.

* Scale for Peaks: Scale to twice base capacity to withstand “registration add attacks” from a compromised registrar system.

* Limit Database CPU Utilization: Limit utilization to no more than 50 percent during peak loads.

* Limit Database Memory Utilization: Each user’s login process that connects to the database allocates a small segment of memory to perform connection overhead, sorting, and data caching. Our standards mandate that no more than 40 percent of the total available physical memory on the database server will be allocated for these functions.

Our SRS is built upon a three-tier architecture as illustrated in Figure 24-1 (see Attachment VRSN_.comHebrew_Q24 Figures for all figures in this response) and detailed here:

* Gateway Layer: The first tier, the gateway servers, uses EPP to communicate with registrars. These gateway servers then interact with application servers, which comprise the second tier.

* Application Layer: The application servers contain business logic for managing and maintaining the registry business. The business logic is particular to each TLD’s business rules and requirements. The flexible internal design of the application servers allows Verisign to easily leverage existing business rules to apply to the HEBREW_TRANSLITERATION_OF_.COM gTLD. The application servers store Verisign’s data in the registry database, which comprises the third and final tier. This simple, industry-standard design has been highly effective with other customers for whom we provide backend registry services.

* Database Layer: The database is the heart of this architecture. It stores all the essential

information provisioned from registrars through the gateway servers. Separate servers query the database, extract updated zone and Whois information, validate that information, and distribute it around the clock to our worldwide domain name resolution sites.

Scalability and Performance

We implement our scalable SRS on a supportable infrastructure that achieves the availability requirements in Specification 10. We employ the design patterns of simplicity and parallelism in both our software and systems, based on our experience that these factors contribute most significantly to scalability and reliable performance. Going counter to feature-rich development patterns, we intentionally minimize the number of lines of code between the end user and the data delivered. The result is a network of restorable components that provide rapid, accurate updates. Figure 24-2 depicts EPP traffic flows and local redundancy in our SRS provisioning architecture. As detailed in the figure, local redundancy is maintained for each layer as well as each piece of equipment. This built-in redundancy enhances operational performance while enabling the future system scaling necessary to meet additional demand created by this or future registry applications.

Besides improving scalability and reliability, local SRS redundancy enables us to take down individual system components for maintenance and upgrades, with little to no performance impact. With our redundant design, we can perform routine maintenance while the remainder of the system remains online and unaffected. For the HEBREW_TRANSLITERATION_OF_.COM gTLD registry, this flexibility minimizes unplanned downtime and provides a more consistent end-user experience.

1.2 Representative Network Diagrams

Figure 24-3 provides a summary network diagram of Verisign’s SRS. This configuration at both the primary and alternate-primary Verisign data centers provides a highly reliable backup capability. Data is continuously replicated between both sites to ensure failover to the alternate-primary site can be implemented expeditiously to support both planned and unplanned outages.

1.3 Number of Servers

We continually review our server deployments for all aspects of our registry service. We evaluate usage based on peak performance objectives as well as current transaction volumes, which drive the quantity of servers in our implementations. Our scaling is based on the following factors:

* Server configuration is based on CPU, memory, disk IO, total disk, and network throughput projections.

* Server quantity is determined through statistical modeling to fulfill overall performance objectives as defined by both the service availability and the server configuration.

* To ensure continuity of operations for the HEBREW_TRANSLITERATION_OF_.COM gTLD, we use a minimum of
100 dedicated servers per SRS site. These servers are virtualized to meet demand.

1.4 Description of Interconnectivity with Other Registry Systems

Figure 24-4 provides a technical overview of Verisign’s SRS, showing how the SRS component fits into this larger system and interconnects with other system components.

1.5 Frequency of Synchronization Between Servers

We use synchronous replication to keep our SRS continuously in sync between the two data centers. This synchronization is performed in near-real time, thereby supporting rapid failover should a failure occur or a planned maintenance outage be required.

1.6 Synchronization Scheme

Verisign uses synchronous replication to keep the SRS continuously in sync between the two data centers. Because the alternate-primary site is continuously up, and built using an identical design to the primary data center, it is classified as a “hot standby.”

2 SCALABILITY AND PERFORMANCE ARE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

As an experienced backend registry provider, we have developed and use proprietary system scaling models to guide the growth of our TLD supporting infrastructure. These models direct our infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. We periodically update these models to account for the adoption of more capable and cost-effective technologies.

Verisign’s scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the HEBREW_TRANSLITERATION_OF_.COM gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to our scaling models, we derived the necessary infrastructure required to implement and sustain this gTLD. Cost related to this infrastructure is provided as “Total Critical Registry Function Cash Outflows” (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

As an experienced backend registry provider, we have developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. We routinely adjust these staffing models to account for new tools and process innovations. These models enable us to continually right-size our staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to our staffing models, we derived the necessary personnel levels required for this gTLD’s initial implementation and ongoing maintenance. This personnel-related cost is included in “Total Critical Registry Function Cash Outflows” (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise our technical work force. (Current statistics are publicly available in our quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, we have maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving our ability to align personnel resource growth to the scale increases of our TLD service offerings.

We project we will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support SRS performance:

* Application Engineers: 19
* Database Administrators: 8
* Database Engineers: 3
* Network Administrators: 11
* Network Architects: 4
* Project Managers: 25
* Quality Assurance Engineers: 11
* SRS System Administrators: 13

*	Storage Administrators: 4
*	Systems Architects: 9

To implement and manage the HEBREW_TRANSLITERATION_OF_.COM gTLD as described in this application, we scale, as needed, the size of each technical area now supporting our portfolio of TLDs. Consistent with our resource modeling, we periodically review the level of work to be performed and adjust staff levels for each technical area.

When usage projections indicate a need for additional staff, our internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all our TLDs instead of creating a new entity to manage only this proposed gTLD, we realize significant economies of scale and ensure our TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as we hold all contributing staff members accountable to the same procedures that guide our execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, we afford new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 EVIDENCE OF COMPLIANCE WITH SPECIFICATION 6 AND 10 TO THE REGISTRY AGREEMENT

Section 1.2 (EPP) of Specification 6, Registry Interoperability and Continuity Specifications

Verisign provides these services using our SRS, which complies fully with Specification 6, Section 1.2 of the Registry Agreement. In using our SRS to provide backend registry services, we implement and comply with relevant existing RFCs (i.e., 5730, 5731, 5732, 5733, 5734, and 5910) and intend to comply with RFCs that may be published in the future by the Internet Engineering Task Force (IETF), including successor standards, modifications, or additions thereto relating to the provisioning and management of domain names that use EPP. In addition, our SRS includes a Registry Grace Period (RGP) and thus complies with RFC 3915 and its successors. Details of the Verisign SRS' compliance with RFC SRS/EPP are provided in the response to Question 25, Extensible Provisioning Protocol. We do not use functionality outside the base EPP RFCs, although proprietary EPP extensions are documented in Internet-Draft format following the guidelines described in RFC 3735 within the response to Question 25. Moreover, prior to deployment, Verisign will provide to ICANN updated documentation of all the EPP objects and extensions supported in accordance with Specification 6, Section 1.2.

Specification 10, EPP Registry Performance Specifications

Verisign's SRS meets all EPP Registry Performance Specifications detailed in Specification 10, Section 2. Evidence of this performance can be verified by a review of the .com and .net Registry Operator's Monthly Reports, which we file with ICANN. These reports detail our operational status of the .com and .net registries, which use an SRS design and approach comparable to the one proposed for the HEBREW_TRANSLITERATION_OF_.COM gTLD. These reports provide evidence of our ability to meet registry operation service level agreements (SLAs) comparable to those detailed in Specification 10. The reports are accessible at the following URL: http://www.icann.org/en/tlds/monthly-reports/.

In accordance with EPP Registry Performance Specifications detailed in Specification 10, our SRS meets the following performance attributes:

*	EPP service availability: Fewer than or equal to 864 minutes of downtime (approximately 98%)

*	EPP session-command round trip time (RTT): Fewer than or equal to 4000 milliseconds (ms), for at least 90 percent of the commands

*	EPP query-command RTT: Fewer than or equal to 2000 ms, for at least 90 percent of the

commands

* EPP transform-command RTT: Fewer than or equal to 4000 ms, for at least 90 percent of the commands

25. Extensible Provisioning Protocol (EPP)

1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF THIS ASPECT OF REGISTRY TECHNICAL REQUIREMENTS

We have used Extensible Provisioning Protocol (EPP) since our inception and possess complete knowledge and understanding of EPP registry systems. Our first EPP implementation—for a thick registry for the .name generic top-level domain (gTLD)—was in 2002. Since then we have continued our RFC-compliant use of EPP in multiple TLDs, as detailed in Figure 25-1 (see Attachment VRSN_.comHebrew_Q25 Figures for all figures in this response).

Our understanding of EPP and our ability to implement code that complies with the applicable RFCs is unparalleled. Mr. Scott Hollenbeck, Verisign's director of software development, authored the Extensible Provisioning Protocol and continues to be fully engaged in its refinement and enhancement (U.S. Patent Number 7299299 – Shared registration system for registering domain names). We have also developed numerous new object mappings and object extensions following the guidelines in RFC 3735 (Guidelines for Extending the Extensible Provisioning Protocol). Mr. James Gould, a principal engineer at Verisign, led and co-authored the most recent EPP Domain Name System Security Extensions (DNSSEC) RFC effort (RFC 5910).

All Verisign registry systems use EPP. Upon approval of this application, we will use EPP to provide registry services for this gTLD. The .com, .net, and .name registries, for which we are the registry operator, use an SRS design and approach comparable to the one proposed for this gTLD. Approximately 915 registrars use our EPP service, and the registry system performs more than 140 million EPP transactions daily without performance issues or restrictive maintenance windows. The processing time service level agreement (SLA) requirements for the Verisign-operated .net gTLD are the strictest of the current Verisign-managed gTLDs. All processing times for Verisign-operated gTLDs can be found in ICANN's Registry Operator's Monthly Reports at http://www.icann.org/en/tlds/monthly-reports/.

We have also been active on the Internet Engineering Task Force (IETF) Provisioning Registry Protocol (provreg) working group and mailing list since work started on the EPP protocol in 2000. This working group provided a forum for members of the Internet community to comment on Mr. Scott Hollenbeck's initial EPP drafts, which Mr. Hollenbeck refined based on input and discussions with representatives from registries, registrars, and other interested parties. The working group has since concluded, but the mailing list is still active to enable discussion of different aspects of EPP.

1.1 EPP Interface with Registrars

Verisign fully supports the features defined in the EPP specifications and provides a set of software development kits (SDK) and tools to help registrars build secure and stable interfaces. Our SDKs give registrars the option of either fully writing their own EPP client software to integrate with the Shared Registration System (SRS), or using the Verisign-provided SDKs to aid them in the integration effort. Registrars can download the Verisign EPP SDKs and tools from the registrar website (http://www.Verisign.com/domain-name-services/current-registrars/epp-sdk/index.html).

The EPP SDKs provide a host of features including connection pooling, Secure Sockets Layer (SSL), and a test server (stub server) to run EPP tests against. One tool—the EPP tool—provides a web interface for creating EPP Extensible Markup Language (XML) commands and sending them to a configurable set of target servers. This helps registrars in creating the template XML and testing a variety of test cases against the EPP servers. An Operational Test and Evaluation (OT&E) environment, which runs the same software as the production system

so approved registrars can integrate and test their software before moving into a live production environment, is also available.

2 TECHNICAL PLAN SCOPE/SCALE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

As an experienced backend registry provider, we have developed and use proprietary system scaling models to guide the growth of our TLD supporting infrastructure. These models direct our infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. We periodically update these models to account for the adoption of more capable and cost-effective technologies.

Our scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the HEBREW_TRANSLITERATION_OF_.COM gTLD
with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to our scaling models, we derived the necessary infrastructure required to implement and sustain this gTLD. Cost related to this infrastructure is provided as “Total Critical Registry Function Cash Outflows” (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

As an experienced backend registry provider, we have developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. We routinely adjust these staffing models to account for new tools and process innovations. These models enable us to continually right-size our staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to our staffing models, we derived the necessary personnel levels required for this gTLD’s initial implementation and ongoing maintenance. Cost related to this infrastructure is provided as “Total Critical Registry Function Cash Outflows” (Template 1, Line IIb.G) within the Question 46 financial projections response.

We employ more than 1,040 individuals of which more than 775 comprise our technical work force. (Current statistics are publicly available in our quarterly filings.) Drawing from this pool of
on-hand and fully committed technical resources, we have maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving our ability to align personnel resource growth to the scale increases of our TLD service offerings.

We project we will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support the provisioning of EPP services:

* Application Engineers: 19
* Database Engineers: 3
* Quality Assurance Engineers: 11

To implement and manage the HEBREW_TRANSLITERATION_OF_.COM gTLD as described in this application, we scale, as needed, the size of each technical area now supporting our portfolio of TLDs. Consistent with our resource modeling, we periodically review the level of work to be performed and adjust staff levels for each technical area.

When usage projections indicate a need for additional staff, our internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed

by the lead of the relevant technical area. By scaling one common team across all our TLDs instead of creating a new entity to manage only this proposed gTLD, we realize significant economies of scale and ensure our TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed TLD, as we hold all contributing staff members accountable to the same procedures that guide our execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, we afford new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 ABILITY TO COMPLY WITH RELEVANT RFCS

We incorporate design reviews, code reviews, and peer reviews into our software development lifecycle (SDLC) to ensure compliance with the relevant RFCs. Our dedicated QA team creates extensive test plans and issues internal certifications when it has confirmed the accuracy of the code in relation to the RFC requirements. Our QA organization is independent from the development team within engineering. This separation helps Verisign ensure adopted processes and procedures are followed, further ensuring that all software releases fully consider the security and stability of the TLD.

For the HEBREW_TRANSLITERATION_OF_.COM gTLD, the Shared Registration System (SRS) complies with the following IETF EPP specifications, where the XML templates and XML schemas are defined in the following specifications:

* EPP RGP 3915 (http://www.apps.ietf.org/rfc/rfc3915.html): EPP Redemption Grace Period (RGP) Mapping specification for support of RGP statuses and support of Restore Request and Restore Report (authored by Verisign's Scott Hollenbeck)

* EPP 5730 (http://tools.ietf.org/html/rfc5730): Base EPP specification (authored by Verisign's Scott Hollenbeck)

* EPP Domain 5731 (http://tools.ietf.org/html/rfc5731): EPP Domain Name Mapping specification (authored by Verisign's Scott Hollenbeck)

* EPP Host 5732 (http://tools.ietf.org/html/rfc5732): EPP Host Mapping specification (authored by Verisign's Scott Hollenbeck)

* EPP Contact 5733 (http://tools.ietf.org/html/rfc5733): EPP Contact Mapping specification (authored by Verisign's Scott Hollenbeck)

* EPP TCP 5734 (http://tools.ietf.org/html/rfc5734): EPP Transport over Transmission Control Protocol (TCP) specification (authored by Verisign's Scott Hollenbeck)

* EPP DNSSEC 5910 (http://tools.ietf.org/html/rfc5910): EPP Domain Name System Security Extensions (DNSSEC) Mapping specification (authored by Verisign's James Gould and Scott Hollenbeck)

5 PROPRIETARY EPP EXTENSIONS

We use our SRS to provide registry services. The SRS supports the following EPP specifications, which we developed following the guidelines in RFC 3735, where the XML templates and XML schemas are defined in the specifications:

* IDN Language Tag (http://www.verisigninc.com/assets/idn-language-tag.pdf): EPP internationalized domain names (IDN) language tag extension used for IDN domain name registrations

* RGP Poll Mapping (http://www.verisigninc.com/assets/whois-info-extension.pdf): EPP mapping for an EPP poll message in support of Restore Request and Restore Report

* Whois Info Extension (http://www.verisigninc.com/assets/whois-info-extension.pdf): EPP

extension for returning additional information needed for transfers

* EPP ConsoliDate Mapping (http://www.verisigninc.com/assets/consolidate-mapping.txt): EPP mapping to support a Domain Sync operation for synchronizing domain name expiration dates

* NameStore Extension (http://www.verisigninc.com/assets/namestore-extension.pdf): EPP extension for routing with an EPP intelligent gateway to a pluggable set of backend products and services

* Low Balance Mapping (http://www.verisigninc.com/assets/low-balance-mapping.pdf): EPP mapping to support low balance poll messages that proactively notify registrars of a low balance (available credit) condition

As part of the 2006 implementation report to bring the EPP RFC documents from Proposed Standard status to Draft Standard status, an implementation test matrix was completed. Two independently developed EPP client implementations based on the RFCs were tested against the Verisign EPP server for the domain, host, and contact transactions. No compliance-related issues were identified during this test, providing evidence that these extensions comply with RFC 3735 guidelines and further demonstrating Verisign's ability to design, test, and deploy an RFC-compliant EPP implementation. A copy of the implementation test matrix that was completed in 2006 to bring the EPP RFC documents from Proposed Standard status to Draft Standard Status can be found here: http://www.ietf.org/iesg/implementation/report-rfc4930-4934.txt

5.1 EPP Templates and Schemas

The EPP XML schemas are formal descriptions of the EPP XML templates. They are used to express the set of rules to which the EPP templates must conform in order to be considered valid by the schema. The EPP schemas define the building blocks of the EPP templates, describing the format of the data and the different EPP commands' request and response formats. The current EPP implementations managed by Verisign use these EPP templates and schemas, as will the proposed TLD. For each proprietary XML template/schema, we provide a reference to the applicable template and include the schema.

XML templates/schema for idnLang-1.0 (IDN Language Tag)

* Template: The templates for idnLang-1.0 can be found in Chapter 3, EPP Command Mapping of the relevant EPP documentation, http://www.verisigninc.com/assets/idn-language-tag.pdf.

* Schema: This schema describes the extension mapping for the IDN language tag. The mapping extends the EPP domain name mapping to provide additional features required for the provisioning of IDN domain name registrations.

```
〈?xml version="1.0" encoding="UTF-8"?〉

〈schema targetNamespace="http://www.Verisign.com/epp/idnLang-1.0"
 xmlns:idnLang="http://www.Verisign.com/epp/idnLang-1.0"
 xmlns="http://www.w3.org/2001/XMLSchema"
 elementFormDefault="qualified"〉

〈annotation〉
  〈documentation〉
   Extensible Provisioning Protocol v1.0 domain name
   extension schema for IDN Lang Tag.
  〈/documentation〉
〈/annotation〉

〈!--
Child elements found in EPP commands.
```

```
--〉
   〈element name=”tag” type=”language”/〉

   〈!--
  End of schema.
  --〉
 〈/schema〉
```

XML templates/schema for rgp-poll-1.0 (RGP Poll Mapping)

* Template: The templates for rgp-poll-1.0 can be found in Chapter 3, EPP Command Mapping of the relevant EPP documentation, http://www.verisigninc.com/assets/rgp-poll-mapping.pdf.
* Schema: This schema describes the extension mapping for poll notifications. The mapping extends the EPP base mapping to provide additional features for registry grace period (RGP) poll notifications.

```
 〈?xml version=”1.0” encoding=”UTF-8”?〉

 〈schema targetNamespace=”http://www.Verisign.com/epp/rgp-poll-1.0”
  xmlns:rgp-poll=”http://www.Verisign.com/epp/rgp-poll-1.0”
  xmlns:eppcom=”urn:ietf:params:xml:ns:eppcom-1.0”
  xmlns:rgp=”urn:ietf:params:xml:ns:rgp-1.0”
  xmlns=”http://www.w3.org/2001/XMLSchema”
  elementFormDefault=”qualified”〉

 〈!--
Import common element types.
--〉
 〈import namespace=”urn:ietf:params:xml:ns:eppcom-1.0”
  schemaLocation=”eppcom-1.0.xsd”/〉
 〈import namespace=”urn:ietf:params:xml:ns:rgp-1.0”
  schemaLocation=”rgp-1.0.xsd”/〉

 〈annotation〉
   〈documentation〉
    Extensible Provisioning Protocol v1.0
    Verisign poll notification specification for registry grace period
    poll notifications.
   〈/documentation〉
 〈/annotation〉

 〈!--
Child elements found in EPP commands.
--〉
 〈element name=”pollData” type=”rgp-poll:pollDataType”/〉

 〈!--
Child elements of the  〈notifyData〉  element for the
redemption grace period.
--〉
 〈complexType name=”pollDataType”〉
   〈sequence〉
     〈element name=”name” type=”eppcom:labelType”/〉
     〈element name=”rgpStatus” type=”rgp:statusType”/〉
     〈element name=”reqDate” type=”dateTime”/〉
```

```
    〈element name=”reportDueDate” type=”dateTime”/〉
  〈/sequence〉
〈/complexType〉
〈
!--
End of schema.
--〉
〈/schema〉
```

XML templates/schema for whoisInf-1.0 (Whois Info Extension)

*	Template: The templates for whoisInf-1.0 can be found in Chapter 3, EPP Command Mapping of the relevant EPP documentation, http://www.verisigninc.com/assets/whois-info-extension.pdf.
*	Schema: This schema describes the extension mapping for the Whois Info extension. The mapping extends the EPP domain name mapping to provide additional features for returning additional information needed for transfers.

```
〈?xml version=”1.0” encoding=”UTF-8”?〉

〈schema targetNamespace=”http://www.Verisign.com/epp/whoisInf-1.0”
 xmlns:whoisInf=”http://www.Verisign.com/epp/whoisInf-1.0”
 xmlns:eppcom=”urn:ietf:params:xml:ns:eppcom-1.0”
 xmlns=”http://www.w3.org/2001/XMLSchema”
 elementFormDefault=”qualified”〉

〈import namespace=”urn:ietf:params:xml:ns:eppcom-1.0”
 schemaLocation=”eppcom-1.0.xsd”/〉

〈annotation〉
  〈documentation〉
   Extensible Provisioning Protocol v1.0
   extension schema for Whois Info
  〈/documentation〉
〈/annotation〉

〈!--
Possible Whois Info extension root elements.
--〉
〈element name=”whoisInf” type=”whoisInf:whoisInfType”/〉
〈element name=”whoisInfData” type=”whoisInf:whoisInfDataType”/〉

〈!--
Child elements for the 〈whoisInf〉 extension which
is used as an extension to an info command.
--〉
〈complexType name=”whoisInfType”〉
  〈sequence〉
    〈element name=”flag” type=”boolean”/〉
  〈/sequence〉
〈/complexType〉

〈!--
Child elements for the 〈whoisInfData〉 extension which
is used as an extension to the info response.
--〉
〈complexType name=”whoisInfDataType”〉
```

```
   ⟨sequence⟩
   ⟨element name=”registrar” type=”string”/⟩
   ⟨element name=”whoisServer” type=”eppcom:labelType”
    minOccurs=”0”/⟩
   ⟨element name=”url” type=”token” minOccurs=”0”/⟩
   ⟨element name=”irisServer” type=”eppcom:labelType”
    minOccurs=”0”/⟩
   ⟨/sequence⟩
   ⟨/complexType⟩

 ⟨/schema⟩
```

XML templates/schema for sync-1.0 (EPP ConsoliDate Mapping)

* Template: The templates for sync-1.0 can be found in Chapter 3, EPP Command Mapping of the relevant EPP documentation, http://www.verisigninc.com/assets/consolidate-mapping.txt.
* Schema: This schema describes the extension mapping for the synchronization of domain name registration period expiration dates. This service is known as ”ConsoliDate.” The mapping extends the EPP domain name mapping to provide features that allow a protocol client to end a domain name registration period on a specific month and day.

```
  ⟨?xml version=”1.0” encoding=”UTF-8”?⟩

    ⟨schema targetNamespace=”http://www.Verisign.com/epp/sync-1.0”
           xmlns:sync=”http://www.Verisign.com/epp/sync-1.0”
           xmlns=”http://www.w3.org/2001/XMLSchema”
           elementFormDefault=”qualified”⟩

      ⟨annotation⟩
        ⟨documentation⟩
         Extensible Provisioning Protocol v1.0 domain name
         extension schema for expiration date synchronization.
        ⟨/documentation⟩
      ⟨/annotation⟩

    ⟨!--
   Child elements found in EPP commands.
   --⟩
      ⟨element name=”update” type=”sync:updateType”/⟩

    ⟨!--
   Child elements of the  ⟨update⟩  command.
   --⟩
      ⟨complexType name=”updateType”⟩
        ⟨sequence⟩
          ⟨element name=”expMonthDay” type=”gMonthDay”/⟩
        ⟨/sequence⟩
      ⟨/complexType⟩

    ⟨!--
   End of schema.
   --⟩
    ⟨/schema⟩
```

XML templates/schema for namestoreExt-1.1 (NameStore Extension)

*	Template: The templates for namestoreExt-1.1 can be found in Chapter 3, EPP Command Mapping of the relevant EPP documentation, http://www.verisigninc.com/assets/namestore-extension.pdf.
*	Schema: This schema describes the extension mapping for the routing with an EPP intelligent gateway to a pluggable set of backend products and services. The mapping extends the EPP domain name and host mapping to provide a sub-product identifier to identify the target sub-product that the EPP operation is intended for.

```
〈?xml version="1.0" encoding="UTF-8"?〉

〈schema targetNamespace="http://www.Verisign-grs.com/epp/namestoreExt-1.1"
 xmlns="http://www.w3.org/2001/XMLSchema"
 xmlns:namestoreExt="http://www.Verisign-grs.com/epp/namestoreExt-1.1"
 elementFormDefault="qualified"〉

〈annotation〉
  〈documentation〉
   Extensible Provisioning Protocol v1.0 Namestore extension schema
   for destination registry routing.
  〈/documentation〉
〈/annotation〉

〈!-- General Data types. --〉
〈simpleType name="subProductType"〉
  〈restriction base="token"〉
    〈minLength value="1"/〉
    〈maxLength value="64"/〉
  〈/restriction〉
〈/simpleType〉

〈complexType name="extAnyType"〉
  〈sequence〉
    〈any namespace="##other" maxOccurs="unbounded"/〉
  〈/sequence〉
〈/complexType〉

〈!-- Child elements found in EPP commands and responses. --〉
〈element name="namestoreExt" type="namestoreExt:namestoreExtType"/〉

〈!-- Child elements of the 〈product〉 command. --〉
〈complexType name="namestoreExtType"〉
  〈sequence〉
    〈element name="subProduct"
     type="namestoreExt:subProductType"/〉
  〈/sequence〉
〈/complexType〉

〈!-- Child response elements. --〉
〈element name="nsExtErrData" type="namestoreExt:nsExtErrDataType"/〉

〈!-- 〈prdErrData〉 error response elements. --〉
〈complexType name="nsExtErrDataType"〉
  〈sequence〉
    〈element name="msg" type="namestoreExt:msgType"/〉
  〈/sequence〉
  〈/complexType〉
```

```
〈!-- 〈prdErrData〉 〈msg〉 element. --〉
〈complexType name="msgType"〉
  〈simpleContent〉
    〈extension base="normalizedString"〉
      〈attribute name="code"
       type="namestoreExt:prdErrCodeType" use="required"/〉
      〈attribute name="lang" type="language" default="en"/〉
    〈/extension〉
  〈/simpleContent〉
〈/complexType〉

〈!-- 〈prdErrData〉 error response codes. --〉
〈simpleType name="prdErrCodeType"〉
  〈restriction base="unsignedShort"〉
    〈enumeration value="1"/〉
  〈/restriction〉
〈/simpleType〉

〈!-- End of schema. --〉
〈/schema〉
```

XML templates/schema for lowbalance-poll-1.0 (Low Balance Mapping)

* Template: The templates for lowbalance-poll-1.0 can be found in Chapter 3, EPP Command Mapping of the relevant EPP documentation, http://www.verisigninc.com/assets/low-balance-mapping.pdf.
* Schema: This schema describes the extension mapping for the account low balance notification. The mapping extends the EPP base mapping so an account holder can be notified via EPP poll messages whenever the available credit for an account reaches or goes below the credit threshold.

```
〈?xml version="1.0" encoding="UTF-8"?〉

〈schema targetNamespace="http://www.Verisign.com/epp/lowbalance-poll-1.0"
 xmlns:lowbalance-poll="http://www.Verisign.com/epp/lowbalance-poll-1.0"
 xmlns:eppcom="urn:ietf:params:xml:ns:eppcom-1.0"
 xmlns="http://www.w3.org/2001/XMLSchema"
 elementFormDefault="qualified"〉

〈!-- Import common element types.--〉
〈import namespace="urn:ietf:params:xml:ns:eppcom-1.0"
 schemaLocation="eppcom-1.0.xsd"/〉

〈annotation〉
  〈documentation〉
   Extensible Provisioning Protocol v1.0
   Verisign poll notification specification for low balance notifications.
  〈/documentation〉
〈/annotation〉

〈!--Child elements found in EPP commands.--〉
〈element name="pollData" type="lowbalance-poll:pollDataType"/〉

〈!--Child elements of the 〈notifyData〉 element for the low balance.--〉
〈complexType name="pollDataType"〉
```

```
  〈sequence〉
    〈element name=”registrarName” type=”eppcom:labelType”/〉
    〈element name=”creditLimit” type=”normalizedString”/〉
    〈element name=”creditThreshold”
     type=”lowbalance-poll:thresholdType”/〉
    〈element name=”availableCredit” type=”normalizedString”/〉
  〈/sequence〉
〈/complexType〉

〈complexType name=”thresholdType”〉
  〈simpleContent〉
    〈extension base=”normalizedString”〉
      〈attribute name=”type”
       type=”lowbalance-poll:thresholdValueType”
       use=”required”/〉
    〈/extension〉
  〈/simpleContent〉
〈/complexType〉

〈simpleType name=”thresholdValueType”〉
  〈restriction base=”token”〉
    〈enumeration value=”FIXED”/〉
    〈enumeration value=”PERCENT”/〉
  〈/restriction〉
〈/simpleType〉

〈!-- End of schema.--〉
〈/schema〉
```

6 PROPRIETARY EPP EXTENSION CONSISTENCY WITH REGISTRATION LIFECYCLE

Verisign’s proprietary EPP extensions, defined in Section 5 above, are consistent with the registration lifecycle documented in the response to Question 27, Registration Lifecycle. Details of the registration lifecycle are presented in that response. As new registry features are required, we develop proprietary EPP extensions to address new operational requirements. Consistent with ICANN procedures we adhere to all applicable Registry Services Evaluation Process (RSEP) procedures.

26. Whois

1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF THIS ASPECT OF REGISTRY TECHNICAL REQUIREMENTS

Verisign has operated the Whois lookup service for the gTLDs and ccTLDs we manage since 1991, and will provide these proven services for the HEBREW_TRANSLITERATION_OF_.COM gTLD registry. In addition, we continue to work with the Internet community to improve the utility of Whois data, while thwarting its application for abusive uses.

1.1 High-Level Whois System Description

Like all other components of our registry service, our Whois system is designed and built for both reliability and performance in full compliance with applicable RFCs. Our current Whois implementation has answered more than five billion Whois queries per month for the TLDs we manage, and has experienced more than 250,000 queries per minute in peak conditions. The proposed gTLD uses a Whois system design and approach that is comparable to the current implementation. Independent quality control testing ensures our Whois service is RFC-

compliant through all phases of its lifecycle.

Our redundant Whois databases further contribute to overall system availability and reliability. The hardware and software for our Whois service is architected to scale both horizontally (by adding more servers) and vertically (by adding more CPUs and memory to existing servers) to meet future need.

We can fine-tune access to our Whois database on an individual Internet Protocol (IP) address basis, and we work with registrars to help ensure their services are not limited by any restriction placed on Whois. We provide near real-time updates for Whois services for the TLDs under our management. As information is updated in the registration database, it is propagated to the Whois servers for quick publication. These updates align with the near real-time publication of Domain Name System (DNS) information as it is updated in the registration database. This capability is important for the HEBREW_TRANSLITERATION_OF_.COM gTLD registry as it is Verisign's experience
that when DNS data is updated in near real time, so should Whois data be updated to reflect the registration specifics of those domain names.

Verisign's Whois response time has been less than 500 milliseconds for 95 percent of all Whois queries in .com, .net, .tv, and .cc. The response time in these TLDs, combined with our capacity, enables the Whois system to respond to up to 30,000 searches (or queries) per second for a total capacity of 2.6 billion queries per day.

The Whois software written by Verisign complies with RFC 3912. We use an advanced in-memory database technology to provide exceptional overall system performance and security. In accordance with RFC 3912, we provide a website at whois.nic. ⟨TLD⟩ that provides free public query-based access to the registration data.

We currently operate both thin and thick Whois systems.

Verisign commits to implementing a RESTful Whois service upon finalization of the relevant standards and protocols by the IETF (Internet Engineering Task Force).

Provided Functionalities for User Interface

To use the Whois service via port 43, the user enters the applicable parameter on the command line as illustrated here:

* For domain name: whois EXAMPLE.TLD

* For registrar: whois "registrar Example Registrar, Inc."

* For name server: whois "NS1.EXAMPLE.TLD" or whois "name server (IP address)"

To use the Whois service via the web-based directory service search interface:

* Go to http://whois.nic. ⟨TLD⟩

* Click on the appropriate button (Domain, Registrar, or Name Server)

* Enter the applicable parameter:
a. Domain name, including the TLD (e.g., EXAMPLE.TLD)
b. Full name of the registrar, including punctuation (e.g., Example Registrar, Inc.)
c. Full host name or the IP address (e.g., NS1.EXAMPLE.TLD or 198.41.3.39)

* Click on the Submit button.

Provisions to Ensure That Access Is Limited to Legitimate Authorized Users and Is in Compliance with Applicable Privacy Laws or Policies

To further promote reliable and secure Whois operations, Verisign has implemented rate-limiting characteristics within the Whois service software. For example, to prevent data mining or other

abusive behavior, the service can throttle a specific requestor if the query rate exceeds a configurable threshold. In addition, QoS technology enables rate limiting of queries before they reach the servers, which helps protect against denial of service (DoS) and distributed denial of service (DDoS) attacks.

Our software also permits restrictions on search capabilities. For example, wild card searches can be disabled. If needed, it is possible to temporarily restrict and/or block requests coming from specific IP addresses for a configurable amount of time. Additional features that are configurable in the Whois software include help files, headers and footers for Whois query responses, statistics, and methods to memory map the database. Furthermore, we are European Union (EU) Safe Harbor certified and have worked with European data protection authorities to address applicable privacy laws by developing a tiered Whois access structure that requires users who require access to more extensive data to (i) identify themselves, (ii) confirm that their use is for a specified purpose and (iii) enter into an agreement governing their use of the more extensive Whois data.

1.2 Relevant Network Diagrams

Figure 26-1 (see Attachment VRSN_.comHebrew_Q26 Figures for all figures in this response) provides a summary network diagram of the Whois service provided by Verisign. The figure details the configuration with one resolution/Whois site. For the HEBREW_TRANSLITERATION_OF_.COM gTLD, we provide Whois service from six of our 17 primary sites based on the proposed gTLD's traffic volume and patterns. A functionally equivalent resolution architecture configuration exists at each Whois site.

1.3 IT and Infrastructure Resources

Figure 26-2 summarizes the IT and infrastructure resources that Verisign uses to provision Whois services from Verisign primary resolution sites. As needed, virtual machines are created based on actual and projected demand.

1.4 Description of Interconnectivity with Other Registry Systems

Figure 26-3 provides a technical overview of Verisign's registry system, and shows how the Whois service component fits into this larger system and interconnects with other system components.

1.5 Frequency of Synchronization Between Servers

Synchronization between the SRS and the geographically distributed Whois resolution sites occurs approximately every three minutes. We use a two-part Whois update process to ensure Whois data is accurate and available. Every 12 hours an initial file is distributed to each resolution site. This file is a complete copy of all Whois data fields associated with each domain name under management. As interactions with the SRS cause the Whois data to be changed, these incremental changes are distributed to the resolution sites as an incremental file update. This incremental update occurs approximately every three minutes. When the new 12-hour full update is distributed, this file includes all past incremental updates. Our approach to frequency of synchronization between servers meets the Performance Specifications defined in Specification 10 of the Registry Agreement for new gTLDs.

2 TECHNICAL PLAN SCOPE/SCALE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

As an experienced backend registry provider, we have developed and use proprietary system scaling models to guide the growth of our TLD supporting infrastructure. These models direct our infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. We periodically update these models to account for the adoption of more capable and cost-effective

technologies.

Our scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the HEBREW_TRANSLITERATION_OF_.COM gTLD
with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to our scaling models, we derived the necessary infrastructure required to implement and sustain this gTLD. Cost related to this infrastructure is provided as “Total Critical Registry Function Cash Outflows” (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

As an experienced backend registry provider, we have developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. We routinely adjust these staffing models to account for new tools and process innovations. These models enable us to continually right-size our staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to our staffing models, we derived the necessary personnel levels required for this gTLD’s initial implementation and ongoing maintenance. Cost related to this infrastructure is provided as “Total Critical Registry Function Cash Outflows” (Template 1, Line IIb.G) within the Question 46 financial projections response.

We employ more than 1,040 individuals of which more than 775 comprise our technical work force. (Current statistics are publicly available in our quarterly filings.) Drawing from this pool of
on-hand and fully committed technical resources, we have maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving our ability to align personnel resource growth to the scale increases of our TLD service offerings.

We project we will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support Whois services:

* Application Engineers: 19
* Database Engineers: 3
* Quality Assurance Engineers: 11

To implement and manage the HEBREW_TRANSLITERATION_OF_.COM gTLD as described in this application, we scale, as needed, the size of each technical area now supporting our portfolio of TLDs. Consistent with our resource modeling, we periodically review the level of work to be performed and adjust staff levels for each technical area.

When usage projections indicate a need for additional staff, our internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all our TLDs instead of creating a new entity to manage only this proposed gTLD, we realize significant economies of scale and ensure our TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as we hold all contributing staff members accountable to the same procedures that guide our execution of the Internet’s largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, we afford new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 COMPLIANCE WITH RELEVANT RFC

Verisign’s Whois service complies with the data formats defined in Specification 4 of the

Registry Agreement. We will provision Whois services for registered domain names and associated data in the top-level domain (TLD). Our Whois services are accessible over Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6), via both Transmission Control Protocol (TCP) port 43 and a web-based directory service at whois.nic. ⟨TLD⟩ , which in accordance with RFC 3912, provides free public query-based access to domain name, registrar, and name server lookups. Our proposed Whois system meets all requirements as defined by ICANN for each registry under our management. Evidence of this successful implementation, and thus compliance with the applicable RFCs, can be verified by a review of the .com and .net Registry Operator's Monthly Reports that we file with ICANN. These reports provide evidence of our ability to meet registry operation service level agreements (SLAs) comparable to those detailed in Specification 10. The reports are accessible at the following URL: http://www.icann.org/en/tlds/monthly-reports/.

5 COMPLIANCE WITH SPECIFICATIONS 4 AND 10 OF REGISTRY AGREEMENT

In accordance with Specification 4, Verisign provides a Whois service that is available via both port 43 in accordance with RFC 3912, and a web-based directory service at whois.nic. ⟨TLD⟩ also in accordance with RFC 3912, thereby providing free public query-based access. We acknowledge that ICANN reserves the right to specify alternative formats and protocols, and upon such specification, we will implement such alternative specification as soon as reasonably practicable.

The format of the following data fields conforms to the mappings specified in Extensible Provisioning Protocol (EPP) RFCs 5730 – 5734 so the display of this information (or values returned in Whois responses) can be uniformly processed and understood: domain name status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers, email addresses, date, and times.

Specifications for data objects, bulk access, and lookups comply with Specification 4 and are detailed in the following subsections, provided in both bulk access and lookup modes.

Bulk Access Mode

This data is provided on a daily schedule to a party designated from time to time in writing by ICANN. The specification of the content and format of this data, and the procedures for providing access, shall be as stated below, until revised in the ICANN Registry Agreement.

The data is provided in three files:

* Domain Name File: For each domain name, the file provides the domain name, server name for each name server, registrar ID, and updated date.

* Name Server File: For each registered name server, the file provides the server name, each IP address, registrar ID, and updated date.

* Registrar File: For each registrar, the following data elements are provided: registrar ID, registrar address, registrar telephone number, registrar email address, Whois server, referral URL, updated date, and the name, telephone number, and email address of all the registrar's administrative, billing, and technical contacts.

Lookup Mode

Figures 26-4 through Figure 26-6 provide the query and response format for domain name, registrar, and name server data objects

5.1 Specification 10, RDDS Registry Performance Specifications

Verisign's Whois service meets all registration data directory services (RDDS) registry performance specifications detailed in Specification 10, Section 2. Evidence of this performance can be verified by a review of the .com and .net Registry Operator's Monthly Reports that we file

monthly with ICANN. These reports are accessible from the ICANN website at the following URL: http://www.icann.org/en/tlds/monthly-reports/.

In accordance with RDDS registry performance specifications detailed in Specification 10, our Whois service meets the following proven performance attributes:

* RDDS availability: Fewer than or equal to 864 min of downtime (approximately 98%)

* RDDS query RTT: Fewer than or equal to 2000 ms, for at least 95% of the queries

* RDDS update time: Fewer than or equal to 60 min, for at least 95% of the probes

6 SEARCHABLE WHOIS

Verisign provides a searchable Whois service for the HEBREW_TRANSLITERATION_OF_.COM gTLD. We have experience in providing tiered access to Whois for the .name registry, and we use these methods and control structures to help reduce potential malicious use of the function. The searchable Whois system currently uses Apache's Lucene full text search engine to index relevant Whois content with near-real time incremental updates from the provisioning system.

Features of our searchable Whois function include:

* Provision of a web-based searchable directory service

* Ability to perform partial match, at least, for the following data fields: domain name, contacts and registrant's name, and contact and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state, or province)

* Ability to perform exact match, at least, on the following fields: registrar ID, name server name, and name server's IP address (only applies to IP addresses stored by the registry, i.e., glue records)

* Ability to perform Boolean search supporting, at least, the following logical operators to join a set of search criteria: AND, OR, NOT

* Search results that include domain names that match the selected search criteria

Our implementation of searchable Whois is EU Safe Harbor certified and includes appropriate access control measures that help ensure that only legitimate authorized users can use the service. Furthermore, our compliance office monitors current ICANN policy and applicable privacy laws or policies to help ensure the solution is maintained within compliance of applicable regulations. Features of these access control measures include:

* All unauthenticated searches are returned as thin results.

* Registry system authentication is used to grant access to appropriate users for thick Whois data search results.

* Account access is granted by our defined HEBREW_TRANSLITERATION_OF_.COM gTLD admin user.

Potential Forms of Abuse and Related Risk Mitigation

Leveraging our experience providing tiered access to Whois for the .name registry and interacting with ICANN, data protection authorities, and applicable industry groups, we are knowledgeable of the likely data mining forms of abuse associated with a searchable Whois service. Figure 26-7 summarizes these
potential forms of abuse and our approach to mitigate the identified risk.

27. Registration Life Cycle

1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF REGISTRATION LIFECYCLES AND STATES

Verisign’s registry implements the full registration lifecycle for domain names supporting the operations in the Extensible Provisioning Protocol (EPP) specification. The registration lifecycle of the domain name starts with registration and traverses various states as specified in the following sections. The registry system provides options to update domain names with different server and client status codes that block operations based on the EPP specification. The system also provides different grace periods for different billable operations, where the price of the billable operation is credited back to the registrar if the billable operation is removed within the grace period. Together Figure 27-1 and Figure 27-2 (see Attachment VRSN_.comHebrew_Q27 Figures for all figures in this response) define the registration states comprising the registration lifecycle and explain the trigger points that cause state-to-state transitions. States are represented as green rectangles within Figure 27-1.

1.1 Registration Lifecycle of Create/Update/Delete

The following section details the create/update/delete processes and the related renewal process that we follow. For each process, this response defines the process function and its characterization, and as appropriate provides a process flow chart.

Create Process
The domain name lifecycle begins with a registration or what is referred to as a Domain Name Create operation in EPP. The system fully supports the EPP Domain Name Mapping as defined by RFC 5731, where the associated objects (e.g., hosts and contacts) are created independent of the domain name.

Process Characterization
The Domain Name Create command is received, validated, run through a set of business rules, persisted to the database, and committed in the database if all business rules pass. The domain name is included with the data flow to the DNS and Whois resolution services. If no name servers are supplied, the domain name is not included with the data flow to the DNS. A successfully created domain name has the created date and expiration date set in the database. Creates are subject to grace periods as described in Section 1.3 of this response.

The Domain Name Create operation (Figure 27-3) requires the following attributes:

* Domain name meets the string restrictions.
* Domain name does not already exist.
* Registrar is authorized to create a domain name in HEBREW_TRANSLITERATION_OF_.COM.
* Registrar has available credit.
* Authorization Information (Auth-Info) value is valid.
* Required contacts (e.g., registrant, administrative contact, technical contact, and billing contact) are specified and exist.
* Specified name servers (hosts) exist, and there is a maximum of 13 name servers.
* Period in units of years with a maximum value of 10 (default period is one year).

Renewal Process
The domain name can be renewed unless it has any form of Pending Delete, Pending Transfer, or Renew Prohibited.

A request for renewal that sets the expiry date to more than ten years in the future is denied. The registrar must pass the current expiration date (without the timestamp) to support the idempotent features of EPP, where sending the same command a second time does not cause unexpected side effects.

Automatic renewal occurs when a domain name expires. On the expiration date, the registry extends the registration period one year and debits the registrar account balance. In the case of an auto-renewal of the domain name, a separate Auto-Renew grace period applies. Renewals are subject to grace periods as described in Section 1.3 of this response.

Process Characterization

The Domain Name Renew command is received, validated, authorized, and run through a set of business rules. The data is updated and committed in the database if it passes all business rules. The updated domain name's expiration date is included in the flow to the Whois resolution service.

The Domain Name Renew operation (Figure 27-4) requires the following attributes:
* Domain name exists and is sponsored by the requesting registrar.
* Registrar is authorized to renew a domain name in HEBREW_TRANSLITERATION_OF_.COM.
* Registrar has available credit.
* Passed current expiration date matches the domain name's expiration date.
* Period in units of years with a maximum value of 10 (default period is one year). A domain name expiry past ten years is not allowed.

Registrar Transfer Procedures
A registrant may transfer the domain name from the current registrar to another registrar. The database system allows a transfer as long as the transfer is not within the initial 60 days, per industry standard, of the original registration date.

The registrar transfer process goes through many process states, which are described in detail below, unless it has any form of Pending Delete, Pending Transfer, or Transfer Prohibited.

A transfer can only be initiated when the appropriate Auth-Info is supplied. The Auth-Info for transfer is only available to the current registrar. Any other registrar requesting to initiate a transfer on behalf of a registrant must obtain the Auth-Info from the registrant.

The Auth-Info is available to the registrant upon request. The registrant is the only party other than the current registrar that has access to the Auth-Info. Registrar transfer entails a specified extension of the expiry date for the object. The registrar transfer is a billable operation and is charged identically to a renewal for the same extension of the period. This period can be from one to ten years, in one-year increments.

Because registrar transfer involves an extension of the registration period, the rules and policies applying to how the resulting expiry date is set after transfer are based on the renewal policies on extension.

Per industry standard, a domain name cannot be transferred to another registrar within the first 60 days after registration. This restriction continues to apply if the domain name is renewed during the first 60 days. Transfer of the domain name changes the sponsoring registrar of the domain name, and also changes the child hosts (ns1.sample.xyz) of the domain name (sample .xyz).

The domain name transfer consists of five separate operations:

* Transfer Request (Figure 27-5): Executed by a non-sponsoring registrar with the valid Auth-Info provided by the registrant. The Transfer Request holds funds of the requesting registrar but does not bill the registrar until the transfer is completed. The sponsoring registrar receives a Transfer Request poll message.
* Transfer Cancel (Figure 27-6): Executed by the requesting registrar to cancel the pending transfer. The held funds of the requesting registrar are reversed. The sponsoring registrar receives a Transfer Cancel poll message.
* Transfer Approve (Figure 27-7): Executed by the sponsoring registrar to approve the Transfer Request. The requesting registrar is billed for the Transfer Request and the sponsoring registrar is credited for an applicable Auto-Renew grace period. The requesting registrar receives a Transfer Approve poll message.
* Transfer Reject (Figure 27-8): Executed by the sponsoring registrar to reject the pending transfer. The held funds of the requesting registrar are reversed. The requesting registrar receives a Transfer Reject poll message.
* Transfer Query (Figure 27-9): Executed by either the requesting registrar or the sponsoring registrar of the last transfer.

The registry auto-approves a transfer if the sponsoring registrar takes no action. The requesting registrar is billed for the Transfer Request and the sponsoring registrar is credited for an applicable Auto-Renew grace period. The requesting registrar and the sponsoring registrar

receive a Transfer Auto-Approve poll message.

Delete Process
A registrar may choose to delete the domain name at any time.

Process Characterization
The domain name can be deleted, unless it has any form of Pending Delete, Pending Transfer, or Delete Prohibited.

A domain name is also prohibited from deletion if it has any in-zone child hosts that are name servers for domain names. For example, the domain name “sample.xyz” cannot be deleted if an in-zone host “ns.sample.xyz” exists and is a name server for “sample2.xyz.”

If the Domain Name Delete occurs within the Add grace period, the domain name is immediately deleted and the sponsoring registrar is credited for the Domain Name Create. If the Domain Name Delete occurs outside the Add grace period, it follows the Redemption grace period (RGP) lifecycle.

Update Process
The sponsoring registrar can update the following attributes of a domain name:

* Auth-Info
* Name servers
* Contacts
* Statuses (e.g., Client Delete Prohibited, Client Hold, Client Renew Prohibited, Client Transfer Prohibited, Client Update Prohibited)

Process Characterization
Updates are allowed provided that the update includes the removal of any Update Prohibited status. The Domain Name Update operation is detailed in Figure 27-10.

A domain name can be updated unless it has any form of Pending Delete, Pending Transfer, or Update Prohibited.

1.2 Pending, Locked, Expired, and Transferred

Verisign handles pending, locked, expired, and transferred domain names as described here. When the domain name is deleted after the five-day Add grace period, it enters into the Pending Delete state. The registrant can return its domain name to active any time within the five-day Pending Delete grace period. After the five-day Pending Delete grace period expires, the domain name enters the Redemption Pending state and then is deleted by the system. The registrant can restore the domain name at any time during the Redemption Pending state.

When a non-sponsoring registrar initiates the domain name transfer request, the domain name enters Pending Transfer state and a notification is mailed to the sponsoring registrar for approvals. If the sponsoring registrar doesn’t respond within five days, the Pending Transfer expires and the transfer request is automatically approved.

EPP specifies both client (registrar) and server (registry) status codes that can be used to prevent registry changes that are not intended by the registrant. Currently, many registrars use the client status codes to protect against inadvertent modifications that would affect their customers’ high-profile or valuable domain names.

Verisign’s registry service supports the following client (registrar) and server (registry) status codes:

* clientHold
* clientRenewProhibited
* clientTransferProhibited
* clientUpdateProhibited
* clientDeleteProhibited
* serverHold
* serverRenewProhibited

*	serverTransferProhibited
*	serverUpdateProhibited
*	serverDeleteProhibited

1.3	Add Grace Period, Redemption Grace Period, and Notice Periods for Renewals or Transfers

*	Add Grace Period: The Add grace period is a specified number of days following the initial registration of the domain name. The current value of the Add grace period for all registrars is five days.

*	Redemption Grace Period: If the domain name is deleted after the five-day grace period expires, it enters the Redemption grace period and then is deleted by the system. The registrant has an option to use the Restore Request command to restore the domain name within the Redemption grace period. In this scenario, the domain name goes to Pending Restore state if there is a Restore Request command within 30 days of the Redemption grace period. From the Pending Restore state, it goes either to the OK state, if there is a Restore Report Submission command within seven days of the Restore Request grace period, or a Redemption Period state if there is no Restore Report Submission command within seven days of the Restore Request grace period.

*	Renew Grace Period: The Renew/Extend grace period is a specified number of days following the renewal/extension of the domain name's registration period. The current value of the Renew/Extend grace period is five days.

*	Auto-Renew Grace Period: All auto-renewed domain names have a grace period of 45 days.

*	Transfer Grace Period: Domain names have a five-day Transfer grace period.

1.4	Aspects of the Registration Lifecycle Not Covered by Standard EPP RFCs

Our registration lifecycle processes and code implementations adhere to the standard EPP RFCs related to the registration lifecycle. By adhering to the RFCs, our registration lifecycle is complete and addresses each registration-related task comprising the lifecycle. No aspect of our registration lifecycle is not covered by one of the standard EPP RFCs and thus no additional definitions are provided in this response.

2	CONSISTENCY WITH ANY SPECIFIC COMMITMENTS MADE TO REGISTRANTS AS ADAPTED TO THE OVERALL BUSINESS APPROACH FOR THE PROPOSED gTLD

The registration lifecycle described above applies to the HEBREW_TRANSLITERATION_OF_.COM gTLD as well as other TLDs managed by Verisign; thus we remain consistent with commitments made to our registrants. No unique or specific registration lifecycle modifications or adaptations are required to support the overall business approach for the HEBREW_TRANSLITERATION_OF_.COM gTLD.

3	COMPLIANCE WITH RELEVANT RFCs

Our registration lifecycle complies with RFCs 5730 – 5734 and 3915. The system fully supports the EPP Domain Name Mapping (RFC 5731), where the associated objects (e.g., hosts and contacts) are created independent of the domain name.

In addition, in accordance with RFCs 5732 and 5733, the registration system enforces the following registration constraints:

*	Uniqueness/Multiplicity: A second-level domain name is unique in the HEBREW_TRANSLITERATION_OF_.COM database. Two identical second-level domain names cannot simultaneously exist in HEBREW_TRANSLITERATION_OF_.COM. Further, a second-level domain name cannot be created if it conflicts with a reserved domain name.

*	Point of Contact Associations: The domain name is associated with the following points of

contact. Contacts are created and managed independently according to RFC 5733.
a. Registrant
b. Administrative contact
c. Technical contact
d. Billing contact

* Domain Name Associations: Each domain name is associated with:
a. A maximum of 13 hosts, which are created and managed independently according to RFC 5732
b. An Auth-Info, which is used to authorize certain operations on the object
c. Status(es), which are used to describe the domain name's status in the registry
d. A created date, updated date, and expiry date

4 DEMONSTRATES THAT TECHNICAL RESOURCES REQUIRED TO CARRY THROUGH THE PLANS FOR THIS ELEMENT ARE ALREADY ON HAND OR READILY AVAILABLE

Verisign has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. These routinely adjusted models enable us to continually right-size staff to meet projected demand, service level agreements, and requirements for Internet security and stability. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to our staffing models, we derived the personnel levels required for this gTLD's initial implementation and ongoing maintenance. Cost related to this infrastructure is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 response.

We employ more than 1,040 individuals; more than 775 comprise our technical work force, enabling us to draw from this pool and align personnel resource growth to the scale increases of our TLD service offerings.

We expect to use the following personnel roles, which are described in Section 5 of the response to Question 31, to support the registration lifecycle:

* Application Engineers: 19
* Customer Support Personnel: 36
* Database Administrators: 8
* Database Engineers: 3
* Quality Assurance Engineers: 11
* SRS System Administrators: 13

To implement and manage the HEBREW_TRANSLITERATION_OF_.COM gTLD as described in this application, we scale, as needed, the size of each technical area now supporting our portfolio of TLDs. Consistent with our resource modeling, we periodically review the level of work to be performed and adjust staff levels for each technical area.

When usage projections indicate a need for additional staff, our internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all our TLDs instead of creating a new entity to manage only this proposed gTLD, we realize significant economies of scale and ensure our TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as we hold all contributing staff members accountable to the same procedures that guide our execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, we afford new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

28. Abuse Prevention and Mitigation

1. COMPREHENSIVE ABUSE POLICIES, WHICH INCLUDE CLEAR DEFINITIONS OF WHAT CONSTITUTES ABUSE IN THE TLD, AND PROCEDURES THAT WILL EFFECTIVELY MINIMIZE POTENTIAL FOR ABUSE IN THE TLD

Verisign has more than 16 years' experience in protecting our domains and Domain Name System (DNS) from malicious abuse, and we offer multiple services, products, and policies to combat abuse of the HEBREW_TRANSLITERATION_OF_.COM gTLD.

Definitions

Malicious abuse of the HEBREW_TRANSLITERATION_OF_.COM gTLD, where software is disseminated to infiltrate or damage a computer system without the owner's informed consent, can include the following types of abuse:

* Trojan / Malware Executable(s): A malicious executable is hosted on a server.

* Trojan / Malware Drive-By: A website is crafted such that it attempts to exploit a vulnerability in a browser or browser plugin (e.g., Flash, PDF, Java) for the purpose of automatically downloading and installing a malicious executable on a client machine.

* Phishing: A link in an email (often sent as spam) points to fraudulent web pages/ website (primarily Trojan / Malware Drive-By). These fraudulent web pages are designed to trick recipients into divulging sensitive data such as user names or passwords.

* Command-and-Control (CnC): A server is used to send and receive commands from infected machines (bots).

* Mass Registrations: Many different domain names are used as part of a CnC infrastructure. The domain names are linked to a specific malware family and are registered in close proximity to each other (time-wise) or by a common entity (malicious actor).

We offer a number of security services to protect registrants and minimize the potential for abuse. These products include:

* Verisign MalDetector: This new commercial service enables registrars to offer malware scanning to their customers. MalDetector analyzes a website's content by scanning the site's web pages (text, video, images, ads, web code) for malware and obfuscations (hidden malware code). If MalDetector detects malware code in the website content, it provides remediation instructions for removing the malicious code.

* Verisign Domain Name System Security Extensions (DNSSEC) Signing Service: This services helps registrars build the infrastructure capability to protect users from redirection to unintended sites while reducing the cost, complexity, and administrative burden associated with implementing DNSSEC.

* Verisign Registry Lock Service: This service enables registrars to offer server-level protection for registrants' HEBREW_TRANSLITERATION_OF_.COM domain name records, thereby guarding against unintended changes, deletions, or transfers. These modification may result in malicious use of the domain name.

* Verisign Registry-Registrar Two-Factor Authentication: Helps registrars better manage and control communications with the Verisign registry by providing a mechanism to validate that requested changes come from authorized personnel and update authorized contacts as personnel changes occur.

In the case of other forms of illegal activity, we work with law enforcement personnel, as needed, to mitigate abuse through the judicial system.

1.1 Abuse Prevention and Mitigation Implementation Plan

The security services described in the preceding section are currently implemented in the other TLDs that Verisign operates. These services are available immediately to the HEBREW_TRANSLITERATION_OF_.COM gTLD, without the need for additional implementation.

The HEBREW_TRANSLITERATION_OF_.COM gTLD is added to the root zone, and second-level domain names are provisioned through Verisign's Shared Registration System

(SRS). Registrars have the HEBREW_TRANSLITERATION_OF_.COM gTLD and the products and services described in this application added to their account in the SRS. Registrars are required to complete a ramp-up period during which they test their Extensible Provisioning Protocol (EPP) client applications and services through our Operational Test Environment (OTE). The OTE is a functional equivalent to the production environment that allows registrars to determine whether their client applications are production ready. Once the registrar has completed the testing and certification of its client applications and services, it is granted access to the production environment and may begin processing domain names registrations to be published in the HEBREW_TRANSLITERATION_OF_.COM gTLD zone.

1.2 Policies for Handling Complaints Regarding Abuse

Verisign handles complaints regarding abuse as detailed in this section.

Abuse complaints are initially addressed to the Registrar of Record (ROR). If registrars or registrants need to escalate an abuse complaint, our Customer Service Center (CSC) is the initial point of contact. Our Customer Support includes the ²⁴/₇ onsite CSC staff and on-call support from Tier 3 teams (e.g., registry operations staff, engineers, and developers) during non-business hours. Our primary concern is to resolve issues quickly. As such, we maintain a formal escalation process to ensure that all issues are addressed promptly by the appropriate person/teams.

Abuse complaints are first directed to the Verisign CSC, which manages the complaint through the processes outlined in Section 3.2.2. Our CSC provides world-class support to our customers with key performance metrics that support a timely response to customer issues, including complaints of abuse. Team leads actively manage all access channels to ensure appropriate responsiveness via each access channel.

1.3 Proposed Measures for Removal of Orphan Glue Records

Although orphan glue records may support correct and ordinary operation of the Domain Name System (DNS), registry operators are required to remove orphan glue records (as defined at http://www.icann.org/en/committees/security/sac048.pdf) when provided with evidence in written form that such records are present in connection with malicious conduct. Verisign's registration system is specifically designed to not allow orphan glue records. Registrars are required to delete/move all dependent DNS records before deleting the parent domain name.

To prevent orphan glue records, we perform the following checks before removing a domain or name server:

Checks during domain delete:

* A parent domain name deletion transaction is not allowed if any other domain name in the zone refers to the child name server.

* If the parent domain name is the only domain name using the child name server, then both the domain name and the glue record are removed from the zone.

Check during explicit name server delete:

* We confirm that the current name server is not referenced by any in-zone domain name before deleting the name server.

Zone-file impact:

* If the parent domain name references the child name server AND if other domain names in the zone also reference it AND if the parent domain name is assigned a serverHold status, then the parent domain name is removed from the zone file, but the name server glue record is not.

* If no domain names reference a name server, then the zone file removes the glue record.

1.4 Resourcing Plans

Details related to resourcing plans for the initial implementation and ongoing maintenance of our abuse plan are provided in Section 2 of this response.

1.5 Measures to Promote Whois Accuracy

Verisign performs periodic Whois reviews to verify accuracy and completeness of data for which the registry is authoritative. For data maintained in the registry database for which the registry is not authoritative and is therefore unable to verify registrant contact data, the registry validates the syntax and completeness of all required contact fields during registration and modification transactions. In addition, we coordinate with the respective registrars to promote accuracy of these data, including periodic notifications of ICANN's Whois Data Reminder Policy.

1.5.1 Authentication of Registrant Information

Authentication of registrant information is performed by the registrant's registrar, since the registry has no direct relationship with the registrant. The registration rules for HEBREW_TRANSLITERATION_OF_.COM require creation of an AuthInfo code for each domain name. This AuthInfo code is required to initiate a request to transfer the domain name between registrars. Use of this authorization by the gaining registrar is intended to prevent unauthorized transfers of domain names.

1.5.2 Regular Monitoring of Registration Data for Accuracy and Completeness

Verisign has established policies and procedures to encourage registrar compliance with ICANN's Whois accuracy requirements. We incorporate the following services into our full-service registry operations.

Registrar Self Certification

Our self-certification program consists, in part, of evaluations applied equally to all operational ICANN accredited registrars and conducted from time to time throughout the year. Process steps are as follows:

* Verisign sends an email notification to the ICANN primary registrar contact, requesting that the contact go to a designated URL, log in with his/her Web ID and password, and complete and submit the online form. The contact must submit the form within 15 business days of receipt of the notification.

* When the form is submitted, we send the registrar an automated email confirming that the form was successfully submitted.

* We review the submitted form to ensure the certifications are compliant.

* We send the registrar an email notification if the registrar is found to be compliant in all areas.

* If a review of the response indicates that the registrar is out of compliance or if we have follow-up questions, the registrar has 10 days to respond to the inquiry.

* If the registrar does not respond within 15 business days of receiving the original notification, or if it does not respond to the request for additional information, we send the registrar a Breach Notice and give the registrar 30 days to cure the breach.

* If the registrar does not cure the breach, we terminate the Registry-Registrar Agreement (RRA).

Whois Data Reminder Process

Verisign regularly reminds registrars of their obligation to comply with ICANN's Whois Data Reminder

Policy, which was adopted by ICANN as a consensus policy on 27 March 2003 (http://www.icann.org/en/registrars/wdrp.htm). We send a notice to all registrars once a year reminding them of their obligation to be diligent in validating the Whois information provided during the registration process, to investigate claims of fraudulent Whois information, and to cancel domain name registrations for which Whois information is determined to be invalid.

1.6 Malicious or Abusive Behavior Definitions, Metrics, and Service Level Requirements for Resolution

Please see Section 1.0 for the definition of potential forms of abuse specific to the HEBREW_TRANSLITERATION_OF_.COM gTLD. See Section 3.2.2 for a definition of Verisign's response procedures.

The initial response from Customer Service is within 20 seconds or less for 90% of phone calls. Verification of malicious activity and removal of confirmed malicious infections is completed within 24 hours.

1.7 Controls to Ensure Proper Access to Domain Functions

The following sections describe various controls that Verisign employs to ensure appropriate access to domain functions.

1.7.1 Multi-Factor Authentication

To ensure proper access to domain functions, we incorporate our Registry-Registrar Two-Factor Authentication Service into our full-service registry operations. The service is designed to improve domain name security and assist registrars in protecting the accounts they manage by providing another level of assurance that only authorized personnel can communicate with the registry. As part of the service, dynamic one-time passwords (OTPs) augment the user names and passwords currently used to process update, transfer, and/or deletion requests. These OTPs enable transaction processing to be based on requests that are validated both by "what users know" (i.e., their user name and password) and "what users have" (i.e., a two-factor authentication credential with a one-time-password).

Registrars can use the OTP when communicating directly with our Customer Service department as well as when using the registrar portal to make manual updates, transfers, and/or deletion transactions. The Two-Factor Authentication Service is an optional service offered to registrars that execute the Registry-Registrar Two-Factor Authentication Service Agreement. As shown in Figure 28-1 (see Attachment VRSN_.comHebrew_Q28 Figures for all figures in this response), the registrars' authorized contacts use the OTP to enable strong authentication when they contact the registry. There is no charge for the Registry-Registrar Two-Factor Authentication Service. It is enabled only for registrars that wish to take advantage of the added security provided by the service.

1.7.2 Requiring Multiple, Unique Points of Contact

Each user of the system is required to have an account established with a responsibility role assigned to him/her. The authoritative contact for the account is the ICANN Primary Contact. In addition to the Administrative Contact, the following roles are available: Billing, Technical, Legal, Marketing, Administrative, CEO, and Technical $^{24}/_{7}$. Only one user is designated as the ICANN Primary and, as such, is the authoritative contact on the account should any conflict arise.

2. TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

As an experienced backend registry provider, we have developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. We routinely adjust these staffing models to account for new tools and process innovations. These models enable us to continually right-size our staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the

projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to our staffing models, we derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Cost related to this infrastructure is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

We employ more than 1,040 individuals of which more than 775 comprise our technical work force. (Current statistics are publicly available in our quarterly filings.)

We project we will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support abuse prevention and mitigation:

* Application Engineers: 19
* Business Continuity Personnel: 3
* Customer Affairs Organization: 9
* Customer Support Personnel: 36
* Information Security Engineers: 11
* Network Administrators: 11
* Network Architects: 4
* Network Operations Center (NOC) Engineers: 33
* Project Managers: 25
* Quality Assurance Engineers: 11
* Systems Architects: 9

To implement and manage the HEBREW_TRANSLITERATION_OF_.COM gTLD as described in this application, we scale, as needed, the size of each technical area now supporting our portfolio of TLDs. Consistent with our resource modeling, we periodically review the level of work to be performed and adjust staff levels for each technical area.

When usage projections indicate a need for additional staff, our internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all our TLDs instead of creating a new entity to manage only this proposed gTLD, we realize significant economies of scale and ensure our TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD. Moreover, by augmenting existing teams, we afford new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

3. POLICIES AND PROCEDURES IDENTIFY AND ADDRESS THE ABUSIVE USE OF REGISTERED NAMES AT STARTUP AND ON AN ONGOING BASIS

3.1 Start-Up Anti-Abuse Policies and Procedures

We incorporate the following domain name abuse prevention service into our full-service registry operations. This service is available at the time of domain name registration.

Registry Lock

The Registry Lock Service allows registrars to offer server-level protection for their registrants' domain names. A registry lock can be applied during the initial standup of the domain name or at any time that the registry is operational.

Specific EPP status codes are set on the domain name to prevent malicious or inadvertent modifications, deletions, and transfers. Typically, these 'server' level status codes can only be updated by the registry. The registrar only has 'client' level codes and cannot alter 'server' level status codes. The registrant must provide a pass phrase to the registry before any updates are made to the domain name. However, with Registry Lock, registrars can also take advantage of server status codes.

The following EPP server status codes are applicable for domain names: (i) serverUpdateProhibited, (ii) serverDeleteProhibited, and (iii) serverTransferProhibited. These statuses may be applied individually or in combination.

The EPP also enables setting host (i.e., name server) status codes to prevent deleting or renaming a host or modifying its IP addresses. Setting host status codes at the registry reduces the risk of inadvertent disruption of DNS resolution for domain names.

The Registry Lock Service is used in conjunction with a registrar's proprietary security measures to bring a greater level of security to registrants' domain names and help mitigate potential for unintended deletions, transfers, and/or updates.

Two components comprise the Registry Lock Service:

* Registrars provide Verisign with a list of the domain names to be placed on the server status codes. During the term of the service agreement, the registrar can add domain names to be placed on the server status codes and/or remove domain names currently placed on the server status codes. We then manually authenticate that the registrar submitting the list of domain names is the registrar of record for such domain names.

* If registrars require changes (including updates, deletes, and transfers) to a domain name placed on a server status code, we follow a secure, authenticated process to perform the change. This process includes a request from a registrar-authorized representative for Verisign to remove the specific registry status code, validation of the authorized individual by Verisign, removal of the specified server status code, registrar completion of the desired change, and a request from the registrar-authorized individual to reinstate the server status code on the domain name. This process is designed to complement automated transaction processing through the Shared Registration System (SRS) by using independent authentication by trusted registry experts.

3.2 Ongoing Anti-Abuse Policies and Procedures

3.2.1 Policies and Procedures That Identify Malicious or Abusive Behavior

We incorporate the following service into our full-service registry operations.

Malware Scanning Service

Registrants are often unknowing victims of malware exploits. We have developed proprietary code to help identify malware in the zones we manage, which in turn helps us to identify malicious code hidden in HEBREW_TRANSLITERATION_OF_.COM domain names.

MalDetector, our malware scanning service, helps prevent HEBREW_TRANSLITERATION_OF_.COM websites from infecting other websites by scanning web pages for embedded malicious content that will infect visitors' websites. Our malware scanning technology uses a combination of in-depth malware behavioral analysis, anti-virus results, detailed malware patterns, and network analysis to discover known exploits for the particular scanned zone. If malware is detected, the service sends the registrant a report that contains the number of malicious domain names found and details about malicious content within its TLD zones. Reports with remediation instructions are provided to help the response team quickly and effectively remove the malicious code.

3.2.2 Policies and Procedures That Address the Abusive Use of Registered Names

Suspension Processes

In the case of domain name abuse, Verisign verifies the nature of the abuse and remediates the abuse using the procedures detailed in this section and in Figure 28-2.

Step 1.1: Verisign Notification. External party escalates the abuse notification to Verisign for processing, documented by:

* Threat domain name

* Registrar of record (ROR)Incident narrative, threat analytics, screen shots to depict abuse,

and/or other evidence

* Threat classification

* Recommended timeframe for action

* Technical details (e.g., Whois records, IP addresses, hash values, anti-virus detection results/nomenclature, name servers, domain name statuses that are relevant to the suspension)

* Contact details (e.g. name, phone, email address)

* Escalation history (initial timeframe of report to ROR, response from ROR, and so on)

Step 1.2: Registry Notification Verification. When we receive a request for escalation from an external party, we perform the following verification procedures:

* Validate that all the required data appears in the notification.
* Validate that the request for escalation is for a registered domain name.
* Return a case number for tracking purposes.

Step 1.3: Escalation Rejection. If required data is missing from the request for escalation, or the domain name is not registered, the request will be rejected and returned to the external party with the following information:

* Threat domain name
* Verisign case number
* Error reason

Step 1.4: Registrar Notification. Once we have performed the verification, we notify the registrar of the issue. Registrar notification includes the following information:

* Threat domain name
* Verisign case number
* Classification of type of domain name abuse
* Evidence of abuse
* Verisign anti-abuse contact name and number

Step 1.5: Registrant Notification. Once the registrar receives the notification from Verisign, it may, at its discretion, notify the registrant and/or take any appropriate action.

Step 1.6: Website/Domain Cleanup. We may work with the registrar to complete the following steps:

* Remediation steps: The registrar performs the remediation, and can elect to have us deploy MalDetector, our malware scanning service, to determine the remediation needed to remove the malware.

* Additional action needed: We provide additional comments to the registrar or information to contact the Internet service provider (ISP) or hosting company for additional action.

Step 1.7: Cleanup Acknowledgement. We notify the external party that the abuse cleanup has been completed. Acknowledgement of the cleanup includes the following information:

* Threat domain name
* Verisign case number
* Domain name
* Verisign abuse contact name and number
* Cleanup status

4. WHEN EXECUTED IN ACCORDANCE WITH THE REGISTRY AGREEMENT, PLANS WILL RESULT IN COMPLIANCE WITH CONTRACTUAL REQUIREMENTS

All Verisign abuse mitigation policies are based on the corresponding terms in the Registry Agreement and the Registry-Registrar Agreement as applicable. Whenever we develop a policy, we look first at the language of our agreements to determine what we can and cannot do. We then structure policies that are based on these determinations and appropriate stakeholders, such as registrars, to develop policies with processes to monitor compliance with the policies.

In addition, ICANN recently asked us to participate (along with some other registries) in its 2011 Pilot Registry Self-Assessment. We are willingly cooperating with this pilot, for which we provide ICANN with our certification that we comply with specific terms of our Registry Agreements (as identified by ICANN).

5. TECHNICAL PLAN SCOPE/SCALE THAT IS CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

We have developed and use proprietary system scaling models to guide the growth of our TLD supporting infrastructure. These models direct our infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. We periodically update these models to account for the adoption of more capable and cost-effective technologies.

Our scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the HEBREW_TRANSLITERATION_OF_.COM gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to our scaling models, we derived the necessary infrastructure required to implement and sustain this gTLD. Cost related to this infrastructure is provided as “Other Operating Cost” (Template 1, Line I.L) within the Question 46 financial projections response.

29. Rights Protection Mechanisms

1 MECHANISMS DESIGNED TO PREVENT ABUSIVE REGISTRATIONS

Rights protection is a core objective of Verisign. We will implement and adhere to any rights protection mechanisms (RPMs) that may be mandated from time to time by ICANN, including each mandatory RPM set forth in the Trademark Clearinghouse model contained in the Registry Agreement, specifically Specification 7. We acknowledge that, at a minimum, ICANN requires a Sunrise period, a Trademark Claims period, and interaction with the Trademark Clearinghouse with respect to the registration of domain names for the HEBREW_TRANSLITERATION_OF_.COM gTLD. It should be noted that because ICANN, as of the time of this application submission, has not issued final guidance with respect to the Trademark Clearinghouse, we cannot fully detail the specific implementation of the Trademark Clearinghouse within this application. We will adhere to all processes and procedures to comply with ICANN guidance once this guidance is finalized.

As described in this response, we implement a Sunrise period and Trademark Claims service with respect to the registration of domain names within the HEBREW_TRANSLITERATION_OF_.COM gTLD. Certain aspects of the Sunrise period and/or Trademark Claims service may be administered on behalf of Verisign by Verisign-approved registrars depending on final implementation specification detail related to the Trademark Clearinghouse.

Sunrise Service

We implement a Sunrise service procedure for at least 30 days prior to launch of the general registration of domain names in the HEBREW_TRANSLITERATION_OF_.COM gTLD as

provided by the Trademark Clearinghouse model set forth in the ICANN Applicant Guidebook. The HEBREW_TRANSLITERATION_OF_.COM Sunrise service will comply with the requirements outlined in the current Applicant Guidebook as well as any final guidance to be issued pertaining to the operation of the Trademark Clearinghouse.

Trademark Claims Service

We also implement a Trademark Claims service for at least 60 days after the launch of the general registration of domain names in the HEBREW_TRANSLITERATION_OF_.COM gTLD. The HEBREW_TRANSLITERATION_OF_.COM Trademark Claims service will comply with the requirements outlined in the current Applicant Guidebook as well as any final guidance to be issued pertaining to the operation of the Trademark Clearinghouse.

2 MECHANISMS DESIGNED TO IDENTIFY AND ADDRESS THE ABUSIVE USE OF REGISTERED NAMES ON AN ONGOING BASIS

In addition to the Sunrise and Trademark Claims services described in Section 1 of this response, we implement and adhere to RPMs post-launch as mandated by ICANN, and we confirm that registrars accredited for the HEBREW_TRANSLITERATION_OF_.COM gTLD are in compliance with these mechanisms. Certain aspects of these post-launch RPMs may be administered on behalf of Verisign by Verisign-approved registrars.

These post-launch RPMs include the established Uniform Domain-Name Dispute-Resolution Policy (UDRP), as well as the newer Uniform Rapid Suspension System (URS) and Trademark Post-Delegation Dispute Resolution Procedure (PDDRP). Where applicable, Verisign implements all determinations and decisions issued under the corresponding RPM.

After a domain name is registered, trademark holders can object to the registration through the UDRP or URS. Objections to the operation of the gTLD can be made through the PDDRP.

The following descriptions provide implementation details of each post-launch RPM for the HEBREW_TRANSLITERATION_OF_.COM gTLD:

* UDRP: The UDRP provides a mechanism for complainants to object to domain name registrations. The complainant files its objection with a UDRP provider and the domain name registrant has an opportunity to respond. The UDRP provider makes a decision based on the papers filed. If the complainant is successful, ownership of the domain name registration is transferred to the complainant. If the complainant is not successful, ownership of the domain name remains with the domain name registrant. Verisign and entities operating on our behalf adhere to all decisions rendered by UDRP providers.

* URS: We also provide for a Uniform Rapid Suspension (URS) system as specified in the Applicant Guidebook. Similar to the UDRP, a complainant files its complaint with a URS provider. The URS provider conducts an administrative review for compliance with applicable filing requirements. If the complaint passes administrative review, the URS provider sends Verisign, the registry operator for HEBREW_TRANSLITERATION_OF_.COM, a Notice of Complaint. Within 24 hours of receipt of the Notice of Complaint, we place the subject domain name on “lock,” (serverUpdateProhibited, serverTransferProhibited, and serverDeleteProhibited) which restricts all changes to the registration data but allows the name to continue to resolve. After the domain name is placed on lock, the URS provider notifies the registrant of the complaint. The registrant is then given an opportunity to respond. The URS provider must then conduct a review of the complaint and response based on the rules outlined in the Uniform Rapid Suspension System Draft Procedures set forth in the Applicant Guidebook. If the complainant is successful, the registry operator is informed and the domain name is suspended for the balance of the registration period; the domain name will not resolve to the original website, but to an informational web page provided by the URS provider. If the complainant is not successful, the lock is removed and full control of the domain name registration is returned to the domain name registrant. Similar to the existing UDRP, Verisign and entities operating on our behalf adhere to the decisions rendered by the URS providers.

* PDDRP: As provided in the Applicant Guidebook, all registries are required to implement the PDDRP. The PDDRP provides a mechanism for a complainant to object to the registry operator’s manner of operation or use of the gTLD. The complainant files its objection with a

PDDRP provider, who performs a threshold review. The registry operator has the opportunity to respond and the provider issues its determination based on the papers filed, although there may be opportunity for further discovery and a hearing. Verisign participates in the PDDRP process for the HEBREW_TRANSLITERATION_OF_.COM gTLD as specified in the Applicant Guidebook.

Additional Measures Specific to Rights Protection

We provide additional measures against potentially abusive registrations. These measures help mitigate phishing, pharming, and other Internet security threats. The measures exceed the minimum requirements for RPMs defined by Specification 7 of the Registry Agreement and are available at the time of registration. These measures include:

* Rapid Takedown or Suspension Based on Court Orders: We comply promptly with any order from a court of competent jurisdiction that directs us to take any action on a domain name that is within our technical capabilities as a TLD registry. These orders may be issued when abusive content, such as child pornography, counterfeit goods, or illegal pharmaceuticals, is associated with the domain name.

* Anti-Abuse Process: We implement an anti-abuse process that is executed based on the type of domain name action requested. These actions are coordinated with the domain name's registrar of record. The anti-abuse process is for malicious exploitation of the DNS infrastructure, such as phishing, botnets, and malware.

* Authentication Procedures: We use two-factor authentication to augment security protocols for telephone, email, and chat communications.

* Registry Lock: This Verisign service allows registrants to lock a domain name at the registry level to protect against both unintended and malicious changes, deletions, and transfers. Only Verisign, as the registry operator, can release the lock; thus all other entities that normally are permitted to update Shared Registration System (SRS) records are prevented from doing so. This lock is released only after the registrar request to unlock is validated.

* Malware Code Identification: This safeguard reduces opportunities for abusive behaviors that use registered domain names in the gTLD. Registrants are often unknowing victims of malware exploits. As a backend registry services provider, we have developed proprietary code to help identify malware in the zones we manage, which in turn helps registrars by identifying malicious code hidden in their domain names.

* DNSSEC Signing Service: Domain Name System Security Extensions (DNSSEC) helps mitigate pharming attacks that use cache poisoning to redirect unsuspecting users to fraudulent websites or addresses. It uses public key cryptography to digitally sign DNS data when it comes into the system and then validate it at its destination. The HEBREW_TRANSLITERATION_OF_.COM gTLD is DNSSEC-enabled as part of our core backend registry services.

* Commingling Restriction: If the Language Tag specified in the IDN registration is not from an approved language authorities table, and so does not have a List of Included Characters, then Verisign applies a restriction to prevent commingling of different scripts in a single domain. That is, if an IDN contains code points from two or more Unicode scripts, then that IDN registration is rejected. For example, a character from the Latin script cannot be used in the same IDN with any HEBREW character. All code points within an IDN must come from the same Unicode script. This is done to prevent confusable code points from appearing in the same IDN.

3. RESOURCING PLANS

As an experienced registry operator, we have developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. We routinely adjust these staffing models to account for new tools and process innovations. These models enable us to continually right-size our staff to accommodate projected demand and

meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to our staffing models, we derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance.

We employ more than 1,040 individuals of which more than 775 comprise our technical work force. (Current statistics are publicly available in our quarterly filings.) Drawing from this pool of
on-hand and fully committed technical resources, we have maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving our ability to align personnel resource growth to the scale increases of our TLD service offerings.

We project we will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support the implementation of RPMs:

* Customer Affairs Organization: 9
* Customer Support Personnel: 36
* Information Security Engineers: 11

To implement and manage the HEBREW_TRANSLITERATION_OF_.COM gTLD as described in this application, we scale, as needed, the size of each technical area now supporting our portfolio of TLDs. Consistent with our resource modeling, we periodically review the level of work to be performed and adjust staff levels for each technical area.

When usage projections indicate a need for additional staff, our internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all our TLDs instead of creating a new entity to manage only this proposed gTLD, we realize significant economies of scale and ensure our TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as we hold all contributing staff members accountable to the same procedures that guide our execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, we afford new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

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

1 DETAILED DESCRIPTION OF PROCESSES AND SOLUTIONS DEPLOYED TO MANAGE LOGICAL SECURITY ACROSS INFRASTRUCTURE AND SYSTEMS, MONITORING AND DETECTING THREATS AND SECURITY VULNERABILITIES AND TAKING APPROPRIATE STEPS TO RESOLVE THEM

Verisign's comprehensive security policy has evolved over the years as part of managing some of the world's most critical TLDs. Our Information Security Policy is the primary guideline that sets the baseline for all other policies, procedures, and standards that we follow. This security policy addresses all of the critical components for the management of backend registry services, including architecture, engineering, and operations.

Our general security policies and standards with respect to these areas are provided as follows:

Architecture

* Information Security Architecture Standard: This standard establishes the Verisign standard for application and network architecture. The document explains the methods for segmenting application tiers, using authentication mechanisms, and implementing application functions.

* Information Security Secure Linux Standard: This standard establishes the information security requirements for all systems that run Linux throughout the Verisign organization.

* Information Security Secure Oracle Standard: This standard establishes the information security requirements for all systems that run Oracle throughout the Verisign organization.

* Information Security Remote Access Standard: This standard establishes the information security requirements for remote access to terminal services throughout the Verisign organization.

* Information Security SSH Standard: This standard establishes the information security requirements for the application of Secure Shell (SSH) on all systems throughout the Verisign organization.

Engineering

* Secure SSL/TLS Configuration Standard: This standard establishes the information security requirements for the configuration of Secure Sockets Layer/Transport Layer Security (SSL/TLS) for all systems throughout the Verisign organization.

* Information Security C++ Standards: These standards explain how to use and implement the functions and application programming interfaces (APIs) within C++. The document also describes how to perform logging, authentication, and database connectivity.

* Information Security Java Standards: These standards explain how to use and implement the functions and APIs within Java. The document also describes how to perform logging, authentication, and database connectivity.

Operations

* Information Security DNS Standard: This standard establishes the information security requirements for all systems that run DNS systems throughout the Verisign organization.

* Information Security Cryptographic Key Management Standard: This standard provides detailed information on both technology and processes for the use of encryption on Verisign information security systems.

* Secure Apache Standard: We have a multitude of Apache web servers, which are used in both production and development environments on the Verisign intranet and on the Internet. They provide a centralized, dynamic, and extensible interface to various other systems that deliver information to the end user. Because of their exposure and the confidential nature of the data that these systems host, adequate security measures must be in place. The Secure Apache Standard establishes the information security requirements for all systems that run Apache web servers throughout the Verisign organization.

* Secure Sendmail Standard: We use sendmail servers in both the production and development environments on the Verisign intranet and on the Internet. Sendmail allows users to communicate with one another via email. The Secure Sendmail Standard establishes the information security requirements for all systems that run sendmail servers throughout the Verisign organization.

* Secure Logging Standard: This standard establishes the information security logging requirements for all systems and applications throughout the Verisign organization. Where specific standards documents have been created for operating systems or applications, the logging standards have been detailed. This document covers all technologies.

* Patch Management Standard: This standard establishes the information security patch and upgrade management requirements for all systems and applications throughout Verisign.

General

* Secure Password Standard: Because passwords are the most popular and, in many cases, the sole mechanism for authenticating a user to a system, great care must be taken to help ensure that passwords are “strong” and secure. The Secure Password Standard details requirements for the use and implementation of passwords.

* Secure Anti-Virus Standard: Verisign must be protected continuously from computer viruses and other forms of malicious code. These threats can cause significant damage to the overall operation and security of the Verisign network. The Secure Anti-Virus Standard describes the requirements for minimizing the occurrence and impact of these incidents.

Security processes and solutions for the HEBREW_TRANSLITERATION_OF_.COM gTLD are based on the standards defined above, each of which is derived from our experience and industry best practice. These standards comprise the framework for the overall security solution and applicable processes implemented across all products under our management. The security solution and applicable processes include, but are not limited to:

* System and network access control (e.g., monitoring, logging, and backup)

* Independent assessment and periodic independent assessment reports

* Denial of service (DoS) and distributed denial of service (DDoS) attack mitigation

* Computer and network incident response policies, plans, and processes

* Minimization of risk of unauthorized access to systems or tampering with registry data

* Intrusion detection mechanisms, threat analysis, defenses, and updates

* Auditing of network access

* Physical security

Further details of these processes and solutions are provided in Part B of this response.

1.1 Security Policy and Procedures for the Proposed Registry

Specific security policy related details, requested as the bulleted items of Question 30 – Part A, are provided here.

Independent Assessment and Periodic Independent Assessment Reports

To help ensure effective security controls are in place, we conduct a yearly American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) SAS 70 audit on all of our data centers, hosted systems, and applications. During these SAS 70 audits, security controls at the operational, technical, and human level are rigorously tested. These audits are conducted by a certified and accredited third party and help ensure that Verisign in-place environments meet the security criteria specified in our customer contractual agreements and are in accordance with commercially accepted security controls and practices. We also perform numerous audits throughout the year to verify our security processes and activities. These audits cover many different environments and technologies and validate our capability to protect our registry and DNS resolution environments. Figure 30A-1 (see Attachment VRSN_.comHebrew_Q30A_Figures for all figures in this response) lists a subset of the audits that Verisign conducts. For each audit program or certification listed in Figure 30A-1, we have included, as attachments to the Part B component of this response, copies of the assessment reports conducted by the listed third-party auditor. (See VRSN_.comHebrew_Q30B-1_Attachment_SAS70; VRSN_.comHebrew_Q30B-2_Attachment_KPMGSysTrust; VRSN_.comHebrew _Q30B-3_Attachment_KPMG 10K; and VRSN_.comHebrew_Q30B-4_Attachment_InfoSecPolicy.)

From our experience operating registries, we have determined that together these audit programs and certifications provide a reliable means to ensure effective security controls are in place and that these controls are sufficient to meet ICANN security requirements and therefore are commensurate with the guidelines defined by ISO 27001.

Augmented Security Levels or Capabilities

See Section 5 of this response.

Commitments Made to Registrants Concerning Security Levels
See Section 4 of this response.

2 SECURITY CAPABILITIES ARE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

As an experienced backend registry provider, we have developed and use proprietary system scaling models to guide the growth of our TLD supporting infrastructure. These models direct our infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. We periodically update these models to account for the adoption of more capable and cost-effective technologies.

Our scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the HEBREW_TRANSLITERATION_OF_.COM gTLD
with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to our scaling models, we derived the necessary infrastructure required to implement and sustain this gTLD. Cost related to this infrastructure is provided as “Total Critical Registry Function Cash Outflows” (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

As an experienced backend registry provider, we have developed and use a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. We routinely adjust these staffing models to account for new tools and process innovations. These models enable us to continually right-size our staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to our staffing models, we derived the necessary personnel levels required for this gTLD’s initial implementation and ongoing maintenance. Cost related to this infrastructure is provided as “Total Critical Registry Function Cash Outflows” (Template 1, Line IIb.G) within the Question 46 financial projections response.

We employ more than 1,040 individuals of which more than 775 comprise our technical work force. (Current statistics are publicly available in our quarterly filings.) Drawing from this pool of
on-hand and fully committed technical resources, we have maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving our ability to align personnel resource growth to the scale increases of our TLD service offerings.

We project we will use the following personnel role, which is described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support our security policy:

* Information Security Engineers: 11

To implement and manage the HEBREW_TRANSLITERATION_OF_.COM gTLD as described in this application, we

scale, as needed, the size of each technical area now supporting our portfolio of TLDs. Consistent with our resource modeling, we periodically review the level of work to be performed and adjust staff levels for each technical area.

When usage projections indicate a need for additional staff, our internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all our TLDs instead of creating a new entity to manage only this proposed gTLD, we realize significant economies of scale and ensure our TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as we hold all contributing staff members accountable to the same procedures that guide our execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, we afford new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 SECURITY MEASURES ARE CONSISTENT WITH ANY COMMITMENTS MADE TO REGISTRANTS REGARDING SECURITY LEVELS

For the HEBREW_TRANSLITERATION_OF_.COM gTLD, no unique security measures or commitments must be made by Verisign to any registrant.

5 SECURITY MEASURES ARE APPROPRIATE FOR THE APPLIED-FOR gTLD STRING (FOR EXAMPLE, APPLICATIONS FOR STRINGS WITH UNIQUE TRUST IMPLICATIONS, SUCH AS FINANCIAL SERVICES-ORIENTED STRINGS, WOULD BE EXPECTED TO PROVIDE A COMMENSURATE LEVEL OF SECURITY)

No unique security measures are necessary to implement the HEBREW_TRANSLITERATION_OF_.COM gTLD. As defined in Section 1 of this response, we commit to providing backend registry services in accordance with the following international and relevant security standards:

* American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) SAS 70

* WebTrust/SysTrust for Certification Authorities (CA)

© Internet Corporation For Assigned Names and Numbers.

EXHIBIT JJN-3

Redacted - Third Party Designated Confidential Information

EXHIBIT JJN-4

JJN-4

Black's Law Dictionary (11th ed. 2019), control

CONTROL

Bryan A. Garner, Editor in Chief

Preface | Guide | Legal Maxims | Bibliography

control *n.* (16c) The direct or indirect power to govern the management and policies of a person or entity, whether through ownership of voting securities, by contract, or otherwise; the power or authority to manage, direct, or oversee <the principal exercised control over the agent>.

- **ceded control.** (1897) Control that has been surrendered or given up.

- **corporate control.** (1905) *Corporations.* **1.** Ownership of more than 50% of the shares in a corporation. — Also termed *effective control*; *working control.* **2.** The power to vote enough of the shares in a corporation to determine the outcome of matters that the shareholders vote on.

- **effective control.** **1.** The physical retention of possession of an item or its maintenance in a secure place. **2.** See *corporate control* (1).

- **superintending control.** (1850) The general supervisory control that a higher court in a jurisdiction has over the administrative affairs of a lower court within that jurisdiction.

- **working control.** (1897) **1.** The effective control of a corporation by a person or group who owns less than 50% of the stock. **2.** See *corporate control* (1).

Westlaw. © 2019 Thomson Reuters. No Claim to Orig. U.S. Govt. Works.

End of Document

© 2022 Thomson Reuters. No claim to original U.S. Government Works.