Dear Ms. Willett and ICANN Staff,

On behalf of our client, Donuts Inc., we respectfully submit the attached comments on the Community Priority Evaluation for <.ART>, along with supporting annexes. Please contact the undersigned with any questions you may have. Thank you.

Respectfully,

John M. Genga
Counsel for DONUTS INC.

Dadotart Application for <.ART>:

Comment to Community Priority Evaluation

INTRODUCTION 1

ANALYSIS 2

CRITERION 1: The Application does not "establish" a "community" under either the "delineation" or "extension" tests, thus clearly yielding less than the maximum four points. 2

The Application reflects no clear "delineation" of any "community." 3

The Application's unbounded "community" lacks "Identification." 3

The Application does not show an "Existing" art *community* 5

The Application demonstrates no community "Organization." 5

The Application cannot receive two points for community "extension.". 6

CRITERION 2: The Application does not establish a sufficient "nexus" to any "community" known as "ART," and certainly not "uniquely.". 8

The <.ART> string does not "match" a "community.". 8

The term "ART" does not "uniquely" identify the claimed "community.". 9

CRITERION 3: The Application can receive no points for registration policies, as it sets forth nothing specific in any of the four Guidebook areas. 10

The Application sets forth no clear eligibility requirements. 10

Application describes no restrictions for the registration of domain names. 11

The Applicant is still analyzing use options, all of which lack requisite specificity. 12

The enforcement planning that appears in the Application lacks the specific policies and procedures required by the Guidebook. 13

CRITERION 4: The few endorsements outside the current deviantart.com membership, and significant comments in opposition, call into question the Applicant's ability to represent the claimed community. 14

CONCLUSION 16

INTRODUCTION

The Community Priority Evaluation ("CPE") is a serious undertaking. It allows for top-level identification of communities by the names for which they are known. Yet, a "successful" CPE also disqualifies applicants that otherwise have met the rigorous criteria to obtain a new gTLD:

> [A] qualified community application eliminates all directly contending standard applications, regardless of how well qualified the latter may be. This is a fundamental reason for very stringent requirements for qualification of a community-based application.

Applicant Guidebook ("Guidebook" or "AGB") § 4.2.3 at 4-9. Accordingly, ICANN created scoring to "identify qualified community-based applications," while preventing "false positives" – *i.e.*, "awarding undue priority to an application that refers to a 'community' construed merely to get a sought-after generic word as a gTLD string." *Id.*

To obtain community priority, an application must score 14 out of 16 possible points. *Id.* at 4-10. "In cases of generic words submitted as community based strings, test runs by [ICANN] staff show that the threshold is difficult to attain …." *See* http://www.icann.org/en/topics/new-gtlds/agv1-analysis-public-comments-18feb09-en.pdf.

An objective analysis demonstrates that the application under review for <.ART> ("Application"), submitted for the Panel's convenience as **Annex A**, does not meet the criteria to garner the 14 points necessary to satisfy the CPE and disqualify all other applicants. Dadotart, Inc., the "Applicant," appears to have concocted a community around a website http://deviantart.com, which has the participation of a limited segment of the global art community. Yet, rather than choosing a string such as <.DEVIANTART>, its organization and the name around which it purports to organize its alleged community, the Applicant seeks to represent a diverse and unconnected universe described by the more generic term, "ART."

While this may qualify as a good decision from a business standpoint, it sacrifices "nexus" and does not meet "establishment" criteria to qualify as a community TLD. The broadly worded TLD name <.ART> does not readily, and certainly does not uniquely, identify a single community. Nor does a cohesive art community with clear boundaries exist; it has no defined size, membership or longevity.

Similarly lacking are the types of registration policies required to pass CPE muster. The Application identifies virtually no eligibility criteria, naming conventions, content and use restrictions or enforcement mechanisms that qualify for community priority.

Finally, the Application provides but a single letter of support from an isolated U.S. company that formed the Applicant and essentially serves as its sponsoring organization. *See* **Annex B**. While some public comments also assert support, they do not meet Guidebook thresholds. Opposing public comments, by contrast, can negatively impact the Application's score.

The Applicant undertakes the CPE essentially as a low cost, high reward gamble. It tries inappropriately to use the CPE to circumvent the appropriate contention set resolution process defined by ICANN.

This does not diminish the Application. By our reading, Dadotart and deviantART earnestly support art and artists.[1] The Application appears competently executed. However, it does not approach the specific criteria that ICANN has provided for a community TLD. This is not surprising, as ICANN has established a rigorous scoring system to prevent gaming and abuses. *See* http://www.icann.org/en/topics/new-gtlds/summary-analysis-proposed-final-guidebook-21feb11-en.pdf, at 117. The Applicant cannot achieve the score necessary to attain community priority, and must instead compete for <.ART> on the same level as all other applicants for the string. .

ANALYSIS

The Guidebook allows the CPE Panel to award up to four points in each of four categories (maximum points in parentheses):

- "Community establishment," which involves "delineation" (2) and "extension" (2), AGB at 4-10 *et seq.*;
- "Nexus," meaning both “nexus” (3) and "uniqueness" (1), *id.* at 4-12 *et seq.*;
- "Registration policies," consisting of "eligibility" (1), "name selection" (1), "content and use" (1) and "enforcement" (1), *id.* at 4-14 *et seq.*; and
- "Community endorsement," which considers "support" (2) and "opposition" (2), *id.* at 4-18 *et seq.*

Applying the standards established by ICANN for these criteria, the Application cannot reach four points on any of them. Giving Applicant the benefit of all doubts on each yields about 5 points, well short of the 14 points needed out of 16.

CRITERION 1: The Application does not "establish" a "community" under either the "delineation" or "extension" tests, thus clearly yielding less than the maximum four points.

A "community" as described in the Guidebook "impl[ies] more cohesion than a mere commonality of interest." AGB at 4-11. As such, the Guidebook calls for examining the claimed community in terms of its "delineation" and "extension." The test for "delineation" considers:

[1] “[A] finding by the panel that an application does not meet the scoring threshold to prevail in a community priority evaluation is not necessarily an indication the community itself is in some way inadequate or invalid.” AGB § 4.2.3

- The "level of public recognition of the group as a community," the existence of "formal boundaries around the community" and "what persons or entities … form" it (hereafter referred to as the "Identification" factors);

- Whether the alleged community pre-dates the commencement of the new gTLD program in 2007 (the "Existence" factor); and

- The level of "organization" of the community through at least one dedicated entity with documented evidence of community activities ("Organization").

AGB at 4-11. "Extension" relates to "the dimensions of the community, regarding its number of members, geographical reach, and foreseeable activity lifetime …." *Id.*

The Application does not identify a community that satisfies these tests, at least not sufficiently to earn all available community "establishment" points. The Applicant defeats any notion of community by its own inability to define it.

The Application reflects no clear "delineation" of any "community."

Satisfying all three of the Identification, Existence and Organization factors will allow an application to score up to a 2. AGB at 4-12. The Application under review does not meet those criteria, and therefore cannot receive 2 "delineation" points.

The Application's unbounded "community" lacks "Identification."

The Application gives no clear guidance as to who makes up the alleged community. Among numerous like examples, it states:

> The arts community is comprised of individuals, groups of individuals and legal entities who identify *themselves* with the Arts and actively participate in or support Art activities or the organization of Art activities.
>
> * * * * *
>
> The international arts community is *diverse and wide-spread* ….
>
> * * * * *
>
> The global arts community at large is constantly growing and *embraces the majority of the world's population*.

See Applic. § 20(a) at 16-17, 19 (emphases added). Such "an unclear, dispersed or unbound definition scores low" in terms of community "Identification." AGB at 4-11. Elsewhere of the Guidebook describes community by the "level of *formal boundaries* around the community and what persons or entities are considered to form the community." AGB § 3.5.4 at 3-22. The above – along with claims by the Applicant's backing organization, deviantART, of "more than

4,500 categories of art," Applic. § 18(b) at 12 – speaks volumes for the proposition that no such formal boundaries exist.

Also, according to ICANN, "community" implies "more cohesion than a mere commonality of interest." AGB at 4-11. The dictionary defines "cohesion" as "the act or state of cohering; tendency to unite, to 'stick together.'" The Application does not demonstrate or even claim any "cohesion" among those engaged in creating, supporting or viewing art around the world, or to whom it would make a <.ART> domain available.

Nor does the term "ART" lend itself to a single, concise definition. Art, of course, encompasses many forms of self-expression. One source defines the term as:

> A visual object or experience consciously created through an expression of skill or imagination. The term *art* encompasses diverse media such as painting, sculpture, printmaking, drawing, decorative arts, photography, and installation. The various visual arts exist within a continuum that ranges from purely aesthetic purposes at one end to purely utilitarian purposes at the other. This should by no means be taken as a rigid scheme, however, particularly in cultures in which everyday objects are painstakingly constructed and imbued with meaning. Particularly in the 20th century, debates arose over the definition of *art*. Figures such as Dada artist Marcel Duchamp implied that it is enough for an artist to deem something "art" and put it in a publicly accepted venue. Such intellectual experimentation continued throughout the 20th century in movements such as conceptual art and Minimalism. By the turn of the 21st century, a variety of new media (e.g., video art) further challenged traditional definitions of art.

http://www.merriam-webster.com/dictionary/art. Another source presents the following definitions:

> The expression or application of human creative skill and imagination, typically in a visual form such as painting or sculpture, producing works to be appreciated primarily for their beauty or emotional power: [uses are:] *the art of the Renaissance, great art is concerned with moral imperfections, she studied art in Paris.*
>
> Works produced by human creative skill and imagination: [uses are:] *his collection of modern art, an exhibition of Mexican art*, [use as a modifier:] *an art critic.*
>
> Creative activity resulting in the production of paintings, drawings, or sculpture: [use:] *she's good at art.*
>
> The various branches of creative activity, such as painting, music, literature, and dance: [use:] the visual arts, the art of photography.
>
> Subjects of study primarily concerned with the processes and products of human creativity and social life, such as languages, literature, and history (as contrasted with scientific or technical subjects): [uses:] *the belief that the arts and sciences were incompatible the Faculty of Arts.*

> Skill at doing a specified thing, typically one acquired through practice: [use:] *the art of conversation.*

http://oxforddictionaries.com/us/definition/american_english/art?q=art. Such widely varied definitions make "Identification" of an art "community" virtually impossible, as confirmed by the Applicant's own struggle with the concept in the Application.

The Application does not show an "Existing" art *community*.

Without question, the arts have existed for nearly as long as civilization itself. Less clear, and certainly not shown by the Application, is whether those who identify with art can be said to have existed *as a community* throughout that time, rather than as individual actors with divergent interests within the broad scope of the highly generalized topic of art. The Applicant appears to have created a "false positive" by "an application that refers to a 'community' construed merely to get a sought-after generic word as a gTLD string." AGB § 4.2.3 at 4-9.

The deviantART website itself serves as an example. The site solicits participation from a wide variety of visual artists, but participation in that narrow field does not cover the entire spectrum of the arts, which includes theatrical art and non-visual arts such as music and literature. The current deviantART website does not reflect participation of all artists because one cannot draw clear boundaries around such a broad set of skills and work. Neither that site nor the Application can point to an identified, pre-existing, cohesive "community" denoted by the single term "art."

The Application demonstrates no community "Organization."

The CPE Guidelines (ver 2.0) ask: "Is there at least one entity mainly dedicated to the community?" Nowhere does the Application identify any. Rather, it states throughout to the contrary:

> The arts community is *very loosely structured* and organized for the most part simply around participation – and by virtue of participation.
>
> * * * * *
>
> There are organized groups within the arts community but *the vast majority of artists and participants in the arts are not structured and are not formally organized* in a hierarchical manner of local/regional, national and international legal entities.
>
> * * * * *
>
> The global arts community at large is constantly growing and *embraces the majority of the world's population*.

Applic. § 20(a) at 18-19 (emphases added). The wide net cast by these sweeping statements does not satisfy the Guidebook's requirement of "Organization" of a "community" through "at least one entity mainly dedicated to the community, with documented evidence of community

activities." AGB at 4-11. The Application identifies no such entity and documents no evidence of its activities. If anything, the Applicant anoints itself the "organizer" of a "community" that it admits has no unifying structure:

> In many ways the strength of the art community lies in its natural openness. The .ART gTLD will provide a globally available locus of communication and identification for the many *millions of arts participants who are not organized* as well as for those who are.

See Applic. § 20(a) at 18 (emphasis added). This *post-hoc* approach does not satisfy Guidebook standards for an "Existing" and "Organized" community.

As a whole, the Application satisfies none of the "delineation" criteria – Identification, Existence, or Organization. Since it must meet *all* of them to earn 2 points, it cannot score more than 1, if that. A "community" of half the world's population cannot have the structure, organization, boundaries or membership requirements described in the criteria to merit the highest score. A generic, broad, encompassing term such as "art" has no concise definition that would enable such delineation. The application fails this very specific test.

We say this not with any intent to diminish the arts. We enjoy art, value those who provide it to us, and believe it makes the world a better place. As applied here, however, the existence of the arts, the benefits they bring, and the 3.5 billion people included within the Applicant's definition of the art community cannot justify awarding a TLD to the exclusion of other qualified, worthy applicants.

The Application cannot receive two points for community "extension."

To receive 2 points for "extension," an application must demonstrate a "community of considerable size and longevity." A "community of either considerable size or longevity, but not fulfilling the requirements for a score of 2," can earn 1 point. One that meets neither gets zero. AGB at 4-10. These size and longevity factors relate "to the dimensions of the community, regarding its number of members, geographical reach, and foreseeable activity lifetime …." *Id.* at 4-11.

In furtherance of these standards, the ICANN application form asks:

- When the community was established, and
- The current estimated size of the community.

The Applicant answers: "The Art community has existed as long people have produced and shared art. The global arts community at large is constantly growing and embraces the majority of the world's population in one way or another …. [T]he arts community has a global presence in every culture." Applic. § 20(a) at 19.

The Applicant itself "is a new organization formed expressly to lead the formation [of] a specialized gTLD devoted to the Arts community. Dadotart is owned and directed by deviantArt (dA), the innovator in creating an entirely Arts-focused community online. dA was formed in

2000 and is headquartered in Los Angeles." *Id.* § 18(a) at 7. "Dadotart's mission is first to unite, support and promote Artists and those who are engaged in the Arts worldwide; and second, to use the .ART gTLD for the co-ordination and protection of their common aims and interests, communication and co-operation, while at the same time conserving and respecting their autonomy." *Id.* § 20(c) at 20.

The Guidebook clearly requires a formation date of some type. The Application reflects that: (1) the art community has existed since essentially the beginning of human time and consists of almost everyone; and (2) Dadotart was formed only a year ago "to unite, support and promote Artists and those who are engaged in the Arts worldwide …." These claims do not entitle the Application to "extension" points.

One cannot merely state, in answer to "how old and how big," that the purported community is as old and big as humanity itself. If there is a community, it has, by the requirements stated in the Guidebook, a specific beginning. The Applicant skirts its responsibility in answering the question by resorting to hyperbole. The arts represent an amorphous, wonderful collection of disparate talents, missions, and enthusiasts – but not a single community with clearly describable age and size boundaries.

A brand new organization such as Dadotart cannot claim to have the age and size necessary to unite and promote the arts worldwide. The dA website is well set out, open and inviting, but relatively unknown to the rest of the world outside its existing sphere of influence; it also ignores segments and geographies in the world of art. It pays little or no attention to theater and non-visual arts. The vast majority of its participants come from North America. The newly minted Dadotart organization is too young, small and geographically confined to meet the age and size requirements of the "extension" test.

The standard for "extension" requires an applicant to describe the community size and age. But the Applicant here has proven this impossible. The term "art" has too many connotations and too much breadth to be described as a single community.

The Application certainly does not merit two "extension" points. With one at most for this prong of the test and at most one more for "delineation," the Application can earn no more than two of the four available "community establishment" points.

Even that would be generous. The Guidebook makes clear that a "community" can exist only where "the requisite awareness and recognition of the community is at hand among the members. *Otherwise the application would be seen as not relating to a real community and score 0* on both 'Delineation' and 'Extension.'" AGB at 4-12 (emphasis added).

CRITERION 2: The Application does not establish a sufficient "nexus" to any "community" known as "ART," and certainly not "uniquely."

Criterion 2 requires a "nexus" between the asserted community and the applied-for string. AGB at 4-12. The test consists of a "nexus" factor of up to three points, and a "uniqueness" score of zero to one.

The claimed community, if it exists, does not go by the specific name "ART" in the same sense that, for example, the "Navajo" and "Boy Scout" communities go by those precise names. The term "ART" means many things, such that it cannot attach uniquely to the divergent interests that the Applicant seeks to designate by that term. As such, the Application can achieve no more than two of the possible four "nexus" points.

The <.ART> string does not "match" a "community."

The Guidebook scores "nexus" as follows:

- For a score of 3: The string matches the name of the community or is a well-known short-form or abbreviation of the community name;
- For a score of 2: String identifies the community, but does not qualify for a score of 3; and
- For a score of 0: String nexus does not fulfill the requirements for a score of 2.

AGB at 4-12 to 4-13. The Applicant states that "the TLD string 'art' matches the name of the community, Art, in the generally accepted sense of the word." Applic. § 20(d) at 21. That casual statement simply does not withstand Guidebook scrutiny.

In order to qualify for a 3, one must apply for the exact name of the community. One can belong to the boy-scouts-of-america or to the uk-philately-society, but not the"art community" because it does not exist as a specifically named organization. The Guidebook held out the score of 3 to those special cases only where a group decided to apply precisely for its name.

Nor does the <.ART> string qualify for a score of two. The Guidebook provides an example that applies squarely here:

> For a score of 2, the applied-for string should closely describe the community or the community members, without over-reaching substantially beyond the community. As an example, a string could qualify for a score of 2 if it is a noun that the typical community member would naturally be called in the context. *If the string appears excessively broad (such as, for example, a globally well-known but local tennis club applying for ".TENNIS") then it* ***would not*** *qualify for a 2*.

Id. at 4-13 (emphases added). Even assuming that the Applicant's sponsoring organization, deviantART, is as "globally well-known" as it claims through its website, the Guidebook example does not allow it to receive two points for the exceedingly broad term "ART." The Applicant

claims a community of half the world's population, 3.5 billion people, and it boasts a large number of registrants to the deviantART website, even if all the registrants were active and supported this application, they could represent only a tiny fraction of the purported community.

The Applicant represents a small subset of an alleged art community in more than one way. While describing itself as global, the company resides in, and the vast majority of staff come from, the United States (matching the Guidebook <.TENNIS> example of a name that would garner zero nexus points). Also, members of the deviantART community register as "deviants,"[2] lessening the nexus between the broader applied-for string and the narrower sponsoring organization.

Closely drawn parallels with the Guidebook example indicate that the Application should receive a score of zero, or at most one, for nexus. It certainly cannot receive 3 or even 2 under the specific Guidebook illustration. .

The term "ART" does not "uniquely" identify the claimed "community."

An applicant can earn a uniqueness score of 1 if the applied-for string has no other significant meaning *beyond identifying the community* described in the application; a score of zero does not fulfill this requirement. AGB at 4-13.

> To be an unambiguous identifier, the "ideal" string would have no other associations than to the community in question. This arguably can be achieved by using the community institution abbreviation as string ….

See http://www.icann.org/en/topics/new-gtlds/agv1-analysis-public-comments-18feb09-en.pdf at 103. This puts the necessary balancing in the hands of applicants. Does an applicant select a popular, well-recognized term that does not uniquely identify a community, such as <.SCOUTS> or <.SCOUTING>? Or does the applicant select a name inarguably unique to it, such as <.BOYSCOUTSOFAMERICA>? Or, more apt here, <.ART> or <.deviantART> (if that could qualify as the name of some "community institution")?

The analysis must focus on the meaning (more accurately, meanings) of the term "ART." In addition to the numerous definitions set forth in the analysis of the first criterion above, it comes as no surprise, even if cliché, that "art" can mean many things to many different people. The term does not describe a "community," but rather a subject, and a virtually boundless one at that.

The Applicant purports to represent the world-wide art "community," but "art" is an ambiguous identifier. The deviantART website caters to visual arts. It mentions theatrical, musical and other art forms, but minimally represents them. While contributors are global, they are primarily American. Finally, those joining the website community are asked to click on the button "become a deviant." The deviant moniker springs out of a following by the organization

[2] https://www.deviantart.com/join/?joinpoint=standard.

of Frank Zappa. However, identification with the label “deviant” cannot be translated into a unique relationship with the label “art.”

The Applicant could have applied for <.deviantART> and matched its own community with the unique name that means nothing else. Instead, it selected the popular, commercially-viable term <.ART>. While that may prove a better business decision in light of the stated goals of the Application, its decision to apply for the mainstream, general name, sacrificed the ability to achieve points in nexus and uniqueness necessary to carry the day as a community applicant.

Evidence of common use of the term "ART" may make it an excellent choice for a top-level domain. However, it does not match the community as described by the Applicant; nor does it identify that newly devised community uniquely. Of the four total points available for "nexus," the Application can earn no more than two.

CRITERION 3: The Application can receive no points for registration policies, as it sets forth nothing specific in any of the four Guidebook areas.

"Registration policies" represent the conditions that the registry will set for prospective registrants of second-level domains. A community application may receive one point for each of the four following policies:

- Eligibility restricted to community members;
- Name selection rules consistent with the articulated community-based purpose of the applied-for gTLD;
- Rules for content and use consistent with the articulated community-based purpose of the applied for gTLD; and
- Specific enforcement mechanisms.

AGB at 4-14 to 4-15. The Panel should score the Application "from a holistic perspective, with due regard for the particularities of the community explicitly addressed." *Id.* at 4-16. Particularly as to "restrictions and corresponding enforcement mechanisms," the Guidebook instructs that these measures "should show an alignment with the community-based purpose of the TLD and demonstrate continuing accountability to the community named in the application." *Id.*

The Application sets forth no clear eligibility requirements.

A point for eligibility requires strict criteria. In a policy advisory, ICANN notes:

> Registration policy is a criterion where a balance is needed between what is reasonably the most appropriate registration policy for a community and the risk for gaming of the process by an "open" application declaring itself as "community-based" to get an advantage in a contention situation. The approach taken is conservative in this respect,

> with the high score reserved for a registration policy only permitting members of the community to register. *A widening has been considered, but it appears reasonable to maintain the chosen approach* ….

See http://www.icann.org/en/topics/new-gtlds/agv1-analysis-public-comments-18feb09-en.pdf, at 103 (emphasis added). The Application, by contrast, would allow virtually anyone to register a <.ART> domain name.

Specifically, the Applicant admits that it "is *still analyzing* potential use case options on the type of domain names that will be permitted to be registered, by whom and when registration will be permitted for defined domain name types." Applic. § 18(b) at 9. In other words, it has no eligibility policies in place. Nor does it contemplate any such policy: "an exhaustive listing of all potential registrants is not possible or desirable." *Id.* § 20(c) at 20.

This comes as no surprise given the Applicant's virtually boundless definition of the art "community." Indeed, it ties what it passes of as eligibility criteria directly to that sweeping definition:

> Eligibility — The arts community at large is made up of Artists and those who are have an identifiable engagement with the Arts worldwide. The following statement describes the feature of community definition for the purposes of eligibility.
>
> Definition—The Art community is comprised of individuals, groups of individuals and legal entities who identify themselves with the Arts and actively participate in or support Art activities or the organization of Art activities.

Id. § 20(e) at 22. This is exactly the type of registration policy susceptible to gaming that ICANN discussed in its February 2009 advisory quoted from above. Which person does not have some sort of "identifiable engagement with the Arts"? Anyone that has had any interaction with the arts, even mere observation, can be eligible to register a name. That is why the Application states that fully one-half of the world's population belongs to the alleged community.

Does this sort of loose eligibility restriction make sense for a <.ART> TLD? Of course. It is completely appropriate that such a TLD be open to all that respect its mission. However, that same openness disqualifies it from earning points in this analysis, and it should receive none.

The Application describes no restrictions for the registration of domain names.

Name selection restrictions serve to protect the identified community. Rules for selecting names must adhere to the articulated community-based purpose of the applied for gTLD.

In this case, the Applicant's "current best thinking involves the ***initial reservation*** of domain names" only, falling within three types:

- Names denoting genres or fields of activity (e.g. theatre, sculpture, painting, photography, sculpture, etc.);

- Names of prominent Art institutions as well as Art-related trademarks; and
- Names of prominent Artists living or dead.

Applic. § 20(c) at 21. These initial reservations do not control subsequent registrations; they simply take certain names "off the table," or create classifications that a registrant can choose to use or not. Otherwise, a registrant can choose whatever name that he, she or it wants, with *no restrictions beyond those otherwise required for every new TLD*. Absent some on-going type of name restrictions, this Application cannot receive a point on for name selection.

The Applicant is still analyzing use options, all of which lack requisite specificity.

The Application does not establish content and use parameters that merit a point for this area. The Guidebook defines "Content and use" restrictions as those "stipulated by the registry as to the content provided in and the use of any second-level domain name in the registry." AGB at 4-16. The Application needs limit content and use in a manner consistent with serving and protecting the global art "community" in order to score a point. *Id.*

According to the Application itself, "Dadotart is still analyzing potential use case options on the type of domain names that will be permitted to be registered, by whom and when registration will be permitted for defined domain name types." Applic. § 18(b) at 9. In other words, the Applicant has not determined restrictions on use and content. What it does indicate provides no guidance whatsoever:

> Content—The arts community is a community of production, support and affinity, and its policies of member definition would be incomplete if they did not hold requirements for name use. Use of a name in artistic production, support and affinity represents ongoing evidence of community eligibility.
>
> [Use —] The registration of domain names under the .ART gTLD will be subject to the further requirement that the registrant's participation or support in the Art community arena and the registrant's use of the domain name must be:
> (1) Generally accepted as legitimate;
> (2) Of a nature that demonstrates the registrant's membership in the Art community; and
> (3) Conducted in good faith at the time of registration and thereafter.

Applic. § 20(e) at 23. The foregoing provides no content and use restrictions at all. It merely states that use of a name expressing an affinity for arts represents evidence of eligibility. Given the virtually limitless definition of "art," this could mean anything. It does not restrict content or use in any way. The Applicant merely says: be legitimate, demonstrate membership in the arts community, and act in good faith. All registries require the first and third item. The second, supposedly demonstrating "membership" in the art "community," encompasses half of the world's population, by Applicant's own admission.

Effective content and use restrictions would set out policies for how the domain names are operated by registrants. Because the TLD is literally "open" to all potential registrants, serious

content and use restrictions cannot realistically come into play.

The weakness of the Applicant's content and use restrictions does not suggest anything untoward. To the contrary, it allows for a legitimate and useful way to operate a TLD targeting a subject as universal and diverse as the arts. However, such a TLD, with its openness to all, cannot also legitimately adopt the community label within the meaning of the Guidebook. It does not merit a point for the virtually nil content and use restrictions resulting from that choice.

The enforcement planning that appears in the Application lacks the specific policies and procedures required by the Guidebook.

Award of a point on enforcement requires specificity: investigation practices, penalties, and takedown procedures – *i.e.*, "tools and provisions set out by the registry to prevent and remedy any breaches of the [content and use] conditions by registrants." AGB at 4-15, 4-16. Lacking such restrictions, as described above, the Application likewise falls short on enforcement procedures. It states:

> [T]he enforcement program will be based on statistically targeted random investigations and on a complaint follow-up process. The statistical targeting is strongly automated and involves the use of search engines and the analysis of registry data related to behavior of registrants. Depending on the type of misuse to be investigated, web site content or content sent to victims of abuse will be reviewed and analyzed by investigators. Enhanced investigation will take place if the registrant has a bad track record in terms of compliance with the rules of the .ART gTLD. Other violations of public record (such as UDRP or URS cases) will also be taken into account.

Applic. § 20(e) at 23. While this provides some basic *direction*, it amounts to prospective thinking in generalities. The Guidebook, by contrast, requires an application to "include specific enforcement measures (e.g. investigation practices, penalties, takedown procedures) constituting a coherent set with appropriate appeal mechanisms." AGB at 4-15. The current "plan," if one can even call it that, lacks policies, procedures, budget, staffing, resource plans and other indicia of a well thought out enforcement or compliance regime.

While the Applicant signals some willingness to establish enforce restrictions, its planning has not risen to a level where a point should be awarded. The lack of specifics as to all other "registration policy" criteria prevents passing this final test; the Application does not adequately identify such policies, especially regarding content and use, such that it does not make clear what to "enforce" on this fourth factor.

In sum, *the Application should earn no points in the area of registration policies*. The Applicant seeks to serve all those who define themselves as associated with the arts. To accomplish that goal, it has foregone the ability to enact strict eligibility, content and use, and name selection policies. The label "ART" does not lend itself to such restrictions. The Application as proposed does not and cannot include the registration restrictions necessary to win any of the four available points in this evaluation.

CRITERION 4: The few endorsements outside the current deviantart.com membership, and significant comments in opposition, call into question the Applicant's ability to represent the claimed community.

The "support" criterion actually looks at both support and opposition in awarding up to four points to an application. For "support," the applicant must demonstrate that:

- It is, or has documented support from, the recognized community institution(s)/member organization(s) or has otherwise documented authority to represent the community. It must have documented support from institutions/organizations representing a *majority* of the overall community in order to score 2.

- Documented support from at least one group with relevance may allow a score of 1, but does not suffice for a score of 2.

AGB at 4-17. On the opposition side, an application will earn two points where it lacks any opposition of relevance, and one where it has "relevant" opposition from "one group of non-negligible size." It will be awarded no points in the case of "relevant opposition from two or more groups of non-negligible size." *Id*. at 4-17.[3]

The ICANN new gTLD comments page includes approximately 300 expressions of support for the Application. However, all or nearly all of these comments come from individuals. No major art organization, institution or museum appears to support the Application.

Many of the support letters come from the staff of Dadotart, a for-profit company. Most of the others belong to the narrow deviantART community who display their work on the deviantart.com website. Little support appears outside that small segment of the art world.

In all events, these expressions of support certainly do not represent a majority of the 3.5 billion-member art community defined by the Applicant, precluding the Application from scoring a "2" under any circumstances. Even crediting the self-serving letters from the Applicant and its sponsoring organization would entitle the Application to no more than a single point.

However, for consideration as relevant support, documentation *must contain a description of the process and rationale used in arriving at the expression of support*, and does not receive a point based merely on the number of comments or expressions of support received. AGB at 4-18. Certain comments call the entire process into question. One states:

> The announcement seeking support does not make it clear that our supporting this movement is helping to decide WHO will run this TLD. It makes it appear instead that we are voting for the TLD to exist at all. I have noticed several people supported

[3] "Relevance" refers to the communities addressed. *Id.* at 4-18. Thus, "relevant" support or opposition means that which comes from those in the named community.

> Dadotart as the TLD manager because they wished to see .art exist at all, clearly not understanding that this was about who will manage TLD not about whether there will be a .art TLD at all. I feel that this is due to the misleading advertisement for support on Deviantart's website.

The apparent vagueness of the solicitation appears in many comments that do not reflect an understanding of the effect of the Application at issue or the CPE. One typical comment (in its entirety): "I'm a design and animation student and I would use a [dot]art address for posting my projects online." This and many comments like it say nothing about such a domain in the particular hands of *this Applicant*.

The Application, therefore, should lose at least one point. At least one (self-interested) group has documented its support, but no others. In addition, any support from individuals outside the deviantART sphere of influence has been called into question by the methods for requesting support.

Meanwhile, dozens of letters oppose the Application as a community TLD. Opposition includes representatives of Artists Rising, a group of 55,000 artists. Some comments question whether the Applicant would be an appropriate steward for the <.ART> TLD:

> The company regularly supports and/or turns a blind eye to copyright infringement on their own site and either doesn't have the time, or integrity to police the original DeviantArt site.
>
> * * * * *
>
> …. countless stolen pictures get to the front page.
>
> * * * * *
>
> Looking at the company's past of ignoring its user-base and acting only in the interests of profit … It is my fear that they will limit use of .ART to content hosted on their site http://deviantart.com . .ART should be managed by a more neutral applicant who supports other art related sites, not their own ecosystem.

One comment provided similar analysis, but in specific Guidebook terms: "Given the foregoing, the App should score 6 on the 16-pt scale, hardly sufficient for priority status. Disqualification is also mandated by common sense. An online marketplace used by a small subset of the world's artists should not control .ART."

Based on the meaningful opposition, including one major organization, the application should lose at least one point for opposition in this case. There is relevant opposition from the Artists Rising group and also significant opposition from many individuals. The maximum single point from the "opposition" side combined with the same highest possible "support" score can result in a total of no more than two points on the last of the four CPE factors.

CONCLUSION

Reviewing the categories considered by the CPE process, this analysis concludes as follows out of the 16 total possible points:

- "Community delineation" (2) and "extension" (2), AGB at 4-10 *et seq.*:
    - ***Zero*** based on the Guidebook statement requiring "awareness and recognition of the community … among the members. Otherwise the application would be seen as not relating to a real community and score 0 on both 'Delineation' and 'Extension.'" AGB at 4-12. ***Maximum*** of ***two*** even apart from this statement.
- "Nexus," meaning both "nexus" (3) and "uniqueness" (1), *id.* at 4-12 *et seq.*:
    - ***Maximum*** of ***one*** based on the Guidebook's <.TENNIS> example prohibiting a score of 2 of the 3 available "nexus" points, and ***zero*** for "uniqueness."
- "Registration policies," consisting of "eligibility" (1), "name selection" (1), "content and use" (1) and "enforcement" (1), *id.* at 4-14 *et seq.*:
    - ***Zero***. The Application sets forth no specific policies in any of these areas.
- "Community endorsement," which considers "support" (2) and "opposition" (2), *id.* at 4-18 *et seq.*:
    - ***Maximum*** of ***one*** for support and ***one*** for opposition; total possible of ***two***.

The Application seeks to gain community priority with a string name that simply is not susceptible to it. The Applicant would have the TLD appeal to a wide range of users, as one would expect for such a universal and important subject. That does not mean the Application merits priority over all other competing applicants who doubtless share similar goals. It can earn no more than 5 of the 14 points needed to gain community priority, and thus fails CPE.

DATED: March 3, 2014

Respectfully submitted,

THE IP & TECHNOLOGY LEGAL GROUP, P.C.
dba New gTLD Disputes

By:_____/jmg/_____
John M. Genga
Attorneys for DONUTS INC.

Annexes

The following Annexes are offered with and in support of this submission:

Annex A: Dadotart Application for <.ART>, App. ID No. 1-1097-20833
Annex B: Support letter accompanying Dadotart Application for <.ART>

Annex A

New gTLD Application Submitted to ICANN by: Dot Registry LLC

String: INC

Originally Posted: 13 June 2012

Application ID: 1-880-35979

Applicant Information

1. Full legal name

Dot Registry LLC

2. Address of the principal place of business

6600 College BLVD
Suite 125
Overland Park Kansas 66211
US

3. Phone number

9136004088

4. Fax number

8169947333

5. If applicable, website or URL

Primary Contact

6(a). Name

Ms. Tess Pattison-Wade

6(b). Title

Executive Director

6(c). Address

6(d). Phone Number

8168986598

6(e). Fax Number

6(f). Email Address

tpw5029@hotmail.com

Secondary Contact

7(a). Name

Shaul Jolles

7(b). Title

CEO

7(c). Address

7(d). Phone Number

8162007080

7(e). Fax Number

7(f). Email Address

sjolles@gmail.com

Proof of Legal Establishment

8(a). Legal form of the Applicant

Limited Liability Company

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

Kansas

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

Attachments are not displayed on this form.

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

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

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

Applicant Background

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

Christopher Michael Parrott	Director of Finance
Paul Eugene Spurgeon	COO
Scott Adam Schactman	Director Law & Policy
Shaul Jolles	CEO

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

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

Ecyber Solutions Group Inc	not applicable

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

having legal or executive responsibility

Applied-for gTLD string

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

INC

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

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

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

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

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

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

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

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

Attachments are not displayed on this form.

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

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

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

There are no known operational or rendering issues associated with our applied for string. We are relying on the proven capabilities of Neustar to troubleshoot and quickly eliminate these should they arise.

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

Mission/Purpose

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

To build confidence, trust, reliance, and loyalty for consumers and business owners alike by creating a dedicated gTLD to specifically serve the Community of Registered Corporations. Through our registry service, we will foster consumer peace of mind with confidence by ensuring that all domains bearing our gTLD string are members of the Registered Community of Corporations. Our verification process will create an unprecedented level of security for online consumers by authenticating each of our registrant’s right to conduct business in the United States. The “.INC” gTLD will

fill a unique void in the current DNS and assist in decreasing the burden on existing domain names by identifying members of the Registered Community of Corporations.

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

With the increased popularity of the Internet as a consumer marketplace and the ease with which individuals are able to access information online, it is essential that safeguards be put in place to validate and identify legitimate businesses. Businesses representing themselves as corporations by including Inc., Incorporated or Corporation in their business names create an expectation amongst consumers that they have the legal right to conduct business as a corporation. Unfortunately, consumers are currently unable to quickly verify the accuracy of this representation. Fraudulent business entities rely on this consumer assumption and the lack of available verification resources to prey on both businesses and consumers. As online commerce replaces brick-and-mortar businesses, there has been a corresponding rise in business identity theft online, which in turn creates a lack of consumer confidence. In the vast majority of states, the Secretary of State is responsible for overseeing the business entities in the state – from the registration of corporations or verification of business filings, to the administration of the Uniform Commercial Code, an act, which provides for the uniform application of business contracts and practices across the United States. The Secretaries' role is critical to the chartering of businesses (including, but not limited to the formation of corporations) that wish to operate in their state. In this regard, the Secretaries of State maintain all records of business activities within the state, and in some states, the Secretary of State has wide-ranging regulatory authority over businesses as well.

The ".INC" gTLD will be exclusively available to members of the Community of Registered Corporations, as verified through the records of each registrant's Secretary of State's Office (or other state official where applicable). By verifying that a registrant is a registered U.S. corporation, DOT Registry will be able to bring unprecedented clarity and security to consumers and business owners, assuring Internet users, registry applicants, and others that web addresses ending in ".INC" are a hallmark of a valid corporation recognized by a governmental authority of the United States. This process will decrease the possibility of identity misrepresentation in a cyber setting and assist lesser-known businesses in legitimizing their services to consumers.

In January 2012, after many public forums and contributions from consumer advocates, the Business Services Committee of the National Association of Secretaries of State (NASS) released the NASS White Paper on Business Identity Theft, indicating that at least 26 states have reported business identity theft cases resulting from fraudulent business representations online. North Carolina Secretary of State Elaine Marshall, who serves as Co-Chair of the NASS Business Services Committee, indicates that the primary function of the White Paper is to "Harness new technology to develop cost-effective solutions, and ultimately make it harder for identity thieves to prey upon state-based businesses."

With the implementation of the ".INC" gTLD, consumers would have the ability to quickly identify the presented business as a valid U.S. corporation. As ".INC" registrations grow, we will see a reduction in the ease with which criminals are able to hide behind fictitious entities because consumers will be conditioned to look for the appropriate gTLD ending before conducting business online. This simple gTLD extension would provide an efficient and cost-effective solution to a growing economic concern in the United States by creating a verifiable online business community network. Through this innovative concept, the DNS system will help to

build a stronger more resilient business platform for members of the Registered Community of Corporations, while fostering increased user confidence, by ensuring accurate business representation.

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

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

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

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

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

Further, the ".INC" gTLD will strive to foster competition by presenting members of the Community of Registered Corporations with a highly valued customized domain name that not only represents their business, but also their validity in the marketplace. Within the current existing top-level domains it is hard for businesses to find naming options that appropriately represent them. One advantage of the ".INC" gTLD is that it will drive the "right" kind of online registrations by offering a valued alternative to the currently overcrowded and often unrestricted name space. Registrants will be inspired to pursue ".INC" domains not only because they will be guaranteed a name representative to their business, but also because of the increased validity for their business operations brought about by the ".INC" verification process. DOT Registry anticipates that the security offered through a ".INC" extension will increase consumer traffic to websites which in turn will boost advertising revenue online and consumer purchasing.

Successful implementation of the ".INC" domain will require two registration goals: (1) capture newly formed corporations and assist them in securing a ".INC" domain

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11) All registration information will be made publicly available. DOT Registry will not accept blind registration or registration by proxy. DOT Registry's registry services operator will provide thick WHOIS services that are fully compliant with RFC 3912 and with Specifications 4 and 10 of the Registry Agreement. Additionally, DOT Registry will provide a Web-based WHOIS application, which will be located at www.whois.inc. The WHOIS Web application will be an intuitive and easy to use application. A complete description of these services can be found in Question 26 below.

12) Awarded names are non-transferrable to entities outside of the designated community, regardless of affiliation to any member of the community. In the event that a registrant's business entity merges, is acquired, or sold, the new entity will be allowed to maintain the previously awarded ".INC" domain until the domain renewal date, at which point they will be evaluated as described in number seven (7) above. Further, any entity acquiring a ".INC" domain through the processes described in this guideline that does not meet the registration criteria and wishes to maintain the awarded domain will be allowed a grace period after the renewal verification process to correct any non-compliance issues in order to continue operating their acquired domain. If the said entity is unable to comply with DOT Registry's guidelines, the awarded domain will be revoked.
13) If an application is unable to be verified or does not meet the requirements of the sponsored community, the application will be considered invalid.
14) DOT Registry will implement a reserved names policy consisting of both names DOT Registry wishes to reserve for our own purposes as the registry operator and names protected by ICANN. DOT Regisgtry will respect all ICANN reserved names including, but not limited to, two letter country codes and existing TLD's. Additionally, DOT Registry will seek ICANN approval on any additional names we plan to reserve in order to appropriately secure them prior to the opening of general availability.

In addition to DOT Registry's comprehensive eligibility, verification, and policing mechanisms, DOT Registry will implement a series of Rights Protection Mechanisms (RPM), including but not limited to: Support for and interaction with the Trademark Clearinghouse ("Clearinghouse"); use of the Trademark Claims Service; segmented Sunrise Periods allowing for the owners of trademarks listed in the Clearinghouse to register domain names that consist of an identical match of their listed trademarks; subsequent Sunrise Periods to give trademark owners or registrants that own the rights to a particular name the ability to block the use of such name; and stringent take down policies and all required dispute resolution policies.

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

".INC" was proposed for the sole purpose of eliminating business and consumer vulnerability in a cyber setting. In order to maintain the integrity of that mission and minimize the negative consequences to consumers and business owners, the following policies will be adhered to:
(a) No information collected from any registrant will be used for marketing purposes.
(b) Data collected will not be traded or sold.
(c) All data collected on any registrant will be available to the registrant free of charge.
(d) Registrants will be allowed to correct data inaccuracies as needed.
(e) All data will be kept secure.
DOT Registry will strictly uphold the rules set forth in their registration guidelines in order to accurately service the Community of Registered Corporations and mitigate any negative consequences to consumers or Internet users.
Price structures for the ".INC" gTLD are designed to reflect the cost of verification within our community requirements and the ongoing cost of operations. Price escalation will only occur to accommodate rising business costs or fees implemented by the Secretaries of State with regard to verifying the "Active" status of a Registrant. Any price increases would be submitted to ICANN as required in our Registry Agreement and will be compiled in a thoughtful and responsible manner, in

order to best reduce the affects on both the registrants and the overall retail market.
DOT Registry does not plan to offer registrations to registrants directly therefore our pricing commitments will be made within our Registry-Registrar Agreements. It is our intention that these commitments will percolate down to registrants directly and that the contractual commitments contained within our Registry-Registrar Agreements will be reflected in the retail sale process of our gTLD, thus minimizing the negative consequences that might be imposed on registrants via the retail process.
DOT Registry plans to offer bulk registration benefits to Registrars during the first 6 months of operation. Registrars wishing to purchase bulk registrations of 1,000 names or more would be offered a 5% discount at the time of purchase. DOT Registry shall provide additional financial incentives to it's Registrars for pre-authentication of Registrant data prior to such data being passed to the registry. DOT Registry will provide for lower renewal and bulk registration fees in its RRAs for registrations which have been pre-authenticated and which DOT Registry can rely on as accurate data to be entered into its WhoIs database.

Additionally, DOT Registry , through our founders program will provide a 25% discount to founders participants as a participation incentive. It is possible that DOT Registry would offer additional pricing benefits from time to time as relative to the market. All future pricing discounts not detailed in this application will be submitted through the appropriate ICANN channels for approval prior to introduction to the market.

Community-based Designation

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

Yes

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

DOT Registry plans to serve the Community of Registered Corporations. Members of the community are defined as businesses registered as corporations within the United States or its territories. This would include Corporations, Incorporated Businesses, Benefit Corporations, Mutual Benefit Corporations and Non-Profit Corporations. Corporations or "INC's" as they are commonly abbreviated, represent one of the most complex business entity structures in the U.S. Corporations commonly participate in acts of commerce, public services, and product creation.
Corporations are the oldest form of organized business in the United States, with the first organized corporation dating back to the 18th century. In 1819 The US Supreme Court formalized their policy on corporation formation by enhancing the rights granted to US Corporations. This policy change for the United States spurred increased corporate registrations and acted as an early economic boom for the states. Well known early corporations included the British East India Company, Carnegie Steel Company, and Standard Oil. The creation of corporations is synonymous with the development of free enterprise in the United States and much of our countries

infrastructure and services were created by early and innovative corporations. Corporation creation has been viewed as especially unique throughout US history because corporations are considered the only business model that are recognized by law to have the rights and responsibilities similar to natural persons. Corporations can exercise human rights against real individuals and the state. Additionally, they themselves can be responsible for human rights violations. This unique human element makes corporations acutely responsible for their actions as an entity. This feature becomes especially applicable when we begin to view corporations as a community. "Community" is defined by Merriam Webster's dictionary as a group sharing common characteristics or interests and perceived or perceiving itself as distinct in some respect from the larger society within which it exists. DOT Registry believes that corporations fall well within this definition due to their specific registration requirements, which set them apart from individuals and other business entities, while granting them operating privileges and distinct rights and responsibilities.

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

Business formation favors the corporate entity structure because it provides its shareholders with limited personal liability and a unique taxing structure. Corporations provide the backbone of the American business culture. Fortune 500's top ten US corporations for 2011 include: Wal-Mart Stores, Exxon Mobil, Chevron, ConocoPhillips, Fannie Mae, General Electric, Berkshire Hathaway, General Motors, Bank of America and Ford Motors. From this listing one can ascertain that corporations span every genre of business and play an intricate role in the daily lives of consumers. From gas stations to hospitals, grocery stores to financial lending institutions corporations drive the stock market, industry production, and consumer spending.

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

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

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

publicly available in order to provide complete transparency for consumers.
Over 64% of US public corporations are registered in the state of Delaware. Because of this preeminence, Dot Registry has drawn on Delaware Law as an example of formation requirements and operating privileges.
According to Delaware Law corporations may be formed by:
(a) Any person, partnership, association or corporation, singly or jointly with others, and without regard to such person's or entity's residence, domicile or state of incorporation, may incorporate or organize a corporation under this chapter by filing with the Division of Corporations in the Department of State a certificate of incorporation which shall be executed, acknowledged and filed in accordance with this title.
(b) A corporation may be incorporated or organized under this chapter to conduct or promote any lawful business or purposes, except as may otherwise be provided by the Constitution or other law of this State.
Entities are required to comply with formation practices in order to receive the right to conduct business in the US. Once formed a corporation must be properly maintained. Corporations are expected to comply with state regulations, submit annual filings, and pay specific taxes and fees. Should a corporation fail to comply with state statutes it could result in involuntary dissolution by the state in addition to imposed penalties, taxes and fees.
All entities bearing the words Corporation or Incorporated in their business name create the assumption that they have been awarded the privileges associated to that title such as: the ability to conduct commerce transactions within US borders or territories, the ability to market products, solicit consumers and provide reputable services in exchange for monetary values, and finally to provide jobs or employment incentives to other citizens.
Membership in the Community of Corporations is established through your business entity registration. In order to maintain your membership to this community you must remain an "Active" member of the community. Active" in this context can be defined as any corporation registered with a Secretary of State in the United States and its territories, that is determined to be authorized to conduct business within that State.

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

DOT Registry, LLC is owned solely by ECYBER Solutions Group, Inc., a registered Corporation in the State of Kansas. DOT Registry has a direct relationship to the proposed community because of our ownership makeup. In addition, DOT Registry is a corporate affiliate of the National Association of Secretaries of State (NASS), an organization which acts as a medium for the exchange of information between states and fosters cooperation in the development of public policy, and is working to develop individual relationships with each Secretary of State's office in order to ensure our continued commitment to honor and respect the authorities of each state.
DOT Registry is acutely aware of our responsibility to uphold our mission statement of: building confidence, trust, reliance, and loyalty for consumers and business owners alike by creating a dedicated gTLD to specifically serve the Community of Corporations.DOT Registry has also specifically pledged to various Secretaries of State to responsibly manage this gTLD in a manner that will both protect and promote business development in the US. Further our policies were developed through direct collaboration with the state offices so as to mitigate any possibility of misrepresenting their regulations.
In order to ensure that we accomplish this goal and preserve the credibility of our operations DOT Registry has taken the following advance actions to ensure compliance

and community protection:

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

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

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

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

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

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

1) Various Secretary of States Offices: Specifically The Secretary of State of Delaware which represents over 55% of public corporations in the United States and a majority of members in this community and The Secretary of State of South Dakota, which is working towards combatting business identity theft and fictitious business registration.

2) Members of the community including but not limited to CSC our registrar partner and Legal Zoom, the nation's leading provider for online business registration.

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

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

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

The goal of the ".INC" gTLD is to build confidence, trust, reliance, and loyalty for consumers and business owners alike by creating a dedicated gTLD to specifically

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

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

End-users for this TLD would include everyday consumers, members of the community, businesses without the community, and consumers looking for more accurate information with regards to those with whom they may conduct business. DOT Registry plans to initiate a robust marketing campaign geared towards the proposed end-users in order to ensure that consumers are aware of what ".INC" stands for and its significance throughout the Community of Corporations. In addition to the vast consumer benefits from the creation of the ".INC" gTLD, DOT Registry believes that ".INC" domains would be considerably beneficial to business end users. Since DOT Registry will not allow blind registration or registration by proxy businesses viewing ".INC" sites would be able to instantly ascertain what businesses operate under the blanket of parent companies, are subsidiaries of other businesses, and of course where a corporation is domiciled. This easily identifiable information not only assists businesses in accurately identifying who they are doing business with, it would also assist in locating sales and use tax information, identifying applicable state records, and tracking an entity's history. These factors could help to determine the outcome of sales, mergers, contract negotiations, and business relationships. Ensuring that this kind of transparency and accountability – qualitities previously not attainable in a TLD – shall be at the fingertips of potential business partners or investors.

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

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

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

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

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

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

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

their principal place of business, which is listed with their applicable Secretary of State's office or legally reciprocal jurisdiction.

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

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

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

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

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

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

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

10) All registration information will be made publicly available. DOT Registry will not accept blind registration or registration by proxy. DOT Registry's registry services operator will provide thick WHOIS services that are fully compliant with RFC 3912 and with Specifications 4 and 10 of the Registry Agreement. Additionally, DOT Registry will provide a Web-based WHOIS application, which will be located at www.whois.inc. The WHOIS Web application will be an intuitive and easy to use application which will allow the general public to easily access registration information for each ".INC" site. A complete description of these services can be found in Question 26 below.

11) Awarded names are non-transferrable to entities outside of the designated community, regardless of affiliation to any member of the community. In the event that a registrant's business entity merges, is acquired, or sold, the new entity will be allowed to maintain the previously awarded ".INC" domain until the domain renewal date, at which point they will be evaluated as described in number seven (7) above. Further, any entity acquiring a ".INC" domain through the processes described in this guideline that does not meet the registration criteria and wishes to maintain the awarded domain will be allowed a 30 day grace period after the renewal verification process to correct any non-compliance issues in order to continue operating their

acquired domain. If the said entity is unable to comply with DOT Registry's guidelines, the awarded domain will be revoked.
12)If an application is unable to be verified or does not meet the requirements of the sponsored community, the application will be considered invalid.In addition to Applicant's comprehensive eligibility, verification, and policing mechanisms, DOT Registry will implement a series of Rights Protection Mechanisms (RPM), including but not limited to: Support for and interaction with the Trademark Clearinghouse ("Clearinghouse"); use of the Trademark Claims Service; segmented Sunrise Periods allowing for the owners of trademarks listed in the Clearinghouse to register domain names that consist of an identical match of their listed trademarks; subsequent Sunrise Periods to give trademark owners or registrants that own the rights to a particular name the ability to block the use of such name; stringent take down policies in order to properly operate the registry; and Applicant shall comply with any RRDRP decision, further reinforcing the fact that Applicant is committed to acting in best interest of the community.DOT Registry will employ an in house Rights Protection Mechanism Team consisting of our Director of Legal and Policy and two additional support personnel. The RPM team will work to mitigate any RPM complaints, while protecting the general rights and integrity of the ",INC" gTLD. The RPM team will strictly enforce the rights protection mechanisms described in this application. Membership verification will be performed via DOT Registry's designated agents that which have software systems in place to efficiently interface with each state's data records. By utilizing the resources of industry leaders in this field, DOT Registry will ensure accurate and timely verification in addition to our ability to meet the needs of such a vast community. "Active" status will be specifically verified by cross referencing an applicant's registration data with state records. If this process is unable to be automated at any given time DOT Registry's agents will manually verify the information by contacting the applicable state agencies. While manual verification will obviously employ a larger pool of resources, DOT Registry believes that its industry partners are sufficiently able to accomplish this task based on their employee pool and past business accomplishments. Registrants will be expected to provide a minimum of their legal registered name, state of incorporation, registered business address, and administrative contact. All additional information required such as proof of incorporation or "active" status verification will be the sole responsibility of DOT Registry or its designated agents and will be acquired through the processes described herein.
DOT Registry will not restrict the content of ".INC" sites other then through the enforcement of our Abuse Mitigation practices or Rights Protection Mechanisms as described in question 28 and 29 of this application. All ".INC" sites will be expected to adhere to the content restrictions described in DOT Registry's abuse policies. Any sites infringing on the legal rights of other individuals or companies, trademarks, or participating in the practice and promotion of illegal activities will be subject to Applicant's take down procedures. ".INC" domains are designed for the sole use of community members with the intention of promoting their specific business activities.

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

Attachments are not displayed on this form.

Geographic Names

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

No

Protection of Geographic Names

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

Applicant has thoroughly reviewed ISO 3166-1 and ISO 3166-2, relevant UN documents on the standardization of geographic names, GAC correspondence relating to the reservation of geographic names in the .INFO TLD, and understands its obligations under Specification 5 of the draft Registry Agreement. Applicant shall implement measures similar to those used to protect geographic names in the .INFO TLD by reserving and registering to itself all the geographic place names found in ISO-3166 and official country names as specified by the UN. Applicant has already discussed this proposed measure of protecting geographic names with its registry services provider, Neustar, and has arranged for such reservation to occur as soon after delegation as is technically possible.

As with the .INFO TLD, only if a potential second-level domain registrant makes a proper showing of governmental support for country or territorial names will Applicant then relay this request to ICANN. At this point, Applicant would wait for the approval of the GAC and of ICANN before proceeding to delegate the domain at issue.

Registry Services

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

23.1 Introduction

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

23.2 Standard Technical and Business Components

Neustar will provide the highest level of service while delivering a secure, stable and comprehensive registry platform. DOT Registry will use Neustar's Registry Services platform to deploy the ".INC" registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to ".INC"):

-Registry-Registrar Shared Registration Service (SRS)

-Extensible Provisioning Protocol (EPP)

-Domain Name System (DNS)

-WHOIS

-DNSSEC

-Data Escrow

-Dissemination of Zone Files using Dynamic Updates

-Access to Bulk Zone Files

-Dynamic WHOIS Updates

-IPv6 Support

-Rights Protection Mechanisms

-Internationalized Domain Names (IDN). [Optional should be deleted if not being offered].

The following is a description of each of the services.

23.2.1 SRS

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

23.2.2 EPP

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

23.2.3 DNS

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

23.2.4 WHOIS

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

Standard WHOIS (Port 43)

Standard WHOIS (Web)

Searchable WHOIS (Web)

23.2.5 DNSSEC

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

23.2.6 Data Escrow

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

-Protect against data loss

-Follow industry best practices

-Ensure easy, accurate, and timely retrieval and restore capability in the event of a hardware failure

-Minimizes the impact of software or business failure.

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

23.2.7 Dissemination of Zone Files using Dynamic Updates

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

23.2.8 Access to Bulk Zone Files

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

23.2.9 Dynamic WHOIS Updates

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

decoupling WHOIS from the SRS. Additional information on WHOIS updates is presented in response to Question 26.

23.2.10 IPv6 Support

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

23.2.11 Required Rights Protection Mechanisms

DOT Registry, will provide all ICANN required Rights Mechanisms, including:

-Trademark Claims Service

-Trademark Post-Delegation Dispute Resolution Procedure (PDDRP)

-Registration Restriction Dispute Resolution Procedure (RRDRP)

-UDRP

-URS

-Sunrise service.

More information is presented in the response to Question 29.

23.2.12 Internationalized Domain Names (IDN)

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

23.3 Unique Services

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

23.4 Security or Stability Concerns

All services offered are standard registry services that have no known security or stability concerns. Neustar has demonstrated a strong track record of security and stability within the industry.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

24.1 Introduction

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

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

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

24.2 The Plan for Operation of a Robust and Reliable SRS

24.2.1 High-level SRS System Description

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

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

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

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

-Fully redundant architecture at two sites

-Support for IDN registrations in compliance with all standards

-Use by over 300 Registrars

-EPP connectivity over IPv6

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

24.2.2 SRS Systems, Software, Hardware, and Interoperability

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

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

The Registry is able to limit the ability of any one registrar from adversely

impacting other registrars by consuming too many resources due to excessive EPP transactions. The system uses network layer 2 level packet shaping to limit the number of simultaneous connections registrars can open to the protocol layer.

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

-The IP address of the client

-Timestamp

-Transaction Details

-Processing Time.

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

24.2.3 SRS Design

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

-Protocol Layer

-Business Policy Layer

-Database.

Each of the layers is described below.

24.2.4 Protocol Layer

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

below. The protocol layer is horizontally scalable as dictated by volume.

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

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

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

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

24.2.5 Business Policy Layer

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

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

The SRS today processes over 30 million EPP transactions daily.

24.2.6 Database

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

Question 33.

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

24.2.7 Number of Servers

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

24.2.8 Description of Interconnectivity with Other Registry Systems

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

-WHOIS

-DNS

-Billing

-Data Warehouse (Reporting and Data Escrow).

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

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

of which have involved the processing of over tens of millions of transactions in the opening hours. The following are the standard three external notifiers used the SRS:

24.2.9 WHOIS External Notifier

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

24.2.10 DNS External Notifier

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

24.2.11 Billing External Notifier

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

24.2.12 Data Warehouse

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

24.2.13 Frequency of Synchronization between Servers

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

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

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

24.2.15 Compliance with Specification 6 Section 1.2

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

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

24.2.16 Compliance with Specification 10

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

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

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

24.3 Resourcing Plans

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

-Development⁄Engineering

-Database Administration

-Systems Administration

-Network Engineering.

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

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

-Development⁄Engineering 19 employees

-Database Administration- 10 employees

-Systems Administration 24 employees

-Network Engineering 5 employees

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

25. Extensible Provisioning Protocol (EPP)

25.1 Introduction

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

25.2 EPP Interface

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

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

The main features of the EPP implementation are:

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

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

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

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

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

-Auditable: The system stores detailed information about EPP transactions from provisioning to DNS and WHOIS publishing. In case of a dispute regarding a name registration, the Registry can provide comprehensive audit information on EPP transactions.

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

25.3 Compliance with RFCs and Specifications

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

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

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

25.3.1 EPP Toolkits

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

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

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

25.4 Proprietary EPP Extensions

[Default Response]

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

The full EPP schema to be used in the ".INC" registry is attached in the document titled EPP Schema Files.

25.5 Resourcing Plans

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

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

-Development/Engineering 19 employees

-Quality Assurance - 7 employees.

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

26. Whois

DOT Registry, LLC recognizes the importance of an accurate, reliable, and up-to-date WHOIS database to governments, law enforcement, intellectual property holders, and the public as a whole, and is firmly committed to complying with all of the applicable WHOIS specifications for data objects, bulk access, and lookups as defined in Specifications 4 and 10 to the Registry Agreement and relevant RFCs.

DOT Registry, LLC's back-end registry services provider, Neustar, has extensive experience providing ICANN and RFC-compliant WHOIS services for each of the TLDs that it operates both as a Registry Operator for gTLDs, ccTLDs, and back-end registry services provider. As one of the first "thick" registry operators in the gTLD space, the WHOIS service provided by DOT Registry, LLC's registry services operator has been designed from the ground up to display as much information as required by ICANN and respond to a very stringent availability and performance requirement.

Some of the key features of DOT Registry, LLC's WHOIS services will include:

- Fully compliant with all relevant RFCs including 3912;
- Production proven, highly flexible, and scalable (DOT Registry, LLC's back-end registry services provider has a track record of 100% availability over the past 10 years);
- Exceeds current and proposed performance specifications;
- Supports dynamic updates with the capability of doing bulk updates;
- Geographically distributed sites to provide greater stability and performance; and
- Search capabilities (e.g., IDN, registrant data) that mitigate potential forms of abuse as discussed below.

DOT Registry, LLC's registry services operator will provide thick WHOIS services that are fully compliant with RFC 3912 and with Specifications 4 and 10 of the Registry Agreement.

DOT Registry, LLC's WHOIS service will support port 43 queries, and will be optimized for speed using an in-memory database and a master-slave architecture between SRS and WHOIS slaves. RFC 3912 is a simple text based protocol over TCP that describes the interaction between the server and client on port 43. DOT Registry, LLC's registry services operator currently processes millions of WHOIS queries per day.

In addition to the WHOIS Service on port 43, DOT Registry, LLC will provide a Web-based WHOIS application, which will be located at www.whois.inc. This WHOIS Web application will be an intuitive and easy to use application for the general public to use. The WHOIS Web application provides all of the features available in the port 43 WHOIS. This includes full and partial search on:

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

The WHOIS web application will also provide features not available on the port 43 service. These include:

- Extensive support for international domain names (IDN)
- Ability to perform WHOIS lookups on the actual Unicode IDN
- Display of the actual Unicode IDN in addition to the ACE-encoded name
- A Unicode to Punycode and Punycode to Unicode translator
- An extensive FAQ
- A list of upcoming domain deletions

DOT Registry, LLC will also provide a searchable web-based WHOIS service in accordance with Specification 4 Section 1.8 The application will enable users to search the WHOIS directory to find exact or partial matches using any one or more of the following fields:

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

The WHOIS user will be able to choose one or more search criteria, combine them by Boolean operators (AND, OR, NOT) and provide partial or exact match regular expressions for each of the criterion name-value pairs. The domain names matching the search criteria and their WHOIS information will quickly be returned to the user. In order to reduce abuse for this feature, only authorized users will have access to

the Whois search features after providing a username and password. DOT Registry, LLC will provide third party access to the bulk zone file in accordance with Specification 4, Section 2 of the Registry Agreement. Credentialing and dissemination of the zone files will be facilitated through the Central Zone Data Access Provider, which will make access to the zone files in bulk via FTP to any person or organization that signs and abides by a Zone File Access (ZFA) Agreement with the registry. Contracted gTLD registries will provide this access daily and at no charge.
DOT Registry, LLC will also provide ICANN and any emergency operators with up-to-date Registration Data on a weekly basis (the day to be designated by ICANN). Data will include data committed as of 00:00:00 UTC on the day previous to the one designated for retrieval by ICANN. The file(s) will be made available for download by SFTP, unless ICANN requests other means in the future.
DOT Registry, LLC's Legal Team consisting of 3 dedicated employees, will regularly monitor the registry service provider to ensure that they are providing the services as described above. This will entail random monthly testing of the WHOIS port 43 and Web-based services to ensure that they meet the ICANN Specifications and RFCs as outlined above, if not, to follow up with the registry services provider to ensure that they do. As the relevant WHOIS will only contain DOT Registry, LLC's information, DOT Registry, LLC's WHOIS services will necessarily be in compliance with any applicable privacy laws or policies.

27. Registration Life Cycle

27.1 Registration Life Cycle

27.1.1 Introduction

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

27.1.2 Domain Lifecycle - Description

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

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

indicating the particular state of the domain and indicating any restrictions placed on the domain. The EPP standard defines 17 statuses, however only 14 of these statuses will be used in the ".INC" registry per the defined ".INC" business rules.

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

-OK Default status applied by the Registry.

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

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

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

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

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

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

-Hold Removes the domain from the DNS zone.

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

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

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

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

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

-Domain may be updated

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

-Domain may be renewed at anytime during the term

-Domain may be auto-renewed by the Registry

-Domain may be transferred to another registrar.

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

27.2 Registration States

27.2.1 Domain Lifecycle Registration States

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

-Active

-Inactive

-Locked

-Pending Transfer

-Pending Delete.

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

27.2.2 Active State

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

27.2.3 Inactive State

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

27.2.4 Locked State

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

27.2.5 Pending Transfer State

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

27.2.6 Pending Delete State

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

27.3 Typical Registration Lifecycle Activities

27.3.1 Domain Creation Process

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

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

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

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

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

27.3.2 Update Process

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

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

-Domain statuses

-Registrant ID

-Administrative Contact ID

-Billing Contact ID

-Technical Contact ID

-Nameservers

-AuthInfo

-Additional Registrar provided fields.

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

27.3.4 Renew Process

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

27.3.5 Transfer Process

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

-Initiate a domain transfer

-Cancel a domain transfer

-Approve a domain transfer

- Reject a domain transfer.

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

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

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

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

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

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

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

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

27.3.6 Deletion Process

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

27.4 Applicable Time Elements

The following section explains the time elements that are involved.

27.4.1 Grace Periods

There are six grace periods:

-Add-Delete Grace Period (AGP)

-Renew-Delete Grace Period

-Transfer-Delete Grace Period

-Auto-Renew-Delete Grace Period

-Auto-Renew Grace Period

-Redemption Grace Period (RGP).

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

The following describes each of these grace periods in detail.

27.4.2 Add-Delete Grace Period

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

27.4.3 Renew-Delete Grace Period

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

27.4.4 Transfer-Delete Grace Period

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

27.4.5 Auto-Renew-Delete Grace Period

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

27.4.6 Auto-Renew Grace Period

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

27.4.7 Redemption Grace Period

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

The RGP period is 30 days, during which time the domain may be restored using the EPP RenewDomain command as described below. Following the 30day RGP period the domain will remain in pendingDelete status for an additional five days, during which time

the domain may NOT be restored. The domain is released from the SRS, at the end of the 5 day non-restore period. A restore fee applies and is detailed in the Billing Section. A renewal fee will be automatically applied for any domain past expiration.

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

27.5 State Diagram

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

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

The details of each trigger are described below:

-Create:Registry receives a create domain EPP command.

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

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

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

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

-Delete: Registry receives a delete domain EPP command.

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

-DeleteWithinAddGrace:Domain deletion falls within add grace period.

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

-Transfer: Transfer request EPP command is received.

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

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

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

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

27.5.1 EPP RFC Consistency

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

27.6 Resources

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

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

-Development/Engineering 19 employees

-Registry Product Management 4 employees

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

28. Abuse Prevention and Mitigation

General Statement of Policy

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

Anti-Abuse Policy

DOT Registry will implement in its internal policies and its Registry-Registrar Agreements (RRAs) that all registered domain names in the TLD will be subject to a Domain Name Anti-Abuse Policy ("Abuse Policy").

The Abuse Policy will provide DOT Registry with broad power to suspend, cancel, or transfer domain names that violate the Abuse Policy. DOT Registry will publish the Abuse Policy on its home website at NIC.INC and clearly provide DOT Registry's Point of Contact ("Abuse Contact") and its contact information. This information shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of abuse complaints, and a telephone number and mailing address for the primary contact. DOT Registry will ensure that this information will be kept accurate and up to date and will be provided to ICANN if and when changes are made.

In addition, with respect to inquiries from ICANN-Accredited registrars, the Abuse Contact shall handle requests related to abusive domain name practices.

Inquiries addressed to the Abuse Contact will be routed to DOT Registry's Legal Team who will review and if applicable remedy any Complaint regarding an alleged violation of the Abuse Policy as described in more detail below. DOT Registry will catalog all abuse communications in its CRM software using a ticketing system that maintains records of all abuse complaints indefinitely. Moreover, DOT Registry shall only provide access to these records to third parties under limited circumstances, such as in response to a subpoena or other such court order or demonstrated official need by law enforcement.

The Abuse Policy will state, at a minimum, that DOT Registry reserves the right to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary to ; (1) to protect the integrity and stability of the registry; (2) to comply with applicable laws, government rules or requirements, or court orders; (3) to avoid any liability, civil or criminal, on the part of DOT Registry, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) to correct mistakes made by the DOT Registry, registry services provider, or any registrar in connection with a domain name registration; (5) during resolution of any dispute regarding the domain; and (6) if a Registrant's pre-authorization or payment fails; or (7) to prevent the

bad faith use of a domain name that is identical to a registered trademark and being used to confuse users.

The Abuse Policy will define the abusive use of domain names to include, but not be limited to, the following activities:

• Illegal or fraudulent actions: use of the DOT Registry's or Registrar's services to violate the laws or regulations of any country, state, or infringe upon the laws of any other jurisdiction, or in a manner that adversely affects the legal rights of any other person;
• Spam: use of electronic messaging systems from email addresses from domains in the TLD to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Web sites and Internet forums;
• Trademark and Copyright Infringement: DOT Registry will take great care to ensure that trademark and copyright infringement does not occur within the .INC TLD. DOT Registry will employ notice and takedown procedures based on the provisions of the Digital Millennium Copyright Act (DMCA) ;
• Phishing: use of counterfeit Web pages within the TLD that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data;
• Pharming: redirecting of unknowing users to fraudulent Web sites or services, typically through DNS hijacking or poisoning;
• Willful distribution of malware: dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and trojan horses.
• Fast flux hosting: use of fast-flux techniques to disguise the location of Web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. Fast flux hosting may be used only with prior permission of DOT Registry;
• Botnet command and control: services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct denial-of-service attacks (DDoS attacks);
• Distribution of pornography;
• Illegal Access to Other Computers or Networks: illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity);
• Domain Kiting⁄Tasting: registration of domain names to test their commercial viability before returning them during a Grace Period;
• High Volume Registrations⁄Surveying: registration of multiple domain names in order to warehouse them for sale or pay-per-click websites in a way that can impede DOT Registry from offering them to legitimate users or timely services to other subscribers;
• Geographic Name: registering a domain name that is identical to a Geographic Name, as defined by Specification 5 of the Registry Agreement;
• Inadequate Security: registering and using a domain name to host a website that collects third-party information but does not employ adequate security measures to protect third-party information in accordance with that geographic area's data and financial privacy laws;
• Front Running: registrars mining their own web and WhoIs traffic to obtain insider information with regard to high-value second-level domains, which the registrar will then register to itself or an affiliated third party for sale or to generate advertising revenue;

- WhoIs Accuracy: Intentionally inserting false or misleading Registrant information into the TLD's WhoIs database in connection with the bad faith registration and use of the domain in question;
- WhoIs Misuse: abusing access to the WhoIs database by using Registrant information for data mining purposes or other malicious purposes;
- Fake Renewal Notices; misusing WhoIs Registrant information to send bogus renewal notices to Registrants on file with the aim of causing the Registrant to spend unnecessary money or steal or redirect the domain at issue.

Domain Anti-Abuse Procedure

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

At all times, DOT Registry will publish on its home website at NIC.INC the Abuse Policy and the contact information for the Abuse Contact. Inquiries addressed to the Point of Contact will be addressed to and received by DOT Registry's Legal Time who will review and if applicable remedy any Complaint regarding an alleged violation of the Abuse Policy. DOT Registry will catalog all abuse communications and provide them to third parties only under limited circumstances, such as in response to a subpoena or other such court order or demonstrated official need by law enforcement.

Any correspondence ("Complaint") from a complaining party ("Complainant") to the Abuse Contact will be ticketed in DOT Registry's CRM software and relayed to DOT Registry's Abuse Team. A member of DOT Registry's Abuse Team will then send an email to the Complainant within forty-eight (48) hours of receiving the Complaint confirming receipt of the email and that DOT Registry will notify the Complainant of the results of the Complaint within ten (10) days of receiving the Complaint.

DOT Registry's Abuse Team will review the Complaint and give it a "quick look" to see if the Complaint reasonably falls within an abusive use as defined by the Abuse Policy. If not, the Contact will write an email to the Complainant within thirty-six (36) hours of sending the confirmation email that the subject of the complaint clearly does not fall within one of the delineated abusive uses as defined by the Abuse Policy and that DOT Registry considers the matter closed.

If the quick look does not resolve the matter, DOT Registry's Abuse Team will give the Complaint a full review. Any Registrant that has been determined to be in violation of DOT Registry policies shall be notified of the violation of such policy and their options to cure the violation.
Such notification shall state:
1) the nature of the violation;
2) the proposed remedy to the violation;
3) the time frame to cure the violation; and
4) the Registry's options to take subsequent action if the Registrant does not cure the violation.
If an abusive use is determined DOT Registry's Abuse Team will alert it's Registry services team to immediately cancel the resolution of the domain name. DOT Registry's Abuse Team will immediately notify the Registrant of the suspension of the domain name, the nature of the complaint, and provide the Registrant with the option to respond within ten (10) days or the domain will be canceled.
If the Registrant responds within ten (10) business days, it'[s response will be reviewed by the DOT Registry's Abuse Team for further review. If DOT Registry's Abuse Team is satisfied by the Registrant's response that the use is not abusive, DOT Registry's Abuse Team will submit a request by the registry services provider to reactivate the domain name. DOT Registry's Abuse Team will then notify the Complainant that its complaint was ultimately denied and provide the reasons for the

denial. If the Registrant does not respond within ten (10) business days, DOT Registry will notify the registry services team to cancel the abusive domain name.

This Anti-Abuse Procedure will not prejudice either party's election to pursue another dispute mechanism, such as URS or UDRP.

With the resources of DOT Registry's registry services personnel, DOT Registry can meet its obligations under Section 2.8 of the Registry Agreement where required to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its TLD. The Registry will respond to legitimate law enforcement inquiries within one (1) business day from receiving the request. Such response shall include, at a minimum, an acknowledgement of receipt of the request, questions, or comments concerning the request, and an outline of the next steps to be taken by Application for rapid resolution of the request.

In the event such request involves any of the activities which can be validated by DOT Registry and involves the type of activity set forth in the Abuse Policy, the sponsoring registrar is then given forty-eight (48) hours to investigate the activity further and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety or providing a compelling argument to the registry to keep the name in the zone. If the registrar has not taken the requested action after the 48-hour period (i.e., is unresponsive to the request or refuses to take action), DOT Registry will place the domain on "serverHold".

Maintenance of Registration Criteria

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

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

While orphan glue often supports correct and ordinary operation of the DNS, we understand that such glue records can be used maliciously to point to name servers

that host domains used in illegal phishing, bot-nets, malware, and other abusive behaviors. Problems occur when the parent domain of the glue record is deleted but its children glue records still remain in the DNS. Therefore, when DOT Registry has written evidence of actual abuse of orphaned glue, DOT Registry will take action to remove those records from the zone to mitigate such malicious conduct.

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

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

WhoIs Accuracy

DOT Registry will provide WhoIs accessibility in a reliable, consistent, and predictable fashion in order to promote Whois accuracy. The Registry will adhere to port 43 WhoIs Service Level Agreements (SLAs), which require that port 43 WHOIS service be highly accessible and fast.

DOT Registry will offer thick WhoIs services, in which all authoritative WhoIs data—including contact data—is maintained at the registry. DOT Registry will maintain timely, unrestricted, and public access to accurate and complete WhoIs information, including all data objects as specified in Specification 4. Moreover, prior to the release of any domain names, DOT Registry's registrar will provide DOT Registry with an authorization code to verify eligible Registrants provide accurate Registrant contact information.

In order to further promote WhoIs accuracy, DOT Registry will offer a mechanism whereby third parties can submit complaints directly to the DOT Registry (as opposed to ICANN or the sponsoring Registrar) about inaccurate or incomplete WhoIs data. Such information shall be forwarded to the registrar, who shall be required to address those complaints with their Registrants. Thirty days after forwarding the complaint to the registrar, DOT Registry will examine the current WhoIs data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or there was some other disposition. If the registrar has failed to take any action, or it is clear that the Registrant was either unwilling or unable to correct the inaccuracies, DOT Registry reserves the right to cancel or suspend the applicable domain name(s) should DOT Registry determine that the domains are being used in a manner contrary to DOT Registry's abuse policy.

DOT Registry shall also require authentication and verification of all Registrant data. DOT Registry shall verify the certificates of incorporation, whether a corporation is in active status, contact information, e-mail address, and, to the best of its abilities, determine whether address information supplied is accurate. Second-level domains in the TLD shall not be operational unless two (2) out of three (3) of the above authentication methods have been satisfied.

With regard to registrars, DOT Registry shall provide financial incentives for pre-authentication of Registrant data prior to such data being passed to the registry. DOT Registry will provide for lower renewal and bulk registration fees in its RRAs

for registrations which have been pre-authenticated and which DOT Registry can rely on as accurate data to be entered into its WhoIs database.

DOT Registry will also maintain historical databases of Registrants and associated information which have provided inaccurate WhoIs information. DOT Registry will endeavor to use this database to uncover patterns of suspicious registrations which DOT Registry shall then flag for further authentication or for review of the Registrant's use of the domain in question to ensure Registrant's use is consonant with DOT Registry's abuse policy.

In addition, DOT Registry's Abuse Team shall on its own initiative, no less than twice per year, perform a manual review of a random sampling of domain names within the applied-for TLD to test the accuracy of the WhoIs information. Although this will not include verifying the actual information in the WHOIS record, DOT Registry will be examining the WHOIS data for prima facie evidence of inaccuracies. In the event that such evidence exists, it shall be forwarded to the registrar, who shall be required to address those complaints with their Registrants. Thirty days after forwarding the complaint to the registrar, the DOT Registry will examine the current WhoIs data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or there was some other disposition. If the registrar has failed to take any action, or it is clear that the Registrant was either unwilling or unable to correct the inaccuracies, DOT Registry reserves the right to suspend the applicable domain name(s) should DOT Registry determine that the Registrant is using the domain in question in a manner contrary to DOT Registry's abuse policy. DOT Registry shall also reserve the right to report such recalcitrant registrar activities directly to ICANN.

Abuse Prevention and Mitigation – Domain Name Access

All domain name Registrants will have adequate controls to ensure proper access to domain functions.

In addition to the above, all domain name Registrants in the applied-for TLD will be required to name at least two (2) unique points of contact who are authorized to request and⁄or approve update, transfer, and deletion requests. The points of contact must establish strong passwords with the registrar that must be authenticated before a point of contact will be allowed to process updates, transfer, and deletion requests. Once a process update, transfer, or deletion request is entered, the points of contact will automatically be notified when a domain has been updated, transferred, or deleted through an automated system run by DOT Registry's registrar. Authentication of modified Registrant information shall be accomplished 48 Hours.

29. Rights Protection Mechanisms

DOT Registry is committed to implementing strong and integrated Rights Protection Mechanisms (RPM). Use of domain names that infringe upon the legal rights of others in the TLD will not be tolerated. The nature of such uses creates security and stability issues for the registry, registrars, and registrants, as well as for users of the Internet in general. DOT Registry will protect the legal rights of others by implementing RPMs and anti-abuse policies backed by robust responsiveness to complaints and requirements of DOT Registry's registrars.

Trademark Clearinghouse

Each new gTLD Registry will be required to implement support for, and interaction with, the Trademark Clearinghouse ("Clearinghouse"). The Clearinghouse is intended to serve as a central repository for information to be authenticated, stored, and disseminated pertaining to the rights of trademark holders. The data maintained in the Clearinghouse will support and facilitate other RPMs, including the mandatory Sunrise Period and Trademark Claims service.

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

Sunrise A Period

DOT Registry will offer segmented Sunrise Periods. The initial Sunrise Period will last [minimum 30 days] for owners of trademarks listed in the Clearinghouse to register domain names that consist of an identical match of their listed trademarks. All domain names registered during the Sunrise Period will be subject to DOT Registry's domain name registration policy, namely, that all registrants be validly registered corporations and all applied-for domains will only be awarded the ".INC" domain that matches or includes a substantial part of the Registrant's legal name. DOT Registry will assign its Rights Protection Team; which is lead by our Director of Legal and Policy and further supported by two dedicated employees to receive and authenticate all Sunrise Registrations.

DOT Registry's registrar will ensure that all Sunrise Registrants meet sunrise eligibility requirements (SERs), which will be verified by Clearinghouse data. The proposed SERs include: (i) ownership of a mark that is (a) nationally or regionally registered and for which proof of use, such as a declaration and a single specimen of current use – was submitted to, and validated by, the Trademark Clearinghouse; or (b) that have been court-validated; or (c) that are specifically protected by a statute or treaty currently in effect and that was in effect on or before 26 June 2008, (ii) optional registry elected requirements concerning international classes of goods or services covered by registration; (iii) representation that all provided information is true and correct; and (iv) provision of data sufficient to document rights in the trademark.

Upon receipt of the Sunrise application, DOT Registry will issue a unique tracking number to the Registrar, which will correspond to that particular application. All applications will receive tracking numbers regardless of whether they are complete. Applications received during the Sunrise period will be accepted on a first-come, first-served basis and must be active corporations in good standing before they may be awarded the requested domain, or able to proceed to auction. Upon submission of all of the required information and documentation, registrar will forward the information to DOT Registry's [RPM Team] for authentication. DOT Registry's [RPM Team] will review the information and documentation and verify the trademark information, and notify the potential registrant of any deficiencies. If a registrant does not cure any trademark-related deficiencies and⁄or respond by the means listed within one (1) week, DOT Registry will notify its registrar and the domain name will be released for registration.
DOT Registry will incorporate a Sunrise Dispute Resolution Policy (SDRP). The SRDP will allow challenges to Sunrise Registrations by third parties for a ten-day period

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

After receiving a Sunrise Complaint, DOT Registry's [RPM Team] will review the Complaint to see if the Complaint reasonably asserts a legitimate challenge as defined by the SDRP. If not, DOT Registry's [RPM Team] will send an email to the Complainant within thirty-six (36) hours of sending the confirmation email that the subject of the complaint clearly does not fall within one of the delineated grounds as defined by the SDRP and that DOT Registry considers the matter closed.

If the domain name is not found to have adequately met the SERs, DOT Registry's [RPM Team] will alert the registrar and registry services provider to immediately suspend the resolution of the domain name. Thereafter, DOT Registry's [RPM Team] will immediately notify the Sunrise Registrant of the suspension of the domain name, the nature of the complaint, and provide the registrant with the option to respond within ten (10) days to cure the SER deficiencies or the domain name will be canceled.

If the registrant responds within ten (10) business days, its response will be reviewed by DOT Registry's [RPM Team] to determine if the SERs are met. If DOT Registry's [RPM Team] is satisfied by the registrant's response, DOT Registry's [RPM Team] will submit a request to the registrar and the registry services provider to unsuspend the domain name. DOT Registry's [RPM Team] will then notify the Complainant that its complaint was ultimately denied and provide the reasons for the denial.

Names secured as described through the Sunrise AT⁄AD processes will result in the registration of resolving domain names at the registry. Names reserved through the Sunrise B process will not result in resolving domain name at DOT Registry. Rather, these names will be reserved and blocked from live use. The applied for string will resolve to an informational page informing visitors that the name is unavailable for registration and reserved from use.

Applications that fit the following criteria will be considered during the Sunrise A period: Applicant owns and operates an existing domain name in another gTLD or ccTLD, in connection with eligible commerce and satisfies the registration requirements described in Section 1.

Sunrise B
Applications that fit the following criteria will be considered during the Sunrise B period:
a) Applicant holds valid trademark registrations or owns rights to a particular name and wishes to block the use of such name.
b) The Applicant must seek to block a name that corresponds to the entire text of its trademark or the complete textual component of a graphical or compound trademark. Certain variances are permitted for trademarks containing spaces or special characters that are not available for domain names.
Any entity, applying for blocks under Sunrise B as a non-member of the sponsored community cannot apply for names in the TLD.

Founder's Program
Applications for the Founder's Program will be accepted after the close of the Sunrise Periods. Potential registrants should understand that certain expectations, as described herein will accompany the issuance of a domain name under the Founder's Program and all registrations resulting from this program will be required to follow the below listed guidelines, which will be further described in their Program Agreement:
a) Registrants awarded a domain through the Founder's Program must use their best efforts to launch a ".INC" website within 30 days of signing the Program Agreement.
b) In addition, each registrant will be required to issue a press release announcing the launch of their ".INC" Founder Website, concurrent with the launch of their .INC Founder Website, said press release must be approved by DOT Registry;
c) Founder's websites should be kept good working order, with unique, meaningful content, user-friendly interfaces, and broad user appeal, for the duration of the License Term,
d) Founders are expected to proactively market and promote ".INC" gTLD in a manner that is likely to produce widespread awareness of the unique advantages gained through the ".INC" string.
e) Founders are expected to participate in reasonable joint marketing initiatives with DOT Registry or its Agents, these would be discussed and mutually agreed upon, given the unique circumstances of each marketing venture.
f) Founders will allow DOT Registry to use in good faith Founder's name, likeness, trademarks, logos, and Application contents (other than Confidential Information,) as well as other Founder information and content as may be mutually agreed, in DOT Registry's marketing, promotional and communications materials.
DOT Registry will randomly verify compliance of the above listed expectations and have the right to revoke any Founder's site, should they be deemed non-compliant.

Additionally, DOT Regsitry may suspend or delete a Founder's site without prior notice to the Registrar or Registrant if the Founder's site is deemed in violation of any of DOT Registry's registration guidelines or policies.
Registrants participating in the Founders program will receive 25% off their initial registration fees, additional discounts may be offered to founders at the time of renewal, should DOT Registry choose to offer additional discounts to founders or term extensions (not to exceed 5 years) DOT Registry will seek advance approval from ICANN via the specified channels.

Landrush
Landrush is a limited time opportunity for companies that want to secure a high value ".INC" name for a small fee (above the basic registration cost). The landrush period will last 30 days. Applications will be accepted and evaluated to determine if they meet the requirements for registration. At the end of the Landrush period domain names with only one application will be awarded directly to the Applicant. Domain names with two or more applications will proceed to a closed mini auction, between the respective Applicants , where the highest bidder wins.

General Availability Period
Applicants must meet registration requirements.
Names will be awarded on a first-come, first serve basis which is determined as of the time of the initial request, not when authentication occurs.

Domain Name Contentions
Name contentions will arise when both a Sunrise A and Sunrise B application are submitted for the same name, the following actions will be taken to resolve the contention.

a) Both Applicants will be notified of the contention and the Sunrise A Applicants will be given first right to either register their requested domain or withdraw their application. Since ".INC" is a sponsored community domain for registered Corporations, a domain applied for under Sunrise A will, all else being equal, receive priority over the identical domain applied for under Sunrise B. Sunrise A names get priority over Sunrise B names.
b) If the Sunrise A Applicant chooses to register their name regardless of the contention, then the Sunrise B Applicant may choose to pursue further action independently of DOT Registry to contest the name.
c) If two Sunrise A Applicants apply for the same domain name (i.e., Delta Airlines and Delta Faucet both seek to be awarded the use of DELTA.INC) then DOT Registry will notify both Applicantts of the contention and proceed to an auction process as described in Section 9.
d) If a Sunrise A Applicant and a Landrush Applicant apply for the same domain name, the Sunrise A Applicant , all else being equal will have priority over the Landrush Applicant .
e) If two Sunrise B Applicants apply for the same domain name (i.e., Delta Airlines and Delta Faucet, both seek to block the use of DELTA. INC), then DOT Registry will accept both applications as valid and block the use of the indicated domain.

Appeal of Rejected Sunrise Applications
An Applicant can file a request for reconsideration within 10 days of the notification of DOT Registry's rejection. Reconsideration can be requested by completing a reconsideration form and filing a reconsideration fee with DOT Registry. Forms, fee information, and process documentation will be available on the DOT Registry website. Upon receipt of the reconsideration form and the corresponding fee, DOT Registry or its Agents will re-examine the application, and notify the Registrant of all findings or additional information needed. The Request for Reconsideration must be submitted through the Registrant's registrar, and a reconsideration fee must be paid to DOT Registry.

Auctions
Sunrise A names found to be in contention as described above will result in Auction. DOT Registry plans to have a qualified third party conduct our auction processes, therefore the rules contained in this document are subject to change based on the selection of an auctioneer:
a) When your auction account is created, it will be assigned a unique bidder alias in order to ensure confidential bidding. The bidder alias will not reflect any information about your account. You may change your bidder alias to a name of your choosing but once set, it cannot be changed again.
b) All auction participants are expected to keep their account information current, throughout the auction process.
c) Auction participants will receive up to date communication from the auctioneer as the auction progresses, bidding status changes, or issues arise.
d) Bidding
i) Auctions will follow a standard process flow: scheduled (upcoming), open and closed.
ii) You will receive an "Auction Scheduled" notice at least ten (10) days prior to the scheduled auction start date. You will receive an "Auction Start" notice on the auction start date, which will indicate that you may begin placing bids through the interface. Once closed, the auction is complete and if you are the winning bidder, you will proceed to the payment process.
iii) If you choose to bid for a particular domain and you are the highest bidder at the end of an auction, you are obligated to complete the transaction and pay the Auctioneer the amount of your winning bid. Carefully consider your bids prior to placing them - bids are not retractable under any circumstances.

iv) If no bids are placed on a particular domain, the Registry will register the domain on behalf of the first customer (in the respective phase) to submit an application through a registrar.

e) Extensions

i) A normal auction period is anticipated to last a minimum of 7 (seven) days. However, in the event of significant auction activity, an auction close may extend during the last twenty-four (24) hours of scheduled operation to better need the volume of the auction.

ii) Auction extensions are meant to provide a mechanism that is fair for bidders in all time zones to respond to being outbid.

iii) An auction extension will occur whenever the auction lead changes in the last twenty four (24) hours of the schedule of an auction. The close will be revised to reflect a new closing time set at twenty four (24) hours after the change in auction lead occurred. Essentially, this means that a winning maximum bid has to remain unchallenged for a period of twenty four (24) hours before the auction will close.

iv) It is important to note that extensions are not simply based on the auction value changing since this could occur as a result of proxy bidding where the same bidder retains their lead. In this case, the maximum bid has not changed, the leader has not changed and therefore no extension will occur.

f) Payment Default

In the event that you as the winning bidder decide not to honor your payment obligations (or in the event of a reversal of payment or a charge back by a credit card company or other payment provider) on any outstanding balance, the Registry has the right to cancel any⁄all of your winning registrations for any .INC domain name, regardless of whether they have been paid for or not. You do not have the right to "pick and choose" the names you wish to keep or not keep. Winning an auction creates an obligation to remit payment. Failure to remit payment is a breach of your agreement. You will lose any previously won domains and will no longer be allowed to bid on any current or future auctions sponsored by DOT Registry. Participants are encouraged therefore to consider carefully each bid submitted as any bid could be a winning bid.

Trademark Claims Service

DOT Registry will offer a Trademark Claims Service indefinitely to provide maximum protection and value to rights holders. The Trademark Claims Service will be monitored and operated by DOT Registry's RPM Team that will receive all communications regarding the Trademark Claims Service and catalog them. DOT Registry's registrar will review all domain name requests to determine if they are an identical match of a trademark filed with the Trademark Clearinghouse. A domain name will be considered an identical match when the domain name consists of the complete and identical textual elements of the mark, and includes domain names where (a) spaces contained within a mark that are either replaced by hyphens (and vice versa) or omitted; (b) certain special characters contained within a trademark are spelled out with appropriate words describing it (e.g., @ and &); and (c) punctuation or special characters contained within a mark that are unable to be used in a second-level domain name are either (i) omitted or (ii) replaced by spaces, hyphens or underscores. Domain names that are plural forms of a mark, or that merely contain a mark, will not qualify as an identical match.

If the registrar determines that a prospective domain name registration is identical to a mark registered in the Trademark Clearinghouse, the registrar will be required to email a "Trademark Claims Notice" (Notice) in English to the protective registrant of the domain name and copy DOT Registry's RPM Team The Notice will provide the prospective registrant information regarding the trademark referenced in the Trademark Claims Notice to enhance understanding of the Trademark rights being claimed by the trademark holder. The Notice will be provided in real time without

cost to the prospective registrant.

After receiving the notice, the registrar will provide the prospective registrant five (5) days to reply to the Trademark Claims Service with a signed document that specifically warrants that: (i) the prospective registrant has received notification that the mark is included in the Clearinghouse; (ii) the prospective registrant has received and understood the notice; and (iii) to the best of the prospective registrant's knowledge the registration and use of the requested domain name will not infringe on the rights that are the subject of the notice. If the warranty document satisfies these requirements, the registrar will effectuate the registration and notify DOT Registry's RPM Team.

After the effectuation of a registration that is identical to a mark listed in the Trademark Clearinghouse, the registrar will provide clear notice to the trademark owner consisting of the domain name that has been registered and copy DOT Registry's RPM Team. The trademark owner then has the option of filing a Complaint under the Uniform Domain Name Dispute Resolution Policy (UDRP) or the Uniform Rapid Suspension System (URS).

Uniform Rapid Suspension System (URS)

DOT Registry will specify in the Registry Agreement, all RRAs, and all Registration Agreements used in connection with the TLD that it and its registrars will abide by all decisions made by panels in accordance with the Uniform Rapid Suspension System (URS). DOT Registry's RPM Team will receive all URS Complaints and decisions, and will notify its registrar to suspend all registrations determined by a URS panel to be infringing within a commercially reasonable time of receiving the decision. DOT Registry's RPM Team will catalog all abuse communications, but only provide them to third-parties under limited circumstances, such as in response to a subpoena or other such court order or demonstrated official need by law enforcement.

Uniform Domain Name Dispute Resolution Policy (UDRP)

DOT Registry will specify in the Registry Agreement, all Registry-Registrar Agreements, and Registration Agreements used in connection with the TLD that it will promptly abide by all decisions made by panels in accordance with the Uniform Domain Name Dispute Resolution Policy (UDRP). DOT Registry's RPM Team will receive all UDRP Complaints and decisions, and will notify its registrar to cancel or transfer all registrations determined to by a UDRP panel to be infringing within ten (10) business days of receiving the decision. DOT Registry's [RPM Team] will catalog all abuse communications, but only provide them to third-parties under limited circumstances, such as in response to a subpoena or other such court order or demonstrated official need by law enforcement.

Proven Registrars

In order to reduce abusive registrations and other activities that affect the legal rights of others, DOT Registry will only contract with ICANN-accredited registrars. The registrar, according to the RRA, will not be able to register any domain names, thus eliminating the possibility of front-running.

Pre-Authorization and Authentication

Registrant authentication shall occur in accordance with the registration eligibility criteria and the Anti-Abuse Policy for .INC as set forth in Question 28.

The verification process is designed to prevent a prospective registrant from

providing inaccurate or incomplete data, such that, if necessary, the registrant can be readily contacted regarding an infringing use of its site; indeed, the process (including verification of a registrant's certificate of incorporation) is designed to ensure that only qualified members of the community are permitted to register in the TLD.

DOT Registry will not permit registrants to use proxy services.

Thick WhoIs

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

Grace Period

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

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

Takedown Procedure

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

At all times, DOT Registry will publish on its home website at NIC.INC contact information for receiving rights protection complaints (Complaint) from rights holders, including but not limited to trademark and copyright Complaints. Complaints will be addressed to and received by DOT Registrys RPM Team who will catalogue and ticket in DOT Registry's CRM software and review as outlined herein. DOT Registry will catalog all rights protection communications and only provide them to third parties under limited circumstances, such as in response to a subpoena or other such court order or demonstrated official need by law enforcement.

Any Complaint from a rights holder will be relayed to DOT Registry's RPM Team. A member of DOT Registry's RPM Team will then send an email to the Complainant within forty-eight (48) hours of receiving the Complaint confirming receipt of the email, and that DOT Registry will notify the Complainant of the results of the Complaint within (10) days of receiving the Complaint.

After sending the confirmation email, DOT Registry's RPM Team will review the Complaint. If DOT Registry or its registrar determines that the registration was in bad faith, DOT Registry or its registrar may cancel or suspend the resolution of the domain name. Bad faith registration includes, but is not limited to, the registration of a domain identical to a registered trademark where the registrant has proceeded with registration after receipt of a Clearinghouse notice, as described above.

If the registrant responds within ten (10) business days, its response will be

reviewed by the DOT Registry's RPM Team If DOT Registry's RPM Team is satisfied by the registrant's response that the content has been taken down or is not infringing, DOT Registry's RPM Team will unsuspend the domain name. DOT Registry's RPM Team will then notify the Complainant that its complaint was ultimately denied and provide the reasons for the denial. If the registrant does not respond within ten (10) business days, DOT Registry or its registrar may cancel or suspend the resolution of the domain name.

This Takedown Procedure will not prejudice any party's election to pursue another dispute mechanism, such as URS or UDRP, as set forth in DOT Registry's response to Question 28.

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

30.(a).1 Security Policies

DOT Registry and our back-end operator, Neustar recognize the vital need to secure the systems and the integrity of the data in commercial solutions. The ".INC" registry solution will leverage industry-best security practices including the consideration of physical, network, server, and application elements.

Neustar's approach to information security starts with comprehensive information security policies. These are based on the industry best practices for security including SANS (SysAdmin, Audit, Network, Security) Institute, NIST (National Institute of Standards and Technology), and CIS (Center for Internet Security). Policies are reviewed annually by Neustar's information security team.

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

1. Summary of the security policies used in the registry operations

2. Description of independent security assessments

3. Description of security features that are appropriate for ".INC"

4. List of commitments made to registrants regarding security levels

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

30.(a).2 Summary of Security Policies

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

-The policies for internal users and our clients to ensure the safe, organized and fair use of information resources.

-The rights that can be expected with that use.

-The standards that must be met to effectively comply with policy.

-The responsibilities of the owners, maintainers, and users of Neustar's information resources.

-Rules and principles used at Neustar to approach information security issues

The following policies are included in the Program:

1. Acceptable Use Policy

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

2. Information Risk Management Policy

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

3. Data Protection Policy

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

4. Third Party Policy

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

5. Security Awareness and Training Policy

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

6. Incident Response Policy

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

7. Physical and Environmental Controls Policy

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

8. Privacy Policy

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

9. Identity and Access Management Policy

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

10. Network Security Policy

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

11. Platform Security Policy

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

12. Mobile Device Security Policy

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

13. Vulnerability and Threat Management Policy

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

14. Monitoring and Audit Policy

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

15. Project and System Development and Maintenance Policy

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

30.(a).3 Independent Assessment Reports

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

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

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

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

-Identification of key systems for further exploitation is conducted

-Exploitation of the identified systems is attempted.

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

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

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

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

-Include annual independent review of information security practices

-Include annual external penetration tests by a third party

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

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

practices

-Are aligned with all aspects of ISO IEC 17799

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

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

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

30.(a).5 Commitments and Security Levels

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

Compliance with High Security Standards

-Security procedures and practices that are in alignment with ISO 17799

-Annual SOC 2 Audits on all critical registry systems

-Annual 3rd Party Penetration Tests

-Annual Sarbanes Oxley Audits

Highly Developed and Document Security Policies

-Compliance with all provisions described in section 30.(b) and in the attached security policy document.

-Resources necessary for providing information security

-Fully documented security policies

-Annual security training for all operations personnel

High Levels of Registry Security

-Multiple redundant data centers

-High Availability Design

-Architecture that includes multiple layers of security

-Diversified firewall and networking hardware vendors

-Multi-factor authentication for accessing registry systems

-Physical security access controls

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

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

-DDoS mitigation using traffic scrubbing technologies

Annex B

Business Entity Search

Date: 02/25/2014

Be advised the business information on this page is for summary informational purposes only. It is not an official filing with the Secretary of State's office and should not be relied on as such. Please view actual documents filed by customers with the secretary of State's office to ensure accurate information. When filing a Uniform Commercial Code statement on an entity, consult with your attorney to ensure the correct debtor name.

Business Summary

Current Entity Name	Business Entity ID Number
ECYBER SOLUTIONS GROUP INC	6063101
File Name Change Online	View History and Documents

Current Mailing Address: 13006 RUSSELL ST, OVERLAND PARK, KS 66209 Update

Business Entity Type: KANSAS FOR PROFIT CORPORATION

Date of Formation in Kansas: 09/30/2005

State of Organization: KS

Current Status: ACTIVE AND IN GOOD STANDING

Certificate of Good Standing

Resident Agent and Registered Office

Resident Agent: YEHIELA GERSHOM

Registered Office: 5925 Nall Avenue Suite 400, MISSION, KS 66209

Update Resident Agent/Office

Annual Reports

The following annual report information is valid for active and delinquent status entities only.

Tax Closing Month: 12

The Last Annual Report on File: 12/2012

Next Annual Report Due: 04/15/2014 File Online

Forfeiture Date: 07/15/2014

Close Your Business

Be advised the business information on this page is for summary informational purposes only. It is not an official filing with the Secretary of State's office and should not be relied on as such. Please view actual documents filed by customers with the secretary of State's office to ensure accurate information. When filing a Uniform Commercial Code statement on an entity, consult with your attorney to ensure the correct debtor name.

Annex C

eCyber Solutions

13006 Russell St
Shawnee Mission, Kansas 66209
United States

Basic Profile

eCyber Solutions

eCyber Solutions is a dynamic company in Software Development & Design industry. eCyber Solutions is committed to filling the needs of ...

Company name: eCyber Solutions

Address: 13006 Russell St, Shawnee Mission, Kansas 66209, United States
View map

Employees: 5 - 10

Website: http://www.ecybersolutions.com

About eCyber Solutions:
eCyber Solutions is a complete Internet and Multimedia design firm specializing in innovative uses of technology. We ...

Business Profile

eCyber Solutions

eCyber Solutions is a supplier of turnkey e-commerce solutions in Shawnee Mission. eCyber Solutions consists several other services in ...

Annual Revenue: $1 mil. - $5 mil.

Industry: Software Development & Design, Software.

Products: turnkey e-commerce solutions, web development tools.

Top Competitors in Shawnee Mission

for eCyber Solutions

Searching for companies like eCyber Solutions? In Shawnee Mission, not just eCyber Solutions, there are also some companies similar to ...

eCyber Solutions

13006 Russell St
Shawnee Mission, Kansas 66209
United States

Products & Services: turnkey e-commerce solutions, web development tools, ...

Share it

Popular local services in Shawnee Mission

- Shawnee Mission industrial products (1)
- Shawnee Mission General farms (1)
- Shawnee Mission Miscellaneous retail stores (3)
- Shawnee Mission Commercial printing (10)
- Shawnee Mission Auditing (7)
- Shawnee Mission bookkeeping services (7)
- Shawnee Mission Industrial and personal service paper (3)
- Shawnee Mission Engineering services (2)
- Shawnee Mission Water supply (1)
- Shawnee Mission healthcare information consulting (1)

Popular companies in turnkey e-commerce solutions

- CLEVELAND turnkey e-commerce solutions (1)
- Shawnee Mission turnkey e-commerce solutions (1)
- Columbus turnkey e-commerce solutions (1)
- Deerfield Beach turnkey e-commerce solutions (1)

Popular companies in Shawnee Mission

- Robert Thomas CPA LLC
- SmallBizAccountants.com
- Benchmark Biolabs Inc

Donegan Optical Company, Incorporated

Chris-Leef General Agency Inc

Waddell & Reed Inc

SPARHAWK LABORATORIES INC

Dwyer Dykes & Thurston Lc

BayerDVM.com

IKE & ASSOCIATES, INC.

Top Competitors in United States

for eCyber Solutions

Explore more companies similar to eCyber Solutions in United States to get more choices. Companies like eCyber Solutions usually offer ...

eCyber Solutions

13006 Russell St
Shawnee Mission, Kansas 66209
United States

Products & Services: turnkey e-commerce solutions, web development tools, ...

Explore more

about eCyber Solutions

Want to know more about eCyber Solutions and explore more rich eCyber Solutions company information? Such as eCyber Solutions's main ...

Additional eCyber Solutions information

Browse eCyber Solutions company information on CompanyInfo. If you are a sales professional, marketer or recruiter, you may get eCyber Solutions's fresh and accurate sales leads, and business eCyber Solutions's contact information.

You will also access to the latest company, industry, and contact information you need about eCyber Solutions to set sales strategy, prepare for calls to eCyber Solutions, and enhance product positioning with industry and competitor insight.

In eCyber Solutions profile, you can also get more relevant industry suppliers, find more eCyber Solutions evaluation information and identify new market opportunities with companies like eCyber Solutions.

...

About US
New Coming Companies
Business Press Release
Business Trade Shows
Job Centers
Global Tenders
App News
Business Headlines
Tech News Express

US Companies Profiles
DUNN NURSERY AND GREENHOUSES
Evergreen Farms Inc
STAGECOACH FARMS
Delaplaine Seed Co
JONESBORO BOLT AND SUPPLY INC
Field Concepts LLC
Pumpkin Hollow LLC
Animals Benefit Club

Canada Companies Profiles
Airport Corporate Centre
Dixie Animal Hospital
American Radiolabeled Chemicals Inc
Norlock Refrigeration
Acorn Graphics Ltd
Growth Financial Services Corp
Car-Ber Testing Services Inc
Abrams & Krochak

Popular Local Services
Tuscaloosa Business Services
Northport Leather Goods
Alma Vegetables
Dewitt Rice
Camden Hardware Stores
Scottsdale Animal Specialty Services
Tempe Citrus Fruits
Los Angeles Candy

New gTLD Application Submitted to ICANN by: Dadotart, Inc.

String: art

Originally Posted: 13 June 2012

Application ID: 1-1097-20833

Applicant Information

1. Full legal name

Dadotart, Inc.

2. Address of the principal place of business

7080 Hollywood Boulevard
Los Angeles CA 90028
US

3. Phone number

323 645 6034

4. Fax number

323 645 6001

5. If applicable, website or URL

Primary Contact

6(a). Name

Joshua Wattles

6(b). Title

Advisor in Chief

6(c). Address

6(d). Phone Number

323 645 6034

6(e). Fax Number

323 645 6001

6(f). Email Address

josh@deviantart.com

Secondary Contact

7(a). Name

Mr. Michael David Palage

7(b). Title

Consultant

7(c). Address

7(d). Phone Number

561 744 6453

7(e). Fax Number

7(f). Email Address

michael@palage.com

Proof of Legal Establishment

8(a). Legal form of the Applicant

Corporation

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

Delaware, United States of America

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

Andrew McCann	Director
Angelo Sotira	Director
Steven Gonzalez	Director

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

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

DeviantART, Inc.	Not Applicable

11(d). For an applying entity that does not have directors, officers,

partners, or shareholders: Name(s) and position(s) of all individuals having legal or executive responsibility

Applied-for gTLD string

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

art

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.

Q16 - Operational or Rendering Considerations with Regard to the gTLD String

The .ART Registry (and CORE Internet Council of Registrars as its technical provider) ensured that there are no known operational or rendering problems concerning the applied-for gTLD string ”ART”.

Since the gTLD string ”ART” is an ASCII-only string, it is safe to assume that, just like with existing ASCII-only TLD strings like .com, .net or .de, no operational or rendering problems may be expected. In particular, the name consists only of ASCII characters that are already used for existing top level domains; all the characters in the name are even used in the leftmost position of existing TLD labels. In order to confirm this, CORE Internet Council of Registrars conducted a thorough research regarding whether operational or rendering issues occurred for any existing ASCII-only top level domain in the past. The results of this research confirmed the assumption.

Since the registry does not support right-to-left scripts on the second level, bi-directional issues (like the ones described at http://stupid.domain.name/node/683) will not occur.

Moreover, the gTLD string exclusively uses characters from a single alphabet, does not contain digits or hyphens, and it contains characters that are not subject to homograph issues, which means there is no potential for confusion with regard to the rendering of other TLD strings.

Finally, CORE Internet Council of Registrars set up a testing environment for the .ART TLD using the CORE Registration System, including an EPP SRS, Whois and DNS servers, in order to conduct a series of tests involving typical use cases (like web

site operation and e-mail messaging) for a TLD. The tests revealed no operational or rendering issues with any popular software (web browsers, e-mail clients) or operating systems.

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 AND PURPOSE OF THE .ART gTLD

Dadotart Inc. ("Dadotart") is submitting this application on behalf of the Arts community, which it regards as Artists and those who have an identifiable engagement with the Arts worldwide. This naturally evolving community is the community represented by Dadotart in its application for the extension, .ART. The community is not static just as the arts themselves never stand still. Art is both a reflection of culture and an integral part of human endeavor. The .ART gTLD would advance the connection of the arts with technology, which in turn will heighten the relevancy of both.

Dadotart is a new organization formed expressly to lead the formation a specialized gTLD devoted to the Arts community. Dadotart is owned and directed by deviantArt (dA), the innovator in creating an entirely Arts-focused community online. dA was formed in 2000 and is headquartered in Los Angeles with employees located around the globe. dA is an Internet-based platform, community and network whose registered members total more than 20 million users, living in essentially every country of the world. In almost 12 years of operation the members of the dA online community have produced and uploaded ––one at a time — nearly 200 million pieces of Art representing genres spanning essentially all known forms of Artistic expression, and many that did not exist prior to the introduction of digital production and sharing. Members of deviantART span all demographic sectors and consist of both artists and those who are drawn to the arts.

dA has proven itself as a community-builder forming a new context for the arts that empowers artists and art lovers through their aggregation and integration, using the Internet at arguably its best application: drawing dispersed populations into hubs of concurrent interest. The term "deviant" in the name deviantART is intended to invoke a quotation from the brilliant 20th century musician and innovator, Frank Zappa, who said: "Without deviation from the norm, progress is not possible." dA is committed to the full breadth of expression and participation in the arts that can be supported by the Internet—the great innovation in communications. DA's success reaching over 60 million unique visitors a month demonstrates the viability of placing the arts within this brilliant technology. The launch of Dadotart and the .ART gTLD are an integral extension of the work of dA and its mission to support the Arts community worldwide.

The .ART gTLD will serve as a trusted, hierarchical, and intuitive namespace for the global Arts community which has been defined for the purposes of this application to include Artists and those who are engaged in the Arts worldwide. All

domain names registered within the .ART gTLD will be required to comply with the following tree policies: (1) Registrant Eligibility (who can register within the .ART gTLD); (2) Name Selection Criteria (what domain names can be registered); and (3) Authorized Usage Policy (how the domain names can be used). This umbrella of policies will provide the arts community the confidence that the .ART gTLD can be operated on behalf of the global Arts community. The registry will incorporate both active and passive safeguards into its operation to ensure that these registrants continue to abide by the terms and conditions set forth in the registration agreement.

18.1.2 Dadotart Legacy as a Trustee to the Global Art Community
Dadotart mission is first to unite, support and promote Artists and those who are engaged in the Arts worldwide. Second, its mission is to use the .ART gTLD for the co-ordination and protection of the community's common aims and interests, communication, co-operation and establishment of core indentity on the Internet, while at the same time conserving and respecting the autonomy of individuals and organizations in the arts. One of the main objectives is to unite and support the Arts community through common identity and to encourage and facilitate knowledge sharing through communication, and by providing expertise in relevant areas. Dadotart aims to increase the visibility of those involved in the arts by establishing and enabling various Art groups, online environments and venues devoted to the Arts community.

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

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

The key benefits to all stakeholders of the .ART gTLD are derived from the intrinsic link of the TLD string to the Art community, and they include:

- The specificity and applicability of its policies to the values embodied by the Art community;
- The support and enhancement of relationships among Artists, audiences, collectors, art institutions, art educators, arts organizers and art sponsors;
- The ability to design and develop the name space from inception; and
- A clear accountability to the Art community.

The specificity and applicability of the .ART gTLD string and the gTLD policies, will enable registrants to communicate in a way that demonstrates their commitment to Art. Thanks to reduced contention potential because the TLD is reserved for the Art community, an Art community member is more likely to be able to register a name that matches her⁄his⁄its needs.

The ability to design and develop a planned portion of the name space creates a strong base of predictable and memorable names that will facilitate access to key resources for users. Predictability relates to both the choice of the name and the content the user may expect from a name corresponding to a certain pattern.

With the planned reservation of key names and their controlled allocation, other names registered on a first-come-first-served basis will generally be highly memorable and predictable. The launch process and the community nexus compliance program are designed to achieve a high degree of relevance of .ART domain names for the artists, performers, organizers, sponsors and protectors of Art.

The focus on Artists and online communication in the .ART gTLD community facilitates clear and easy communications from, to and within the Art community. It also creates value for consumers of the Arts by establishing the meaning and reputation of the domains ending in .ART.

Because the arts themselves generate immensely valuable intellectual properties the .ART TLD will have a policy providing strong intellectual property support, including strong protections against ambush marketing (the illegitimate use of advertising opportunities related to a Art and Artists).

This provides high value to local and international trademark holders whose brands are intrinsically Art-related: for those who use it, it is a token of legitimate use based on the production or other forms of contribution to Art. For those who do not wish to register names under .ART, defensive registrations are unnecessary thanks to the high degree of protection against trademark infringement in the .ART registration policy. For Internet users interested in Art, it facilitates intuitive access to the Art content they are interested in. Conversely, for organizers of Art, be they associations, schools, art galleries or dealers and collectors, it helps establish an easy-to find channel to their members, audiences, consumers and for the public at large. Since copyright and moral rights are fundamentally author and artist generated rights, the .ART gTLD will become synonymous with respectful attention to intellectual property rights and author's rights as applied in the arts and a welcome vehicle for educational outreach within the arts on the subject.

It is critical to understand that the distinctiveness of the .ART gTLD provides registrants, as artists or as art-centric organizations, with a pure opportunity to establish authentic identity on the Internet for themselves. The .com TLD suggests commercial endeavors that many in the arts do not identify themselves as pursuing. The .net TLD suggests an emphasis on technology, which may be a contradiction to many artistic pursuits. The .org TLD suggests an identity to an organization, which for many artists defeats the whole experience of being in the arts. Country-specific TLDs limit the ability of the arts, as a matter of identity, to soar beyond borders and contribute to world cultural development.

Art is universal and providing identity to the arts is a universal good.

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

The goal of the .ART gTLD is the focus on the needs of the Art community as defined in these answers. Service levels will match or exceed the high end of currently existing TLDs. The support of the .ART gTLD by CORE, and CORE's strong service record, is evidence of the high value placed on service levels and reputation and what can be expected with the .ART gTLD. The .ART gTLD registry will vigorously build and defend the reputation of .ART as an orderly and progressive TLD for the Art community.

18.2.1.1 Potential Business Models

For the creation, operation and funding of the .ART gTLD, Dadotart has partnered with CORE Association ("CORE"), an international not-for-profit organization based in Geneva, Switzerland, aiming to operate TLDs in the public trust. CORE has been among the promoters of the .museum gTLD. Dadotart is still analyzing potential use case options on the type of domain names that will be permitted to be registered, by whom and when registration will be permitted for defined domain name types. This analysis will also be undertaken by an independent Policy Advisory Board (PAB) supported by Dadotart and CORE, for the purpose of recommending policy and best

practice advice for the .ART gTLD and for any other Art-themed gTLD that may later wish to voluntarily adopt its best practices.

It is anticipated that the PAB will provide an opportunity for leading world arts organizations and prominent artists to participate in key advisory capacities during the decision making process. Dadotart and CORE will approach The Getty Trust, the UNESCO secretariat, international associations for artists, musicians, photographers, dancers, and authors, cultural ministers and major art associations such as ART Basel and the World Monuments Fund to provide representatives on the PAB (or for greater levels of participation).

The current best thinking on potential business models includes the following elements. First, Dadotart is keenly aware that any new gTLD must be seeded with relevant content to drive traffic and build consumer recognition and trust. Having closely evaluated the dotAsia Pioneering program which was incorporated into the launch of the .ASIA gTLD, it is critical that this content be available as soon as possible and ideally before any general registration periods. Dadotart would ideally like to launch a series of information portals shortly after delegation. These portals in addition to driving awareness and recognition within the community, will also provide appropriate IT staff to test for a seamless and secure access to .ART domain names.

Second, as noted above, the .ART gTLD will incorporate the following minimal safeguards into any business model at the time of launch: Registrant Eligibility; Name Selection Criteria; and Authorized Usage. In addition, the current best thinking involves the initial reservation of domain names falling within three types:

(1) Names denoting genres, sub-genres or fields of activity and interests (e.g. theatre, sculpture, painting, photography, drawing, cgi, curation, etc.);

(2) In addition, a second reserved list of names of prominent Art institutions and organizations as well as Art-related and adjacent trademarks will be created; and

(3) Names of prominent Artists living or dead.

The exact composition of this reserve list will be compiled with the assistance and guidance of the PAB. There will also be a corresponding policy that will set forth the specific policy by which these reserved domain names can be registered by the appropriate entity.

Domain name registration is planned to occur on both the second and third level: at the second level (e.g. Stella.ART) and at the third level (e.g. Stella.Sculpture.ART). The PAB will define policies to ensure that name spaces are managed in accordance with all policies and in accordance with the interests of service to the Arts community. Registrant Eligibility criteria at the second level within the .ART gTLD will be deferred to PAB for development and later adoption by Dadotart. The universe of registrants that could potentially be permitted to register in accordance with any final Registrant Eligibility criteria at either the second or third level include, Artists and those who have an identifiable engagement with the Arts.

All domain names within the .ART name space would be subject to suspension and or cancellation upon the violation of the terms and conditions set forth in the domain name registration agreement. In addition, the registry will incorporate both active and passive safeguards into its operation to ensure that these registrants continue to abide by the terms and conditions set forth in the registration agreement.

Following these operational best practices, Dadotart believes that the following goals and objectives can be realized.

- Provide a trusted, hierarchical, and intuitive namespace for the art community;
- Facilitate digital communication, from, to and within the art community;
- Provide a platform for the development in the digital space of the Art community;
- Promote the values of Art; and

- Allow the Arts to expand its daily relevance and influence in the Internet culture itself.

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

The Art TLD will create a name space specific to the Art community including, artists, audiences, educators, institutions, organizers, associations, sponsors and consumers of Art. The Art community has considerable economic and cultural significance in all parts of the world. The .ART TLD will therefore fill a large gap in terms of online choice. From a competition standpoint, it creates a level playing field with respect to the market power of large unspecific TLDs. It is naturally differentiated by its scope, by its governance model and by its intrinsic meaning as against other TLDs. Innovation is greatly enhanced by the proactive structured development of the name space. The development process involves an open process with the PAB identifying purpose-built community-specific services based on designated portions of the .ART name space. This approach turns worldwide resource to the benefit of the Art community and for the advancement of the global Internet.

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

Compared to most existing TLDs, the .ART user experience will greatly enhance predictability and memorability of domain names. The community-based focus, the orderly development process and strong intellectual property support ensure that users will generally find the services they are looking for under the names they intuitively tend to use for them.

In particular, the names genres, traditions, artists and crafts-people, as well as the acronyms of international and national Art institutions and associations, the names of Art disciplines, key terms related to various Art disciplines, the names of Art clubs, as well as important slogans or keywords for Art will be identified and registered in an organized and controlled framework. This affords users a high degree of certainty that they will find, or have found, an intended Art-related resource if the domain name ends in .ART.

Users will have greater comfort flowing from the context of naming variants: in key portions of the .ART name space, alternative names and variants (redirected to the canonical forms) will systematically be activated. Users in the Art community will be able to get accustomed to the predictability of .ART domain names. As a result, they also avoid stumbling upon typo-squatting, robotized pay-per-click traps or domain-for-sale pages.

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

The registration policies are best seen along the anticipated phases of the launch: (1) creation of the PAB; (2) pre-launch phase, launch phase and; (3) general availability.

Prior to launch the PAB will be formed, a secretariat created and initial policies drafted along with a detailed implementation plan. It is anticipated that policies will be created governing:

(1) Registration eligibility with nexus rules;
(2) Name selection;
(3) Name use;
(4) Creation of the reserved lists noted above;

(5) Allocation of names placed on reserved lists;
(6) Protection for two-letter country codes at the second level; and
(7) Revocation.

During pre-launch, a limited number of names will be registered to be used for promotion of the .ART gTLD and for testing of the portals built around those names. Projects and content provision commitments will be sought and negotiated, especially for key public-interest portions of the name space built during this phase. All potential registrants and mandate holders will be subject to screening and thorough pre-validation.

During the launch phase, all registrations will be pre-validated; launch phase pre-validation depends on priority status (public service, trademark, no prior rights) but will always involve community nexus.

During the phase of general availability, community nexus will be subject to post-validation by way of an extensive compliance program. The ongoing compliance program will regularly be adapted to current needs based on experience and audit findings. Community nexus validation combined with strong protection of trademarks will help to stamp out cybersquatting and abusive registrations.

18.2.5 Will your proposed gTLD impose any measures for protecting the privacy or confidential information of registrants or users? If so, please describe any such measures

The protection of privacy and confidential information of registrants and users will comply with applicable Law, in particular the European Data Protection framework. Within the bounds of applicable regulations, the registry will implement anti-data mining measures by way of rate limitation, authenticated access or white-listing⁄black-listing, as well as tools to prevent unauthorized recourse to repetitive automated access.

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

The .ART gTLD will create and use specific outreach programs to achieve the .ART gTLD goals in each of its phases. Since dA can be described as primarily a vehicle that uses the Internet for outreach and communication to artists, the .ART gTLD will draw on the skills and experience of dA to deliver the best possible outreach and communications.

The outreach that dA is capable of bringing to bear can be judged simply by the metrics that define its current stature as the largest arts community on the Internet:

- It covers more than 4,500 categories of art;
- Over 20,000,000 registered members;
- Over 60,000,000 million unique visitors per month;
- Over 100,000 daily uploads of original art works;
- Over 1,250,000 comments a day;
- Artists ranging from seasoned professionals to beginners from all countries of the world; and
- Nearly 200,000 self-identified groups comprised of site members.

PAB Creation Phase—In order to ensure representation of the full spectrum of the Arts community, Dadotart will seek nominations to the PAB from established arts associations and institutions, cultural organizations as well as from the online art community. Once the PAB is formed and its initial members defined the PAB

secretariat will work with the PAB to define all necessary registration, name selection and name use policies.

Pre-launch Phase—The pre-launch phase will involve implementation of all policies as well as the development of test websites and portals using .ART domain names. These portals will disseminate information on launch and registration. They will foster the intuitive usability of the .ART gTLD with a focus on the needs of the Art community. Once these domain names are active, they become an outreach mechanism in their own right because they establish the touch-and-feel of the .ART gTLD in the minds of the users.

Launch and Ongoing Registration Phase—The launch and ongoing registration phase will involve outreach mechanisms that specifically leverage participation by local artists, organizations, institutions and locally relevant trademarks and local communications mechanisms.

Promotion codes distributed through community-specific channels will serve as an ongoing form of outreach available at any time. They are also a low-cost method to achieve community nexus and to prevent abusive registrations.

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

18.3.1 What operating rules will you adopt to eliminate or minimize social costs (e.g., time or financial resource costs, as well as various types of consumer vulnerabilities)?

Dadotart believes the proposed operating rules that undertake to initially reserve key names including trademarks, as well as its proposed policies on eligibility, name selection and name use will provide clarity and predictability to name registration, thereby reducing social costs. In full operation the .ART gTLD will provide a trusted online environment for the arts community. There should be no need for other trademark and brand owners to defensively register in the gTLD. This verified eco-system also provides consumers with a single trusted source for arts information and communication. Dadotart also believes that the safeguards set forth in the Applicant Guidebook and the proposed business modeled outlined in Sections 18.1 and 18.1.2 and the policies planned and noted in 18.2.4 will minimize and potential negative social costs.

18.3.2 What other steps will you take to minimize negative consequences/costs imposed upon consumers?
Dadotart believes that the proposed operation of the .ART gTLD as set forth in this application has no known negative consequences or cost implications for consumers. To the contrary, the proposed operation of this registry will likely lead to direct and quantifiable benefits to consumers. Dadotart believes that by following the core values as identified in Section 18.2 it will be able provide real value to the consumer and minimize any potential negative consequences/costs.

More particularly, the three phases of PAB creation, pre-launch, and launch and ongoing registration of the .ART gTLD are designed to minimize social costs and negative externalities. They protect potential registrants and potentially affected parties while maximizing the value of the name space to its registrants and users.

This approach is based on the premise that extensive screening efforts by the registry in the early stages will create a fair and orderly name space with lower compliance costs in the long term.

18.3.3 How will multiple applications for a particular domain name be resolved, for example, by auction or on a first-come/first-serve basis?
In phases and areas where the first-come-first-served principle tends to yield perverse results, alternative modes will be used.

(1) In the PAB creation phase community research will identify names to be entered into reserved lists and the rules by which they will be allocated;
(2) In the pre-launch phase key portal names of use to the entire community will be registered and used for communication and outreach; and
(3) A launch phase led by protection for and registration by trademark holders and those eligible to hold names on reserved lists.

It is anticipated that the pre-launch portal development program identified in (2) above will involve key participants in the Art Community. The portal development program will allocate domain names based on an open and transparent project selection process. This process is highly economical in terms of social costs and yields substantial external benefits.

The portal development program is an essential part of .ART outreach. It begins before delegation of the TLD. In terms of workload and it mainly affects proposers who themselves are required to demonstrate support for their projects. Support will be required to come from the segment of the community concerned with the respective portion of the name space. Given the high value of the resulting on-line resources for the community and the public interest, and given the economic benefits that can be derived from their operation, the administrative effort is largely justified. To further protect affected parties, all adjudications in name space mandates have a safety-valve clause, allowing for later adjustments based on community input. The principle of the safety-valve is that affected parties can obtain adjustments to a component of a mandate if they propose (and commit to) an improved use of the underlying domain names from a public interest perspective.

The launch programs referred to in (3) above combine the so-called “sunrise” and “landrush” processes simultaneously in one phase. The use of domain applications instead of domain registrations means that the registry accepts multiple applications the same domain name. (By contrast, only a single registration can exist for a given domain.) In this way, contention resolution can take place without time pressure in a transparent, fair and orderly manner.

At the time of ongoing registration the first-come rule will be followed. Registrations will be checked in a post-validation process and subject to an enforcement program based on statistically targeted random investigation and complaint follow-up. This program minimizes both costs to registrants and third parties. In particular, it strongly diminishes the attractiveness of rights violations, abuse or malignant behavior. Having been preceded by a controlled launch phase, the validation and enforcement workload faces no resource bottleneck and thus achieves a high degree of credibility, further dissuading abuse from the start. This mode of operation has a strong positive side effect in the interest of trademark holders.

18.3.3 How will multiple applications for a particular domain name be resolved, for

example, by auction or on a first-come/first-serve basis?
As described below, during pre-launch and launch phase, the first-come-first-served principle is NOT applied. Adjudication by auction is one of the solutions available to the parties in the context of the contention resolution process. In the phase of ongoing registrations the first-come/first-served basis of name allocation will be followed, unless the name is one that is on a reserved list, in which case the allocation rules applicable to that list will be followed.

In phases and areas where the first-come-first-served principle tends to yield perverse results, alternative modes will be used.

(1) In the PAB creation phase community research will identify names to be entered into reserved lists and the rules by which they will be allocated;
(2) In the pre-launch phase key portal names of use to the entire community will be registered and used for communication and outreach; and
A launch phase led by protection for and registration by trademark holders and those eligible to hold names on reserved lists.

It is anticipated that the pre-launch portal development program identified in (2) above will involve builders and users in the Art community. The portal development program will allocate domain names based on an open and transparent project selection process. This process is highly economical in terms of social costs and yields substantial external benefits.

The portal development program is an essential part of .Art outreach. It begins before delegation of the TLD. In terms of workload, it mainly affects proposers who themselves are required to demonstrate support for their projects. Support will be required to come from the segment of the community concerned with the respective portion of the name space. Given the high value of the resulting on-line resources for the community and the public interest, and given the economic benefits that can be derived from their operation, the administrative effort is largely justified. To further protect affected parties, all adjudications in name space mandates have a safety-valve clause, allowing for later adjustments based on community input. The principle of the safety-valve is that affected parties can obtain adjustments to a component of a mandate if they propose (and commit to) an improved use of the underlying domain names from a public interest perspective.

The launch programs referred to in (3) above combine the so-called “sunrise” and “landrush” processes simultaneously in one phase. The use of domain applications instead of domain registrations means that the registry accepts multiple applications the same domain name. (By contrast, only a single registration can exist for a given domain.) In this way, contention resolution can take place without time pressure in a transparent, fair and orderly manner.

At the time of ongoing registration the first-com rule will be followed. Registrations will be checked in a post-validation process and subject to an enforcement program based on statistically targeted random investigation and complaint follow-up. This program minimizes both costs to registrants and third parties. In particular, it strongly diminishes the attractiveness of rights violations, abuse or malignant behaviour. Having been preceded by a controlled launch phase, the validation and enforcement workload faces no resource bottleneck and thus achieves a high degree of credibility, further dissuading abuse from the start. This mode of operation has a strong positive side effect in the interest of trademark holders.

18.3.4 Explain any cost benefits for registrants you intend to implement (e.g., advantageous pricing, introductory discounts, bulk registration discounts).

The focus of the .ART gTLD is a competitive cost to registrants and stakeholders that takes into account the limited community nature of the gTLD. This takes into account all burdens, including the effort needed to register or the potential alternative cost to obtain a name on the secondary market. The direct per-unit cost is merely a component of the bottom-line cost.

The cost is greatly reduced by avoiding contention between legitimate community-based applicants and speculators. Community-specific promotion code programs will be used from time to time to offer registrations at low cost. This is a way to avoid perverse effects of low prices, such as speculation with ultimately high costs to registrants, large-scale confusion and waste of the name space, or cybersquatting.

The portal development program will have special terms in order ensure that key portions of name space are used in the public interest.

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

The .ART TLD will not be based on or otherwise involve contractual clauses regarding price escalation between the .ART Registry and its registrars.

The .ART business plan is designed to avoid any future necessity to increase registry price in real terms. The fundamental principle is prudence: starting from conservative price levels that allow self-sustainability at the registration levels projected and gradually lowering prices as registration volumes increase beyond the minimum necessary for self-sustained operation. This method ensures sufficient financial reserves, favors optimal allocation of domain names, helps prevent misuse and supports an orderly registration process.

Community-based Designation

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

Yes

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

Dadotart is committed to serving the arts community, through the creation and operation of the .ART gTLD.
In its simplest definition the arts community is comprised of individuals, groups of individuals and legal entities who identify themselves with the Arts and actively

participate in or support Art activities or the organization of Art activities. The international arts community is diverse and wide-spread, but it is nonetheless a community joined by the output of artists and the support and affinity of its organized members, audiences, institutions and consumers. Indeed, most communities are identified in this way. Sport communities are a well-known example. Participation and self-identification delineate communities as diverse as car enthusiasts, mountain climbers and practitioners of yoga. The experience of deviantArt shows that that an arts community of more than twenty million will not only identify itself online, but will produce and upload more than 140,000 unique art objects every day.

The Art community is also based on common values shared by its members. While all artistic activity is related to a line of cultural and artistic history, the respect of ownership and authenticity of an artwork are core values of the Art community. The community values also include openness of mind, critical reflection as well as commitment to the integrity in freedom of expression, in both content and means. Artistic activity, the striving for artistic mastery, is an aim for its own ends, nurturing the aesthetic aspect of human nature.

The .ART gTLD is therefore defined and readily identifiable by the actions of its members, with members at all levels sharing interests, aims and commitments to producing and enjoying art of all types.

The .ART gTLD will be directed to and by the Art community through their participation as registrants and in the Policy Advisory Board ("PAB").

The arts community is a community of production, support and affinity, and its policies of member definition would be incomplete if they did not hold requirements for participation and support not just for name registration eligibility but also for name use. Use of a name in artistic production, support and affinity represents ongoing evidence of community eligibility. The following four statements describe the features of community definition combined with community participation through use of a .ART domain name.

(1) Definition—The Art community is comprised of individuals, groups of individuals and legal entities who identify themselves with the Arts and actively participate in or support Art activities or the organization of Art activities.
(2) Registration of .ART domains: Qualifying factors—The registration of domain names under the .ART gTLD will be restricted to bona-fide members of the Art community and is subject to the further requirement that the registrant's participation or support in the Art community arena and the registrant's use of the domain name must be:
a. Generally accepted as legitimate;
b. Of a nature that demonstrates the registrant's membership in the Art community; and
c. Conducted in good faith at the time of registration and thereafter.
(3) Policy Authority—Dadotart will act as the coordinating body of the members and representative organizations for the Art community with respect to the .ART gTLD in consultation with the stakeholders of the Art community and their representative organizations.
(4) Policy Advisory Board—In order to achieve as broad and inclusive a representation of all Art community stakeholders as possible, policy development of the .ART gTLD will be based upon advice provided by the .ART Policy Advisory Board ("PAB") The PAB will be specifically established for this purpose. The PAB will include members of Dadotart as well as representatives of the various international community stakeholder groups, cultural organizations and will also involve participation of interested artists who might not necessarily be represented by established community organizations.

• How the community is delineated from Internet users generally.

The global arts community has hallmarks of identification and commonality that set it apart from these Internet users. These hallmarks include:
(1) Identification through production, support and affinity
(2) Continued participation
(3) Shared action and participation around numerous traditions, genres and styles.

1. Membership Identification
The first question any community faces is, can its members be identified? The most common way to identify a community is to look at the actions of its potential members. The arts community is one of these natural communities. It is not defined by holding a license or by creation by a regulatory body or necessarily by membership in an established association or organization. It is a community of participation.

The term "art" describes a diverse range of creative human activities and the products of those activities, but is most often understood to refer to painting, film, photography, sculpture, and other visual media. Music, theatre, dance, literature, and interactive media are included in a broader definition of "art" or "the arts". In our formulation, the arts community is comprised of individuals, groups of individuals and legal entities who identify themselves with the Arts and actively participate in or support Art activities or the organization of Art activities.

Dadotart and its PAB will have no trouble identifying its members. The definition we have formulated is that the Art community is comprised of individuals, groups of individuals and legal entities who identify themselves with the Arts and actively participate in or support Art activities or the organization of Art activities.

2. Continued Participation
Continued participation through name use rules will be a requirement of the .ART gTLD, acting as a further assurance that community members alone hold .ART domain names.

3. Shared Action and Participation
At the time of registration, eligibility will be shown in part by the way in which the potential registrant shares in the actions around traditions, practices, genres and styles identified with the art community. Everyone knows that action as a fan of baseball is not evidence that a person is part of the arts community. Actively writing, painting or sculpting (or supporting these activities) is.

• How the community is structured and organized.

The arts community is very loosely structured and organized for the most part simply around participation - - and by virtue of participation. Certainly, there are organized groups within the arts community but the vast majority of artists and participants in the arts are not structured and are not formally organized in a hierarchical manner of local⁄regional, national and international legal entities. In many ways the strength of the art community lies in its natural openness. The .ART gTLD will provide a globally available locus of communication and identification for the many millions of arts participants who are not organized as well as for those who are.

• When the community was established,

The Art community has existed as long people have produced and shared art.

• The current estimated size of the community

The global arts community at large is constantly growing and embraces the majority of the world's population in one way or another.

As production and enjoyment of art lie within the human nature, the arts community has a global presence in every culture.

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

By the very nature of art, there is no hierarchical system of legal bodies to officially represent the arts community, nor an alliance of groups that might claim this authority. Dadotart is owned and directed by deviantArt, an innovator in creating an Arts community online which has proven its commitment to support the Arts community online with more than 20 million members and 60 million monthly unique visitors.

Starting from the relation with this community organization, Dadotart will partner with other community organizations, both online art communities and established art associations and institutions from the "offline" art world. A key part of the community ties lies in the .ART Policy Advisory Board (PAB), which is to embody representatives of all relevant stakeholder groups in the art community.

The PAB will also build the strongest line of accountability between the Arts community and the .ART gTLD. Through their own representatives in the PAB, registrants and members of the Arts community generally will create policy, advise on pricing, name use, reserved lists and all other matters of interest to the community.

Through the .ART gTLD portal program key sites will serve to gather members and to communicate with the gTLD. The many .ART domain names and their diverse uses and users will constitute the key means for the art community to relate to Dadotart and Dadotart to them.

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

Intended Registrants—The guiding definition we have adopted is that the Art community is comprised of individuals, groups of individuals and legal entities who identify themselves with the Arts and actively participate in or support Art activities or the organization of Art activities.

The .art TLD is to serve the collective interest of the all the members of the art community. For the largest portion of members of the gross art community in numeric

terms – art enthusiasts, spectators, audience, visitors and fans worldwide – the greatest value of .art lies in the reliability and trustworthiness of the .art name space. They want to see .art domain names in the right hands rather than to own .art domain names themselves.

The inverse analysis comes to the same conclusion: given the intrinsic scarcity of domain names (each name can only exist once), the objective of the .art TLD cannot be to provide a domain name each to billions of art affectionatos. An approach where all art lovers could register any .art name would destroy the value of all .art names. Fair allocation of names would be impossible, community members would be pushed into sterile contention. In such an environment, all stakeholders would experience .art as a nuisance rather than a useful resource.

An exhaustive listing of all potential registrants is not possible or desirable, but a summary list may provide some guidance:

- Artists, the creators and performers of art (including but not limited to: painters, sculptors; dancers, digital artists, photographers, actors, musicians, singers and other performers; architects; designers; writers, composers and directors; art students);
- Other art professionals (curators, producers, art historians, restoration professionals, professors of art-related topics, art consultants, editors, publishers, managers of performing art venues, etc.);
- Museums, art centers and other institutional exhibition and art show organizers (biennials, foundations, art fairs, etc.);
- Performing arts venues and agencies like theaters, opera houses, concert halls, studios, dance companies, etc.;
- Galleries, auction houses and other art traders and distributors including publishing houses, online distributors and legal download platforms;
- Associations and guilds of artists, museums, galleries and other art intermediaries; collecting societies; associations of patrons and art enthusiasts;
- Art platforms, in particular online platforms and social networks with a focus on art;
- Art schools and academies;
- Art journalists and art media;
- Collectors;
- Foundations and other private entities involved in the support of artistic activities;
- Governmental bodies and public entities involved in the support of art on any level (local, regional, national, international, multinational).

Purpose and Mission—Dadotart's mission is first to unite, support and promote Artists and those who are engaged in the Arts worldwide. Second, its mission is to use the .ART gTLD for the co-ordination and protection of their common aims and interests, communication and co-operation, while at the same time conserving and respecting their autonomy.

End Users—Dadotart is committed to serving the arts community at large, through the creation and operation of the .ART gTLD. In serving the arts community .ART gTLD will also be serving its intended end-users who are primarily those we are part of the arts community, whether they are registrants or not.

Related Activities—Dadotart is focusing on the early stages prior to launch to put in place the activities that will help to carry out its purposes. First, Dadotart is keenly aware that any new gTLD must be seeded with relevant content to drive traffic and build consumer recognition and trust. Having closely evaluated the dotAsia Pioneering program which was incorporated into the launch of the .ASIA gTLD, it is critical that this content be available as soon as possible and ideally before any

general registration periods.

Second, the .ART gTLD will incorporate the following minimal safeguards into any business model at the time of launch: Registrant Eligibility; Name Selection Criteria; and Authorized Usage. In addition, the current best thinking involves the initial reservation of domain names falling within three types:
(1) Names denoting genres or fields of activity (e.g. theatre, sculpture, painting, photography, sculpture, etc.);
(2) In addition, a second reserved list of names of prominent Art institutions as well as Art-related trademarks will be created; and
(3) Names of prominent Artists living or dead.

The exact composition of this reserve list will be compiled with the assistance and guidance of the PAB. There will also be a corresponding policy that will set forth the specific policy by which these reserved domain names can be registered by the appropriate entity.
Lasting Nature—Internationally and historically the arts have played a central role in the development of every culture, whether it was seen in the clay pots used for cooking or the high art of painting found in our national galleries. Supporting the arts as an engaged participant is one of most important ways that we nurture our own humanity and why all the arts continue their practice over time. The purpose of the .ART gTLD is first to unite, support and promote Artists and those who are engaged in the Arts worldwide and second, its mission is to use the .ART gTLD for the co-ordination and protection of their common aims and interests, communication and co-operation, while at the same time conserving and respecting their autonomy. These are purposes that are essential to the life of the arts community.

The .ART gTLD will ensure that Internet users know a site is one of the few locations on the Internet providing only content on Art. A simple search limited to .ART second-level registrants will provide the Internet user with results completely culled of the irrelevant. The fact that arts content will be required on .ART sites will provide a level of user assurance that going to a .ART site will not lead to an empty page.

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

The .ART gTLD serves the Art community.

The TLD string “art” matches the name of the community, Art, in the generally accepted sense of the word, in French and English and in many other internationally-used languages it is seen as “arte”, a form to which the string “Art” is readily identified.

Membership to sub-communities within the arts, e.g. the music or actors’ community, does in no way affect their identification with the art community at large.

The string, ART, is of long-standing and is not used in any significant way beyond the community. Minor English uses include the phrase “term of art” or the word “artless”. But these uses are minimal and easily distinguishable from the word Art as a single noun. By contrast, the term “art” can be used with the meaning of an occupation requiring skillful use of the hands (synonym to handcraft), or a subtle or imaginative ability in inventing, devising, or executing something (skillfulness, masterfulness, artistry, cleverness, craft). This figurative use of the word “art”

does not in any sense interfere with its main meaning.

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

Descriptions should include proposed policies, if any, on the following:
• Eligibility: who is eligible to register a second-level name in the gTLD, and how will eligibility be determined.
• Name selection: what types of second-level names may be registered in the gTLD.
• Content/Use: what restrictions, if any, the registry operator will impose on how a registrant may use its registered name.
• Enforcement: what investigation practices and mechanisms exist to enforce the policies above, what resources are allocated for enforcement, and what appeal mechanisms are available to registrants.

Eligibility— The arts community at large is made up of Artists and those who are have an identifiable engagement with the Arts worldwide. The following statement describes the feature of community definition for the purposes of eligibility.

Definition—The Art community is comprised of individuals, groups of individuals and legal entities who identify themselves with the Arts and actively participate in or support Art activities or the organization of Art activities.

Domain name registration is planned to occur on both the second and third level: at the second level (e.g. Stella.ART) and at the third level (e.g. Stella.Sculpture.ART). The PAB will define policies to ensure that Art-specific name spaces are managed in line with the interests of the Art community. Registrant Eligibility criteria at the second- and third-level within the .ART gTLD will be deferred to PAB for development and later adoption by Dadotart. The universe of registrants that could potentially be permitted to register in accordance with any final Registrant Eligibility criteria at either the second or third level include, Artists and those who have an identifiable engagement with the Arts.

Eligibility will be reviewed before registration in the pre-launch phase. During the launch phase pre-validation will apply for reserved names or trademarks, but will always involve community nexus.
During the post-launch phase of general availability, community nexus will be subject to post-validation by way of an extensive compliance program along with statistically targeted random validation, backed up by a ongoing enforcement program.

From time to time in cases of special promotion, eligibility review may be assisted by pre-identification of potential registrants using existing community channels, in particular through promotion codes.
Projections for the maximum size of the .ART gTLD are 50,000 names by the end of year three, as described more fully in Questions 45-49. Given the anticipated size of the gTLD review of eligibility will not be a problem for the staff identified.
Name Selection— Name selection will be limited by several policies and procedures: reserved lists, landrush and "sunrise" rules, and "portal" names allocated in pre-launch. Reserved names restriction will involve preparation of several lists of

reserved names as follows:

(1) Names denoting genres or fields of activity (e.g. theatre, sculpture, painting, photography, sculpture, etc.);

(2) In addition, a second reserved list of names of prominent Art institutions as well as Art-related trademarks will be created; and

(3) Names of prominent Artists living or dead.

Name selection will further be limited by provisions restricting registration of country codes at the second level. In addition a sunrise and landrush program will provide special provision for trademarks.

In the pre-launch phase key portal names of use to the entire community will be registered and used for communication and outreach. It is anticipated that the pre-launch portal development program will involve builders and users in the Art community. The portal development program will allocate domain names based on an open and transparent project selection process based on proposals for use of the names for the benefit of the Art community.

Content—The arts community is a community of production, support and affinity, and its policies of member definition would be incomplete if they did not hold requirements for name use. Use of a name in artistic production, support and affinity represents ongoing evidence of community eligibility

The registration of domain names under the .ART gTLD will be subject to the further requirement that the registrant's participation or support in the Art community arena and the registrant's use of the domain name must be:

(1) Generally accepted as legitimate;

(2) Of a nature that demonstrates the registrant's membership in the Art community; and

(3) Conducted in good faith at the time of registration and thereafter.

To facilitate validation, registrants will be required to state their intended use of the registered domain name. A false statement of intended use is an indication of bad faith and can be the basis for the suspension or revocation of the domain name

Enforcement— The purpose of the enforcement program is to protect the credibility of the .ART gTLD for users.

The enforcement program will be based on statistically targeted random investigations and on a complaint follow-up process. The statistical targeting is strongly automated and involves the use of search engines and the analysis of registry data related to behavior of registrants.

Depending on the type of misuse to be investigated, web site content or content sent to victims of abuse will reviewed and analyzed by investigators.

Enhanced investigation will take place if the registrant has a bad track record in terms of compliance with the rules of the .ART gTLD. Other violations of public record (such as UDRP or URS cases) will also be taken into account.

If the intended use cannot be deemed legitimate, the registration will be rejected at the time of initial application. If content or later use of an existing .ART domain demonstrate that the registrant has shown bad faith by stating a false intended use, or has changed use, the domain name will be suspended.

If a registrar is complicit with systematic violations of the .ART policies or causes an unacceptable burden for the validation and enforcement program by negligence, the registry can restrict that registrar's access to the new registrations, subject its inventory of .ART domains to enhanced investigation and require it conduct its own post-validation program.

An appeals process will available for all administrative measures taken in the framework of the enforcement program. The first instance of the appeals process will be managed by the registry service provider.

The PAB set up by Dadotart provides the second and last instance of an appeals process by itself or entrusts it to an alternative dispute resolution provider. The charter of the appeals process will be promulgated by the PAB.

The ongoing compliance program will regularly be adapted to current needs based on experience and audit findings. Community nexus validation combined with strong

protection of trademarks will help to stamp out cybersquatting and abusive registrations. Non-complying registrations will be subject to revocation. Eligibility and name use conditions must always be fulfilled. The strength of the validation will be kept in line with the nature of the underlying domain name base and the reasonable expectations of a typical user.
The validation and enforcement program will be supported by an integrated issue tracking system. This system allows validating agents and personnel to cooperate and interact with the registrant. The system keeps track of decisions made by the agents and stores supplemental documentary evidence that may be supplied by the registrants.
Projections for the maximum size of the .ART gTLD are 50,000 names by the end of Year three, as described more fully in Questions 45-49. Given the anticipated size of the gTLD enforcement will not be a problem for the staff identified.

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.

Answer for No. 22

22 Dadotart Inc. Has Properly Researched This Topic

Dadotart Inc. is keenly aware of the sensitivity of national governments in connection with protecting country and territory identifiers in the Domain Name System (DNS). In preparation for answering this question, Dadotart Inc. reviewed the following relevant background material regarding the protection of geographic names in the DNS:

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

22.1 Initial Reservation of Country and Territory Names

Dadotart Inc. 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 all other levels within the .ART generic top-level domain (gTLD) at which it will provide for registrations. Specifically, Dadotart Inc. will reserve:

1. 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;

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

3. 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.

22.2 Fair & Non-Misleading Use of Geographical Identifiers

Dadotart Inc. believes the use of geographical identifiers to the left of the TLD and as part of the domain name itself can have a direct and material impact on search engine algorithms and their corresponding query results. In addition, such naming conventions are intuitive and practiced by direct navigation Internet users (those that type their intended destination into address bars as opposed to search engines). As ICANN has largely premised this new gTLD round on promoting innovation, Dadotart Inc. would like to see if this type of hierarchical and intuitive use of second-level domain names within its gTLD provides increased consumer functionality.

22.3 The Legal Protection of Geographical Identifiers

One of the more authoritative resources on the current state of the law in connection with the protection of geographical identifiers was authored by the World Intellectual Property Organization (WIPO) in its 2001 "Second WIPO Internet Domain Name Process: The Recognition of Rights and the Use of Names in the Internet Domain Name System" report. Chapter six of this report was devoted exclusively to the

protection of geographical identifiers.

From its analysis of the well-established framework against the misuse of geographical identifiers at the international, regional, and national levels, WIPO identified the following two elements for the protection of geographical identifiers: (i) a prohibition of false descriptions of the geographical source of goods; and (ii) a more extensive set of rules prohibiting the misuse of one class of geographical source indicators, known as geographical indications, see "Second WIPO Internet Domain Name Process" (Paragraphs 206 and 210). Neither of these elements is present in Dadotart Inc.'s current or proposed use of geographical identifiers.

Notwithstanding WIPO's recommendation that the protection of geographical identifiers is "a difficult area on which views are not only divided, but also ardently held" (Paragraph 237), national governments within the ICANN Governmental Advisory Committee (GAC) and other international fora have continued to advocate for increased safeguards to protect against the misuse of geographical identifiers within the DNS.

Dadotart Inc. seeks to minimize any potential business practices that might mislead consumers. At the same time, however, Dadotart Inc. believes that it is important to be able to use geographical identifiers in a fair and non-misleading manner, if such use can benefit Internet users as proposed in its business model.

22.4 Fair & Non-Misleading Use of Geographical Identifiers

In undertaking a thorough research of this subject matter prior to filing this application, Dadotart Inc.'s subject matter experts were able to uncover the following representative sampling of fair and non-misleading use of geographical identifiers used in the existing gTLD domain name space:

Fair Use of National Geographical Identifiers

AUSTRALIA.COOP – Is operated by Co-operatives Australia, the national body for State Co-operative Federations, and provides a valuable resource about co-operatives 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 co-operative mutual businesses 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, DE 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.

Fair Use Regional ⁄Local

TEXAS.JOBS – Is operated through a joint effort between DE, the Texas Workforce Commission, and the National Labor Exchange to connect job seekers with

approximately 96,000 job openings. An additional domain name operated by this joint effort was WORKINTEXAS-VETERANS.JOBS, a resource devoted to helping Texas veterans translate their military skills to jobs in the civil marketplace.

BOISE.COOP – Is operated by Boise Co-op, a member-owned co-operative founded in 1973 by a few dozen individuals who shared a mutual interest in buying healthy and organic food at reasonable prices.

BROOKLYN.COOP – Is operated by Brooklyn Cooperative Federal Credit Union, which began as a modest storefront business in 2001, but is now New York City's fastest growing credit union and a model for community development credit unions nationwide.

HYDERABAD.AERO – Is operated by the Hyderabad International Airport and provides a range of interactive services and information for both business and leisure travelers.

SACRAMENTO.AERO – Is a portal website operated by Sacramento County to provide links to each of the airports serving the Sacramento area: Sacramento International Airport (SMF), Mather Airport (MHR), Executive Airport (SAC), and Franklin Field (F72).

22.5 Protection of Regional and Local Geographic Names for Misleading Use

Although Dadotart Inc. is considering using non-reserved geographic identifiers as part of a hierarchical and intuitive framework in a fair and non-misleading manner to help consumers navigate the .ART namespace, Dadotart Inc. is committed to operating the .ART namespace in a manner that minimizes potential consumer confusion, and will actively work with others in the ICANN community regarding any future policy development in this area.

22.6 Potential Future Release of Initially Reserved Names

Dadotart Inc. looks forward to collaborating with other new gTLD registry operators in potentially working with ICANN's GAC to explore potential processes that could permit the release of initially reserved country names (including ISO-3166 two characters). Specifically, Dadotart Inc. is interested in exploring other Registry Service Evaluation Processes (RSEP) that have been filed by existing gTLD registry operators in releasing previously reserved domain names.

22.7 Creation and Updating the Policies

Dadotart Inc. is also committed to continually reviewing and updating these lists to prevent the misleading use of geographical identifiers. Consistent with this commitment, Dadotart Inc. intends to participate in any ongoing ICANN policy discussion regarding the protection of geographic names within the DNS. Should the need arise in the future for the creation or updating of the policies regarding this class of domain names, Dadotart Inc. LLC will act in a responsible manner.

Registry Services

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

provided.

Q23 - Registry Services

1. Overview

CORE Internet Council of Registrars will provide the technical registry services for the operations of the .art Registry.

The CORE Registration System offers the usual registry services for the .art TLD: Receipt of data from registrars

concerning registration of domain names and name servers via EPP (SRS; see also answer to Question 24, SRS Performance);

Dissemination of top-level domain (TLD) zone files (DNS; see also answer to Question 35, DNS service, configuration and

operation of name servers); Dissemination of contact or other information concerning domain name registrations (port-43

Whois, web-based Whois; see also answer to Question 26, Whois service); Internationalised Domain Names (see also answer to

Question 44, Support for Registering IDN domains); DNS Security Extensions (DNSSEC; see also answer to Question 43,

DNSSEC). These services are introduced below. For more detailed descriptions, please refer to the answer to the respective

question in the gTLD Applicant Guidebook. Additional benefits offered by the registry are full support for Internet

Protocol version 6 (IPv6), data escrow, registrar reports and support for Sunrise and Landrush phases. All of these are

compliant with the new gTLD requirements. No further registry services according to the definition in the gTLD Applicant

Guidebook are offered for the .art TLD.

The Shared Registry System (SRS) is the central coordinating instance in the overall system concept. It is the

authoritative source of the domain, host and contact data, provides client⁄server-based access methods for the registrars

and internal personnel to this data, is responsible for the zone generation, performs accounting and reporting, and feeds

the Whois servers.

The SRS is responsible for managing the domain registrations by accepting requests for the creation, update and deletion of

domains and related information from the registrars, who act on behalf of the

registrants.

The CORE Internet Council of Registrars and its developers have ample experience in designing, developing and operating

shared registry systems. The CORE Registration System is compliant with established standards like Internet Engineering

Task Force (IETF) Requests for Comments (RFCs) and can be customised for the specific needs of a top level domain, ensuring

Internet Corporation for Assigned Names and Numbers (ICANN) gTLD standards compliance.

CORE Internet Council of Registrars has been entrusted with the technical operation of the .cat and .museum TLDs on behalf

of the puntCAT and MuseDoma registries. Therefore, CORE has the knowledge and experience that are necessary to provide the

mentioned registry services. Since the software development is handled exclusively in-house, the .art Registry Services do

not depend on any external companies or developers. Software development at CORE is always based on principles like

efficiency, scalability and security by design.

2. Infrastructure Design

2.1 Goals

The design of the .art Registry infrastructure achieves three goals:

2.1.1 High Availability

The resolution of domain names by the Domain Name System (DNS) infrastructure is the most critical part. If it fails, not

only a large fraction of Internet users is affected, but other Internet infrastructure depends on the domain name

resolution as well, causing a cascade of failures.

The shared registry system itself is also in the focus. While theoretically, a short outage would not have a direct and

larger impact to the TLD users, a longer outage can become problematic, especially in the light of DNSSEC: If the registry

is unable to re-sign the zone in time, the zone will become bogus and the effect will be similar to a failure of the whole

DNS infrastructure.

2.1.2 Scalability

The aspects of scalability must be observed for two reasons: The infrastructure must grow with the demand; economic

considerations let it seem unreasonable to launch with oversized hardware equipment. The software design must be able to

cope with increasing demand, it must allow the long term upgrade of the infrastructure. Scalability must also be provided

for unforeseeable load peaks. The infrastructure must be resilient and one step ahead; spare resources must be available.

2.1.3 Security

In an increasingly adverse environment, security is a cardinal goal. Various attack vectors need to be addressed. For

example, the public infrastructure must be protected against pure (distributed) denial of service attacks and exploits of

bugs in devices, operating systems and application software, and the SRS must be protected against intrusion by third

parties with the intent of deletion or manipulation of data or stealing private keys used for DNSSEC.

2.2 Design Principles

The design principles that follow these goals are as follows:

Shared Registry System (SRS)

The SRS (actually all services except the name servers) is run on two sites, a primary and a secondary site. These sites

are geographically separated for an event of force majeure that makes one of the sites unavailable.

Fail-over strategies are used systematically, either by the software itself or by employing cluster technologies where

applicable.

Systematic data replication/backup/escrow is ensured.

Modularisation of the software and avoidance of monolithic structures improves scalability and maintainability.

Intrinsic support for multiple instances of software components to distribute load is guaranteed.

State-of-the-art security technology reduces chances for attackers to a minimum.

Some components like the Extensible Provisioning Protocol (EPP) interfaces may run in multiple instances. Incoming requests

are distributed to these instances with the help of load balancers. Excluding

instances one by one allows maintainance in

respect to both hardware and software without interrupting the actual service.

DNS Infrastructure

Diversity in software and hardware increases security.

Use of Anycast networks ensures high availability.

3. Features

3.1 Receipt of Data from Registrars

The SRS receives data from the registrars, writes the data into the database and passes on TLD zone files to the DNS

services. The registry has a Whois function to make information about contacts and domain registrations available to the

general public. DNS and Whois are updated dynamically. The registry TLD name servers receive DNSSEC-signed master zone

data.

The .art TLD will be operated as a so-called ”thick” registry, i.e. the data for domain registrants, administrative

contacts, technical contacts and billing contacts is stored in the registry repository. Registry policy mandates that each

domain must be associated with exactly four contacts, one contact of each type. In contrast to a ”thin” registry (which

doesn’t store contact information), this allows the registry Whois service to provide contact information itself, i.e. it

doesn’t rely on registrars to operate their own Whois services for the inquiry of domain contact data.

Registrars can provide the data necessary for the registration of domains, contacts and name servers (hosts) in two ways.

Firstly, using the EPP interface of the CORE Registration System, which allows completely automatic processing of requests.

Secondly, there is the option of using a password-protected web interface (”Control Panel”). The Control Panel offers

copious amounts of information and many tools for registrars and registry administrators. Registry objects can be inquired

and modified, creating new objects is possible just as easily. In addition, automatically generated reports for registrars

are made available for download. Each report contains detailed information about the registry objects of the respective

registrar. The Control Panel also allows the administration of registrars. Such administrative functions are of course

limited to users belonging to the registry. These can also - their privileges permitting - inspect the tariffs and make

corrective entries in the billing system.

3.2 Internationalised Domain Names

The CORE Registration System supports internationalised domain names (IDN, see RFC 3490, 5890-5894) in several ways.

In the extensible provisioning protocol (EPP), there are various XML elements that expect a domain name. The EPP

implementation of the CORE Registration System accepts domain names in A-label notation (punycode) as well as in U-label

notation (unicode). The former notation is preferred; all EPP responses use A-labels, even if the respective request used

U-labels.

Internationalised domain names are not only supported as first-class objects, but also as so-called variants of a base

domain. In this case, a domain has more than one representation. The alternatives are organised as attributes of the base

domain, meaning they cannot exist by themselves. This has the advantage that they are much less subject to domain

squatting, since the variants always belong to the same registrant as the base domain. In the DNS the variants are

represented by DNAME records (as it is done in the .cat and .gr TLDs) or published with the same name servers as the base

domain. A precondition for the use of variants is that the specified language(s) allow the derivation of a canonical name

from any valid domain name. This is, for example, achieved by the principles defined in RFC 3743 for the

Chinese/Japanese/Korean languages.

For more information about IDN support, please refer to the answer to Question 44, Support for Registering IDN Domains.

3.3 DNSSEC

Support of the DNSSEC extension according to RFC 5910 allows to specify the DNSKEY data. The CORE Registration System

calculates the delegation signer (DS) records from the DNSKEY data and adds them to

the zone file. Further information

about the DNSSEC implementation can be found in the answer to Question 43, DNSSEC.

3.4 IPv6 Support

The .art Registry infrastructure supports IPv6 on all levels: Firstly, the name servers use IPv6 addresses on the DNS

protocol level (port 53), i.e. domain names can be resolved by using the IPv6 protocol. Secondly, the registry software is

able to assign IPv6 addresses to in-zone hosts as provided in the EPP Host Mapping (RFC 5732) and to publish these

addresses via AAAA records in the zone. Thirdly, registrars can connect to the registry by using the EPP transport protocol

via IPv6. Fourthly, the Whois service (both port 43 and web interface) can be accessed via IPv6. Fifthly, the registrar web

interface can be accessed via IPv6. Details about the IPv6 capabilities can be found in the answer to Question 36, IPv6

Reachability.

4. Zone Management

Whenever the authoritative data of a domain or host is altered, the change is forwarded to the DNS component and other

components. Upon reception of this change, the DNS-specific database tables are updated. The structure of these tables

directly corresponds to the structure of the zone file, so that the zone file can be generated with little effort.

The generated zone is then fed into the DNSSEC signing component. Since the zone changes only marginally between the runs,

the signing component re-uses RRSIG signatures and NSEC3 name mappings from previous runs. This reduces the run time of the

signing process by an order of magnitude on average.

In the next step, the zone is delivered to the ironDNS system, which manages the distribution of the zone to the name

servers independently. For more details about this process, please refer to the answer to Question 35, DNS Service.

The whole process is covered by integrity checks. The zone is inspected by heuristic rules, for example, the change in size

between the previous and new zone is determined and checked against limits. If there is any evidence that the zone may

contain problems, the deployment process is halted and manual inspection by the support team is requested. Where

applicable, the distribution is accompanied by safeguards, like cryptographic digests, to allow the detection of changes or

truncations.

5. Whois service

The CORE Registration System contains a public service that can be used to inquire data of registry objects (i.e. domains,

contacts, hosts and registrars), the Registration Data Directory Services (RDDS). At the moment, this is implemented as a

Whois service. Details regarding the Whois service can be found in the answer to Question 26, Whois service. Abuse of this

service is effectively prevented, for details refer to the answer to Question 28, Abuse Prevention and Mitigation.

6. Escrow and Reports

The SRS also handles the monthly reports to ICANN and the generation of escrow files according to ICANN's specifications.

The reports and escrow files are automatically sent to ICANN and the escrow provider, respectively.

In its role as the registry backend operator for .museum and .cat, CORE Internet Council of Registrars has continuously

provided reliable registry data escrow services for these registries, in full compliance with the escrow specifications of

the respective ICANN registry agreements.

In the same fashion, CORE also produces registrar escrow files for its registrar activities, in full compliance with

ICANN's Registrar Data Escrow (RDE) requirements.

Fully automated daily processes are in place that create the full or incremental XML escrow files as required, then split,

sign and encrypt them according to the requirements from ICANN and the escrow agent, and finally transfer the resulting

data to the escrow agent's server. The escrow files contain the main SRS data, zone data and RDDS/Whois data. CORE Internet

Council of Registrars also provides access to full zone data for the .museum and .cat TLDs to eligible parties upon sign-up

to this service. Access is granted to authenticated users via an SSL/TLS-secured web interface.

All registry agreements with ICANN require the registry operator to submit a monthly report about the registry's

activities, inventory and performance to ICANN. CORE's registry system is able to create such a report containing (among

other things) data about: domain⁄host inventory statistics, domain transfer statistics and domain renewal⁄deletion⁄restore

statistics per registrar; service availability, outage durations and response times for SRS, DNS and Whois; Whois request

statistics.

In addition, the following reports may be created for each registrar: Inventory report: domain, contact and host objects

sponsored by the registrar on a specific date; Transfer report: transfers in progress, completed or rejected on a specific

date; Autorenewal report: domains being automatically renewed on a specific date; Billing report: detailed information

about every single billing operation that has been performed on the registrar's account (including refunds).

7. Support for Sunrise Phase

A common problem that arises during the initial launch of a new top level domain (and, potentially, subsequently when new

features like IDNs are introduced) is to ensure that trademark owners or otherwise eligible parties can claim their names

in an organised manner that can be audited in case of legal disputes. To this end, registries ususally offer a so-called

"Sunrise" phase, i.e. a certain period of time during which only eligible parties are allowed to register domain names.

Eligibility has to be proved by providing information about a trademark related to the domain name, for example. Such

additional information is provided by the registrars during registration of the domain name, with the help of a special EPP

extension (see answer to Question 25, Extensible Provisioning Protocol, for details).

The validity of a Sunrise domain name application is checked by an external service provider, the so-called Trademark

Clearinghouse. At the time of writing, ICANN has issued a request for information for providers to perform the Trademark

Clearinghouse functions. It is envisaged that the CORE Registration System will use

a suitably defined interface of the

Trademark Clearinghouse to submit requests according to the trademark data submitted by domain name applicants.

To facilitate the handling of Sunrise applications, the CORE Registration System is equipped with a built-in issue system

that offers registry personnel a convenient web interface to review domain name applications and to approve or reject them

accordingly.

The issue system allows searching for applications by various criteria (e.g. domain name or current workflow⁄approval

state). It offers a two-level review workflow that allows the delegation of pre-selection tasks to the first level support

staff, after which a final decision - if still required - can be made by second level personnel. All application details,

including registrant information and all supplied trademark information is conveniently displayed. The issue system fully

tracks and documents application status and history, allowing for a complete audit in case of legal issues. Furthermore, it

is fully integrated with the registry backend, i.e. it automatically notifies the SRS about the reviewers' decisions and

immediately activates the respective domain in case of an approval.

The issue system was first used during puntCAT's elaborate multi-phase Sunrise period in 2006 and proved to be an

invaluable tool for efficiently organising a TLD roll-out process.

The CORE Registration System offers built-in support for Sunrise and Landrush phases. In the case of the .art Registry,

only a Sunrise phase will be supported.

8. Domain Expiration and (Auto-)Renewal Policies

Domains are registered for a certain interval only. The possible intervals are multiples of a year. The system maintains a

so-called "expiration" date, which represents the date up to which the registrar has paid the fees for the respective

domain. This date is also published on the public Whois servers and is included in reports generated for the registrars.

Domains must be registered at least for a year. The registration period can be extended at any time by issuing a "renew"

request to the registry. However, the resulting expiration date must be not beyond 10 full years in the future.

Since usually the registrars use the same intervals for their customers, there is always the problem that some customers

make up their decisions whether to keep a domain or to delete it at the very end of the registration term. To accommodate

the registrars with this problem, it is common practice among the registries to grant a so-called grace period, which

starts at the expiration date. During this 45 day period, the registrar may delete the domain without paying any fees for

the already started next term. If after 45 days the domain has neither been deleted nor renewed by the registrar, the

registry itself automatically renews the domain by one year.

9. Billing

The registry maintains an account for each registrar. All registrations, transfers, renewals and other billable operations

have to be prepaid, and corresponding fees are deducted from the registrar's account.

Whenever a billable operation is attempted, the registrar's account is first checked for sufficient funds. If the account

is lacking the required funds, the operation is rejected. A corresponding result code is returned if the rejection affects

a realtime EPP command, as opposed to e.g. an internal autorenew operation that was not directly triggered by a registrar

command. However, the autorenewal of expired domains is treated differently; to avoid accidental domain deletions,

autorenewals are continued even in case of insufficient registrar funds. Non-billable operations (like all read-only

commands) and activities that trigger refunds are always executed, regardless of the registrar's account balance.

If sufficient funds are available, the operation is executed and the registrar's account is charged with the corresponding

fee (if the operation was completed successfully).

Each registrar may provide an account balance threshold value. The billing subsystem will automatically send an e-mail

containing a "low account balance warning" to the registrar whenever the registrar's funds drop below the configured

threshold value.

Some commands, like domain deletions or transfer cancellations, result in refunds if corresponding grace periods apply. The

affected registrar's account is immediately credited for each refund.

The billing subsystem utilises its own database, containing tables for registrar accounts (including current balance and

warning threshold), tariffs for billable operations along with their validity periods and book entries (each one

representing a single credit or debit).

The SRS component responsible for actual registry operation communicates with the billing component. Any billable or

refundable event (such as domain creation, domain deletion within grace period, request for domain transfer, domain renewal

or autorenewal) results in the lookup of a suitable tariff in the tariff table, the creation of a corresponding record in

the book entry table and the update of the registar's account.

The entire implementation is carefully designed to ensure billing accuracy. The checking for sufficient funds as well as

the processing of book entries representing the billable events are always done within the same database transaction that

performs the actual billable repository change, thus ensuring transactional integrity and account consistency.

10. OT+E and Staging Environment

In addition to the production registry system, CORE Internet Council of Registrars provides an independent Operational Test

and Evaluation (OT+E) system to give registrars the opportunity to develop and test their client software in a self-

contained "sandbox" environment that does not interfere with production business.

The OT+E system emulates the behaviour of the production system as closely as possible to allow for realistic testing. It

also includes a Whois server, as well as a name server fed from the sandbox data, which facilitates the testing of transfer

policy and DNSSEC implementations on the registrar side, respectively.

The OT+E system differs, however, from the production system in some respects to further simplify development for the

registrars: Firstly, each registrar is granted two independent identities on the OT+E system. This enables each registrar

to test domain transfers easily by creating domains with the first identity and transferring them to the second identity

(or vice versa). Secondly, to allow short turnaround times for registrars during their tests, most of the periods and

deadlines used by the production system are significantly shortened (or entirely disabled) on the OT+E system. For example,

the OT+E system – contrary to the production SRS – uses an Add Grace Period shorter than 5 days to allow registrars to test

domain name redemption more easily.

Apart from the mentioned differences, the OT+E system will always run the exact same software as the production system.

Both systems are updated at the same time whenever a new release is deployed.

To facilitate a smooth roll-out of major software upgrades, especially those that involve protocol or policy changes

requiring changes to client systems, a separate so-called ”Staging” system is operated, on which these new software

versions are deployed with appropriate lead time before the same changes are applied to the production and OT+E systems.

The actual lead time depends on the nature and the extent of the changes involved.

The SRS is routinely adapted to improved standards and to cope with new technical, capacity and organisational demands.

11. Additional⁄New Registry Services

One potential unique service that Dadotart is considering at this time is the imposition of an annual cost recovery based

fee to validate registrars that will be providing domain name registration services in the .STRING gTLD.

An additional service which Dadotart may offer, commonly used in the marketplace today, is the use of RFPs (Request for

Proposals) and Auctions to determine string allocation in appropriate circumstances.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

Q24 - Shared Registration System (SRS) Performance

CORE Internet Council of Registrars provides a unified registration system for its members since 1997. This system grants access to a multitude of top-level domain registries, currently including .com, .net, .org, .info, .biz, .name, .us, .asia, .eu, .coop and .tel domains, via a single entry point. The activities concerning the CORE Registration System provide CORE with a great deal of expertise and know-how regarding the implementation, operation, maintenance and support of a shared registration system, facing a very heterogeneous user group regarding location, language, enterprise size and structure.

CORE is also handling the technical operation of the .cat and .museum TLDs on behalf of the puntCAT and MuseDoma registries. This proves that CORE has the knowledge and experience necessary to provide the offered registry services.

1. High-Level System Description

The Shared Registry System for the .ART Registry is a local installation of the CORE Registration System, developed by CORE. Consequently, the SRS is compliant with the various relevant standards for EPP (s. Question 25), Whois (s. Question 26), DNS (s. Question 35), DNSSEC (s. Question 43) and IDNs (s. Question 44).

Each registry service is handled by its own server. Overall, the services are set up ensuring n+1 redundancy. It is envisaged that further frontends will be added later, when increasing system usage requires such a step.

1.1 Multiple sites

The .ART Registry as a whole is distributed among a set of independent sites. Besides the geographical diversity of the sites, each site is designed to be independent of other sites. A complete failure of one site or of related infrastructure (i.e. upstream providers) does not affect the operation of the others. No networks or vital base services (like DNS resolvers, LDAP or SMTP servers) are shared among the sites.

For the main registry operation, i.e. all services except the name servers, two sites are designated, the primary one in Dortmund, Germany and the secondary one in Amsterdam, the Netherlands. Name servers, as far as operated by the .ART Registry itself, are located on other sites. Other name servers operated by contractors can be seen to be operated on other sites as well in this context.

To support scalability of the system, the SRS is modularised into components where possible. Components are allowed to run on different machines, so that the overall load of the system can be distributed hardware-wise. This approach also improves the efficiency of cluster technologies and fail-over strategies within a site.

Some components, for example the EPP interfaces to the registrars, are allowed to run in multiple instances if necessary. With the help of load balancers, the incoming requests are distributed to these instances. By directing the load balancers to exclude an instance, this instance can be maintained with respect to both hardware and software. The latter allows minor patches to be applied to the SRS software without interrupting the actual service.

Each of the two .ART Registry sites contains the full set of components that are required for operation and provides for redundancy. Under normal conditions, the

primary site is active, while the secondary is inactive (components are in hot standby). In case of failure or maintenance that cannot or should not be compensated by redundant systems on the active site, the inactive site can take over the operation. The full switch-over, however, is not a requirement. Since the system consists of multiple subcomponents, the task of a failed subcomponent on one site can be transferred to the mirror subcomponent on the other site, while the other subcomponents remain on the first site. This gives the administration team freedom and flexibility to react to an incident and to minimise the impact on users. Switching of services is done using HSDNS pointers, see the answer to Q32, System and Network Architecture, for details.

The various sites are interconnected by virtual private networks (VPNs). This ensures the security and confidentiality of the communication. The VPNs are used both for data transferred between the sites as part of the .ART Registry operations (e.g. zone files to the name servers, replication data between the databases, data feed of the Whois servers) and for administrative purposes, including monitoring.

In the unlikely event of a simultaneous outage of multiple components that makes it impossible to provide the service at the SRS's main operating site (data centre) in spite of the redundancy provided within each site, or in case of natural/man-made disaster at that main site, a switch-over to a different site is possible. Thanks to continuous database replication, the other site is equipped with the entire data of the repository.

Figure Q24-F1 presents a "bird view" on the registry's sites, the services hosted at these sites (as described above), as well as the connections between them. The meanings of the graphical elements and symbols is described in Figure Q24-F2 (which provides a legend for all graphics attached to the answers throughout this gTLD application).

Figure Q24-F3 shows the overall structure of the registry systems per site. The various depicted resources and the relationship between them are described in detail in the answer to Question 31, Technical Overview of Proposed Registry, et seqq.

1.2 Software Development

Like all crucial components of CORE's registry system, the SRS has been developed from scratch by CORE staff or vendors . The custom-built main server component consists of 100% Java code. While it utilises a couple of proven, open-source third-party libraries and products (such as SLF4J for logging and PrimeFaces for the web applications), the core registry functionality remains fully under CORE's control and may thus be customised as needed.

1.2.1 Change Control

All Java code comprising CORE's SRS is maintained in a repository managed by Subversion (SVN), the leading open-source revision control system. All code check-ins into this repository — either into the SVN trunk or into dedicated development branches (for larger additions or changes) — are closely monitored by senior developers.

Software releases meant to be deployed on staging, OT+E or production environments (see below and answer to Question 23, Registry Services) are always built from so-called "release" branches within the SVN repository, i.e. not from the SVN trunk or development branches. Such branches are essentially snapshots of the code known to

offer stable functionality with regard to a certain specification of the system. The exclusive use of these release branches ensures that no inadvertent changes from SVN trunk or development branches are affecting code deployed on systems used by registrars or the public.

1.2.2 Quality Assurance

Each release scheduled to be deployed undergoes a series of extensive tests by an internal QA team within CORE. This includes functional tests, but also stress tests to evaluate the system's behaviour under extreme load conditions.

Any issues found during these tests are reported back to the developers via JIRA, a widely used, enterprise-grade ticketing and issue system. Only after all issues were fixed to the satisfaction of the testers, a release is deployed — usually on the staging system first (also to give registrars an early opportunity to test their client systems against the new version), then on OT+E and production.

In addition to functional and stress testing, CORE's developers also write so-called unit tests with JUnit, a widely used Java unit testing framework that greatly facilitates regression testing.

1.3 Synchronisation Scheme

The synchronisation scheme is designed to enable any of the two sites to act as the master. However, in all cases except emergency and short annual fail-over tests, the system in Dortmund is the master. Data is synchronised on database level in real time.

The database software used will be PostgreSQL 9 (current version). There are four database systems altogether: two at the primary site (Dortmund) and two at the secondary site (Amsterdam). At any time, one of these four systems is active. Its data is replicated to the other three systems: locally to the other system at the same site and remotely to the other site, where a local copy is maintained, too.

2. System Reliability, Stability and Performance

2.1 Outage Prevention

2.1.1 Data Centre Precautions

The data centres hosting the system components of the .ART Registry have taken various precautions to ensure a continuous operation, such as backup power supply, technical and facility security. Please refer to the answer to Question 31, Technical Overview of Proposed Registry, for more details.

2.1.2 Availability by Design

The general system design includes various features to reduce the risk of outages. These are summarised in the following paragraphs.

The network infrastructure of the SRS is designed to compensate a failure of one of

its components. This is achieved by doubling each of these components, i.e. the firewall/VPN system, the load balancer and the switches that represent the internal backbone. They are operated in an active-active configuration. All servers within the system are equipped with two Ethernet interfaces for each logical connection. Where applicable, the components themselves are equipped with redundant power supplies. The interconnection between the servers and the network components provides redundant paths between each two nodes without a single point of failure. For more details please refer to Question 32, System and Network Architecture.

For the database system used by the SRS, double redundancy is provided. Firstly, there are two database servers, a primary and a secondary one. The secondary database is operated as a hot-standby solution. Secondly, there are two more database servers at the secondary site. The database data at the active site is replicated to the non-active site.

To process the EPP requests of the registrars, multiple systems are provided, which run the SRS software simultaneously. A load balancer distributes the incoming requests to these systems. An outage of one server does not interrupt the service. Although the available computing power is reduced by such an outage, the provisioned spare capacities ensure that the overall performance does not violate the service level agreement.

In the unlikely event of a simultaneous outage of multiple components that makes it impossible to provide the service, or in case of natural/man-made disaster at the ″main″ site, a switch-over to the ″mirror″ site is performed. Thanks to continuous database replication, the mirror site is equipped with the entire data of the repository. Depending on the nature of the main site's failure, a limited data loss regarding transactions that were performed in the last few minutes of main site uptime may occur. Compared to the damage caused by a long-term outage, this is considered negligible.

The actual switch-over procedure consists mainly of the following steps: Complete shutdown of the main site if necessary. Despite the failure, some components may still be in an operative state. To avoid interference with the mirror site, these are deactivated. IP address change of the DNS address records belonging to externally visible servers to the corresponding servers on the mirror site. To facilitate this, a short time-to-live (TTL) setting will be used, and registrars are advised to use solely domain names to connect (not IP addresses). Name servers and Whois servers are reconfigured to use the mirror site as their data source. The registrars are informed about the switch-over, enabling them to adapt or restart their clients if necessary.

The Whois subsystem has the intrinsic ability to run an arbitrary number of Whois instances in geographically diverse locations (all fed from the same data source in a near-realtime fashion). The Whois servers operate their own databases for managing the Whois data. Load balancers are used to distribute the incoming requests to these instances. In such a setup, the outage of a single Whois instance will not disrupt Whois services for Internet users. Additional Whois servers can be added quickly to the existing setup if need be.

The huge number of different name server locations used by CORE and the involved diversity (in terms of both geography and network topology) provide a high degree of inherent protection against DNS outages. In particular, the use of state-of-the-art Anycast methodology ensures that a server will be able to respond to requests as long as at least one of the sites in its Anycast cloud is available. In addition, reliable facilities with sufficient redundancy are provided at the individual sites hosting the name servers.

2.1.3 Hardware supplies and Software Availability

The data centres will keep spare parts for all critical hardware involved, which allows fast replacement in case of hardware failures. In addition, continuous 24⁄7 phone and on-site support from the vendors ensures the availability of hardware and software, including operating systems. Contracts guarantee that out-of-stock components are delivered within hours.

2.2 Performance Specifications

All components of the registry system (SRS, Whois, DNS) are operated in full compliance with ICANN's performance requirements as set forth in Specification 10 of the gTLD Applicant Guidebook. In particular, the SRS will meet the following specifications.

2.2.1 SRS Performance

Upper bounds for the round-trip time (RTT) of EPP requests have to be met by at least 90 per cent of all commands. The upper bound for session commands (login, logout) is four seconds, for query commands (check, info, poll, transfer) it is two seconds and for transform commands (create, delete, renew, transfer, update) it is four seconds. The downtime of the EPP service will be not more than 12 hours per month.

2.2.2 Registration Data Directory Services (RDDS) Performance

The upper bound for the round-trip time (RTT) of RDDS queries and for the RDDS update time has to be met by at least 95 per cent of all queries⁄updates. The upper bound for the collective of "Whois query RTT" and "Web-based-Whois query RTT" is two seconds. The upper bound for the update time (i.e. from the reception of an EPP confirmation to a domain⁄host⁄contact transform command until the RDDS servers reflect the changes made) is 60 minutes. The downtime of the RDDS service will be not more than 8 hours per month, where non-availability of any service counts as downtime.

2.2.3 DNS Performance

The upper bound for the round-trip time (RTT) of DNS queries and for the DNS update time has to be met by at least 95 per cent of all queries⁄updates. The upper bound for the TCP DNS resolution RTT is 1500 milliseconds, for the UDP DNS resolution RTT it is 500 milliseconds. The upper bound for the DNS update time (i.e. from the reception of an EPP confirmation to a domain transform command until the name servers of the parent domain name answer DNS queries with data consistent with the change made) is 60 minutes. The downtime of the DNS service will be zero, i.e. continuous availability of this service is assured.

2.3 Operational Scalability

Operational scalability is primarily achieved by the underlying architecture of the components comprising the CORE Registration System.

The software used for the processing of EPP commands is designed to run on multiple systems simultaneously. Due to the fact that the software makes extensive use of Java's multi-threading capabilities, it scales well with the number of processors in each system. Therefore, long-term scalability due to increased registry activity can be accomplished by extending the system with additional processors and/or machines.

The SRS is dimensioned to run with about ten per cent load during regular operation. The initial system is able to handle the additional load resulting from increased domain numbers. To further cope with temporary unexpected load peaks, CORE ensures that at least 100 per cent spare capacity is available all the time.

The above measures can be applied to scale the system from handling 10000 names to up to 20 million names and beyond. The initial capacity will be 1 million names and can be increased in steps of at least 1 million names within a mutually agreed time frame.

An important point is fair and acceptable use of system resources by registrars. As far as transaction numbers are concerned, the .ART Registry subjects registrars' access to acceptable use policies that forbid wasteful use of system resources. The registry systematically avoids situations where registrars or potential registrants find themselves under pressure to enter into a race against one another with respect to registry system resources. This applies in particular to launch phases, where a contention resolution mechanism (including the use of auctions) replaces time priority. The .ART Registry furthermore imposes acceptable use restrictions to prevent the abuse of grace periods.

Additionally, the number of concurrent EPP connections per registrar is limited to a certain maximum, which is initially set to 10. Rate limiting is also implemented by limiting the EPP requests within a sliding window of one minute to a configurable number, in order to prevent monopolisation of the service by one registrar.

Thanks to these measures, the .ART Registry avoids disproportionate demand for registry resources.

3. Employed Hardware

For server and storage systems, products of HP are to be used. Network equipment products of CISCO, HP, Juniper and Foundry are to be used. Employment of upgradable blade and RAID systems as well as ensuring redundancy of network components, power supplies and such increases not only scalability, but also availability and data integrity.

The database server as the central system component is dimensioned to be able to keep the relevant database content in memory to avoid slow disk I/O operations. An HP server system with 2 six-core 3 GHz CPUs and 48 GB RAM will be used. All other servers will be equipped with 24 GB of RAM. The database server is connected to a storage attached network (SAN), which is connected to a high-performance RAID system, namely HP P6300 EVA 2.4 TB SFF SAS.

4. Resourcing Plans

4.1 Implementation

Since the CORE Registration System itself has already been implemented, no resources are necessary for the initial implementation. For setting up and configuring database servers, firewalls and so on, the following resource allocations are estimated:

System Administrator: 25 man hours;

Network Operation Centre Officer: 25 man hours;

DNSSEC Signing Operator: 5 man hours.

4.2 Ongoing Maintenance

For ongoing maintenance and occasional adaption of the system, the following resource allocations are estimated:

System Administrator: 5 man hours per month;

Network Operation Centre Officer: 5 man hours per month;

Software Developer: 2 man hours per month;

Quality Assurance Agent: 1 man hour per month;

DNSSEC Signing Operator: 1 man hour per month.

Employees already working for CORE Internet Council of Registrars will be handling these tasks. The numbers above were determined by averaging the effort required for comparable tasks conducted by CORE in the past over the course of 12 months.

25. Extensible Provisioning Protocol (EPP)

Q25 - Extensible Provisioning Protocol (EPP)

1. Experience

The EPP interface for registrars of the .ART Registry is based on CORE's EPP implementation, which has been used for several registries.

Since 2006, CORE handles the backend registry operation for puntCAT (responsible for the .cat top-level domain). Right from the start, CORE's .cat Shared Registration System (SRS) offered an EPP frontend fully compliant with RFCs 3730-3734 (updated to compliance with 5730-5734 in the meantime), using various EPP extensions to cope with puntCAT's special requirements. The SRS also fully supports the provisioning of DNSSEC data in accordance with RFC 5910; for backward compatibility, the previous DNSSEC EPP extension (RFC 4310) is also supported.

In addition, based on the same technology, CORE Internet Council of Registrars is currently in the process of taking over back-end operations for a country code top-level domain managing between 200,000 and 500,000 domain names. The details of this cooperation cannot be disclosed at the time of writing. While this registry's DNS services have already been transitioned to CORE at this point, the migration of SRS

and Whois operations are currently being finalised.

CORE Internet Council of Registrars provides the unified CORE Registration System for its members since 1997. This system grants access to a multitude of top-level domain registries, currently including .com, .net, .org, .info, .biz, .name (with support for domain name and e-mail forwarding addresses), .us, .asia, .cn, .tw, .eu, .mobi, .aero, .me, .tel, .coop, .ch and .li domains, via a single entry point. CORE members can access all supported registries using a single, unified protocol. The CORE Registration System maps the commands issued by the user to the corresponding EPP commands, sends them to the appropriate registry server and translates back the received results. Members do not need to cope with problems regarding registry communication (like different flavours of EPP, SSL⁄TLS certificate handling or Punycode conversion for internationalised domain names) themselves.

Since the CORE Registration System acts as a client regarding all the supported registries, its implementation also allowed CORE Internet Council of Registrars to gain considerable experience concerning all client side aspects of (different versions of) EPP. In particular, client-side EPP support had already started with the introduction of EPP by Afilias and Neulevel. On the server side, EPP has been in use since starting the operation of the puntCAT registry some five years ago. At the heart of the EPP implementation lies the so-called Unikit, CORE's EPP toolkit implementation. The Unikit includes code for the client side and for the server side. In the context of the .ART Registry, the server-side part of the Unikit will be used.

In the person of Klaus Malorny, CORE also actively participated in the IETF Provisioning Registry Protocol (provreg) working group and contributed to some RFCs (see Acknowledgements in RFCs 5730-5733 and RFC 5910).

The software implementing the actual shared registry system, including its EPP interface, was entirely built by CORE, involving an international team of developers from several member companies — thus demonstrating the software development skills at CORE's disposal.

2. Standards Compliance

The EPP interface of the .ART Registry, provided by the CORE Registration System, is fully compliant with RFCs 5730-5734. These define mappings for the provisioning and management of Internet domain names, Internet host names and individual or organisational social information identifiers ("contacts") stored in a shared central repository.

Apart from these standards, the .ART Registry also supports the proposed standard for DNSSEC (RFC 5910). This is an EPP extension mapping for the provisioning and management of Domain Name System security (DNSSEC) extensions for domain names stored in a shared central repository.

The proposed standard for an EPP extension for "grace period" policies defined by the Internet Corporation for Assigned Names and Numbers (ICANN) is fully supported also (RFC 3915). Such grace period policies exist to allow protocol actions to be reversed or otherwise revoked during a short period of time after the protocol action has been performed.

Furthermore, a few proprietary EPP extensions are used by the .ART Registry to allow registrars to provide trademark information during the Sunrise phase, auction information during Sunrise and Landrush phases as well as language information.

Documentation consistent with RFC 3735 for these proprietary EPP extensions can be found below.

All incoming requests will be validated against the schema definitions in the relevant RFCs and the ones of the proprietary EPP extensions, if applicable. This adds to security and stability, as invalid requests are dismissed early on. The EPP implementation of the .ART Registry is compatible with existing toolkits that produce valid EPP requests.

Pending, asynchronous operations are fully supported by the registry implementation. The SRS returns an EPP result code of 1000 if a command has succeeded synchronously, i.e. immediately. In contrast, a result code of 1001 is returned if a command was accepted but requires asynchronous processing before it can be completed.

3. Stability

A stable EPP interface is very important for smooth operation of a shared registry system. To ensure this, the CORE Registration System contains a multi-threaded, asynchronous communication implementation allowing a high number of concurrent EPP connections.

The incoming requests are filtered by their IP addresses via firewall rules in order to disallow access from unauthorised sites. This increases not only the security of the system, but also its stability, since the load on the EPP servers is reduced.

4. Equal opportunity

EPP access limitations for registrars are enforced by the CORE Registration System, allowing a certain number of concurrent connections only. This further enhances the stability of the system and is an important ingredient for equal opportunity as well. Registrars cannot effectively hinder their competitors from connecting by simply opening a great many connections themselves.

For the sake of equal opportunity, the .ART Registry also avoids first-come, first-served (FCFS) policies where possible. This is why the general availability (GA) phase is the only one using this principle. All popular domain names will probably have been registered already when GA starts (during previously conducted launch phases not using FCFS), so FCFS during GA does not contradict the idea of equal opportunity.

5. Proprietary Extensions

CORE Internet Council of Registrars has already shown its ability to design, specify and implement proprietary EPP extensions in the context of the puntCAT registry. There, extensions exist for the specification of promotion codes, sponsor e-mail addresses, application objects (used during the Sunrise phase) and poll messages to notify registrars about application outcomes, for example. In the following, the proprietary EPP extensions planned to be used for .ART are described.

5.1 Extension for Trademark Information during Launch Phases

The CORE Registration System used to operate the .ART Registry provides a proprietary EPP extension for submitting special data needed during launch phases.

5.1.1 Introduction

This part of this answer describes an extension mapping for version 1.0 of the Extensible Provisioning Protocol (EPP) described in RFC 5730. This mapping is an extension of the domain name mapping described in RFC 5731. It is specified using the Extensible Markup Language (XML) and XML Schema notation.

This extension serves the purpose of supplying and querying information for special phases, usually at the beginning of registry operation. A typical use case is a ”Sunrise” phase during which trademark holders have a prerogative to register a domain name related to their trademark. In particular, this extension allows the provisioning of trademark information and the querying of the current status of a domain name application.

In addition, the extension allows the specification of additional information about the application, such as the intended use for the domain name, a URL demonstrating prior use of similar names in other TLDs etc.; the registry’s Sunrise policy determines whether and how this information is utilised.

An extension to the <poll> command is not included. Registrars are notified of application results via the poll message mechanism already included in EPP.

This extension has been developed along the lines of the Internet draft by Tan and Brown (see http://tools.ietf.org/html/draft-tan-epp-launchphase-01). Even though that document is currently only a draft, it serves the purpose needed for the .ART Registry and is clearly a step forward regarding the standardisation of launch phase handling in EPP. Since this draft does not supply a schema definition at the moment, the CORE Registration System implements its own, which can be found in attachment Q25-Ext-LP.pdf, Section 1. Once the draft was augmented by a concrete schema definition, the CORE Registration System will be adapted to utilise it, retaining the custom XML namespace identifier. Once the draft becomes an RFC, a transition will be conducted to adopt the standard.

5.1.2 Object Attributes

This extension for launch phases adds additional elements to the EPP domain name mapping. Only new element descriptions are documented here.

Since registries usually allow multiple applications for a particular domain name during launch phases, an application object is used internally. Such an object has a unique ID that is returned upon creation and is used to refer to this application in further requests. Within this extension, an <lp:applicationID> element is used to specify this ID.

5.1.2.1 Phase

The <lp:phase> element can be used to distinguish multiple simultaneous launch phases. Its content is a server-defined identifier corresponding to a particular launch phase.

5.1.2.2 Application Status

The <lp:status> element is used to communicate extended status(es) of the application object, beyond what is specified in the object mapping to which this application object belongs.

The following status values are defined: ”pending”, the initial state of a newly-created application object; ”validated”, the application meets relevant registry rules; ”invalid”, the application does not validate according to registry rules; ”allocated”, the object corresponding to the application has been provisioned (one of two possible end states of an application object); ”rejected”, the object was not provisioned (the other possible end state).

5.1.2.3 Claim Data

An application may have one or more <lp:claim> elements. An <lp:claim> element describes the applicant’s prior right to the domain name.

The <lp:claim> element has the boolean ”preValidated” attribute, which indicates whether a third party validation agency has already validated the claim. When this attribute has a true value, the <lp:pvrc> element must always be present.

Several child elements of the <lp:claim> element are defined. <lp:pvrc>, the Pre-Validation Result Code, is a string issued by a third-party validation agent. <lp:claimIssuer> contains the ID of a contact object (as described in RFC 5733) identifying the contact information of the authority which issued the right (for example, a trademark office or company registration bureau). <lp:claimName> identifies the text string in which the applicant is claiming a prior right. <lp:claimNumber> contains the registration number of the right (i.e. trademark number or company registration number). <lp:claimType> indicates the type of claim being made (e.g. trademark, symbol, combined mark, company name). <lp:claimEntitlement> indicates the applicant’s entitlement to the claim (i.e. owner or licensee). <lp:claimRegDate> contains the date of registration of the claim. <lp:claimExDate> contains the date of expiration of the claim. <lp:claimCountry> indicates the country in which the claim is valid. <lp:claimRegion> indicates the name of a city, state, province or other geographic region in which the claim is valid. This may be a two-character code from World Intellectual Property Organisation (WIPO) standard ST.3.

5.1.2.4 Additional Application Information

An application may carry a <lp:applicationInfo> element. If present, it contains additional information (beyond the claim) about the application, such as the domain name’s intended use.

5.1.3 EPP Command Mapping

This section deals with the specific command mappings for the .ART Registry EPP extension for launch phases.

5.1.3.1 EPP Query Commands

There are four EPP commands to retrieve object information: <check> to find out whether an object is known to the server, <info> to ask for detailed

information associated with an object, <poll> to discover and retrieve queued service messages for individual clients and <transfer> to get transfer status information for an object.

5.1.3.1.1 EPP <check> Command

This extension does not add any elements to the EPP <check> command or to the <check> response described in the EPP domain mapping (s. RFC 5731).

5.1.3.1.2 EPP <info> Command

This extension adds elements to the EPP <info> command and response described in the EPP domain mapping for launch phase processing.

The EPP <extension> element of the <info> command contains a child <lp:info> element to indicate that an application object should be queried. It identifies the registry launch phase namespace and the location of the registry launch phase schema. The <lp:info> element contains the following child elements: <lp:applicationID>, the application identifier for which the client wishes to query, and <lp:phase> (optional), the phase the application is associated with.

When such an <info> command has been processed successfully, the EPP <extension> element in the response contains a child <lp:infData> element that identifies the registry launch phase namespace and the location of the registry launch phase schema. The <lp:infData> element contains the following child elements. <lp:applicationID> contains the application identifier of the returned application. <lp:phase> (optional) contains the phase the application is associated with. <lp:status> (optional) contains the status of the application. One or more <lp:claim> elements (optional) give the submitted data establishing the applicant’s prior right to the domain name.

If any <lp:claim> element is present, each of them may contain the following child elements. <pvrc> gives the Pre-Validation Result Code. <claimIssuer> contains the ID of a contact object representing the issuing authority. <claimName> contains the textual representation of the right. <claimNumber> contains the registration number. <claimType> contains the type of claim being made. <claimEntitlement> contains the entitlement. <claimRegDate> contains the registration date. <claimExDate> contains the expiry date.

If additional information about the application was specified when the application was created, an <applicationInfo> element will be present containing that information.

Examples of an <info> command and corresponding response can be found in attachment Q25-Ext-LP.pdf, Section 2.1. EPP <info> command, since the TLD Application System (TAS) is not well suited to pre-formatted text.

5.1.3.1.3 EPP <poll> Command

This extension does not add any elements to the EPP <poll> command or to the <poll> response described in the EPP domain mapping (s. RFC 5731).

5.1.3.1.4 EPP <transfer> Command

This extension does not add any elements to the EPP <transfer> command or to the <transfer> response described in the EPP domain mapping (s. RFC 5731).

5.1.3.2 EPP Transform Commands

There are five EPP commands to transform objects: <create> to create an instance of an object, <delete> to delete an instance of an object, <renew> to extend the validity period of an object, <transfer> to manage object sponsorship changes and <update> to change information associated with an object.

5.1.3.2.1 EPP <create> Command

This extension adds elements to the EPP <create> command and response described in the EPP domain mapping for launch phase processing.

The EPP <extension> element of the <create> command contains a child <lp:create> element to indicate that an application object for a launch phase should be created. It identifies the registry launch phase namespace and the location of the registry launch phase schema. The <lp:create> element contains the following child elements: <lp:phase> (optional), the phase the application should be associated with, zero or more <lp:claim> elements to substantiate the prior rights of the applicant, and an optional <lp:applicationInfo> element providing additional information about the application, such as the intended use of the domain name.

When such a <create> command has been processed successfully, the EPP <extension> element in the response contains a child <lp:creData> element that identifies the registry launch phase namespace and the location of the registry launch phase schema. The <lp:creData> element contains a child <lp:applicationID> element, which informs the registrar about the application ID the server has assigned.

Examples of a <create> command and corresponding response can be found in attachment Q25-Ext-LP.pdf, Section 2.2. EPP <create> command, since the TLD Application System (TAS) is not well suited to pre-formatted text.

5.1.3.2.2 EPP <delete> Command

This extension defines additional elements to extend the EPP <delete> command described in the EPP domain mapping for launch phase processing. No additional elements are defined for the <delete> response.

Clients may withdraw an application if permitted by registry policy. To do so, clients submit an EPP <delete> command along with an <lp:delete> element to indicate the application object to be deleted. The <lp:delete> element contains the following child elements: <lp:applicationID>, the identifier of the application to be deleted, and <lp:phase> (optional), the phase the application is associated with.

An example of a <delete> command can be found in attachment Q25-Ext-LP.pdf,

Section 2.3. EPP <delete> command, since the TLD Application System (TAS) is not well suited to pre-formatted text.

The CORE Registration System supports the withdrawal of an application using this extension to the <delete> command. Note, however, that support for the withdrawal of an application depends on the .ART Registry Sunrise policy, which is described elsewhere.

5.1.3.2.3 EPP <renew> Command

This extension does not add any elements to the EPP <renew> command or to the <renew> response described in the EPP domain mapping (s. RFC 5731).

5.1.3.2.4 EPP <transfer> Command

This extension does not add any elements to the EPP <transfer> command or to the <transfer> response described in the EPP domain mapping (s. RFC 5731).

5.1.3.2.5 EPP <update> Command

This extension defines additional elements to extend the EPP <update> command described in the EPP domain mapping for launch phase processing. No additional elements are defined for the <update> response.

Clients may modify an application if permitted by registry policy. To do so, clients submit an EPP <update> command along with an <lp:update> element to indicate the application object to be modified. The <lp:update> element contains the following child elements: <lp:applicationID>, the identifier of the application to be modified, and <lp:phase> (optional), the phase the application is associated with.

An example of an <update> command can be found in attachment Q25-Ext-LP.pdf, Section 2.4. EPP <update> command, since the TLD Application System (TAS) is not well suited to pre-formatted text.

The CORE Registration System supports the modification of an application using this extension to the <update> command. Note, however, that support for the modification of an application depends on the .ART Registry Sunrise policy, which is described elsewhere.

5.1.4 Formal Syntax

The formal syntax of this EPP extension is a complete schema representation of the object mapping suitable for automated validation of EPP XML instances. The schema definition is listed in attachment Q25-Ext-LP.pdf, Section 1. Schema Definition (Formal Syntax), since the TLD Application System (TAS) is not well suited to pre-formatted text.

5.2 Extension for Auction Information

The CORE Registration System used to operate the .ART Registry provides a proprietary EPP extension for submitting special data needed for auctions as they

occur after launch phases (e.g. Sunrise and Landrush).

5.2.1 Introduction

This part of this answer desribes an extension mapping for version 1.0 of the Extensible Provisioning Protocol (EPP) described in RFC 5730. This mapping is an extension of the domain name mapping described in RFC 5731. It is specified using the Extensible Markup Language (XML) and XML Schema notation.

This extension serves the purpose of supplying and querying information for special phases, usually at the beginning of registry operation. A typical use case is a ″Sunrise″ phase during which trademark holders have a prerogative to register a domain name related to their trademark.

Registries usually allow multiple applications for a particular domain name during launch phases. This extension helps to resolve such situations by means of an auction in an automated way. This is not a normal auction, however, insofar as every application has a ″bid″ associated with it. Bids cannot be modified after the phase the application belongs to has ended. Among all valid applications for a given domain name, the one with the highest bid wins the auction.

5.2.2 Object Attributes

This extension for auctions adds additional elements to the EPP domain name mapping. Only new element descriptions are documented here.

This extension allows the provisioning of auction information in the form of bids. A bid can be made when applying for a domain name. In case there is more than one valid application, an auction mechanism is used as a tie-breaker. The highest bid submitted for the domain name in question will win the auction.

5.2.2.1 Bid

The <auction:bid> element is used to set and inform about a bid for a domain name. Its content is the amount of money the applicant is willing to pay for the domain name in case of an auction. The currency is given in the required currency attribute, specified by the corresponding ISO 4217 currency code.

Note that the amount is given as a non-negative number. This allows to submit a bid of zero in case the applicant is not interested in an auction at all.

5.2.3 EPP Command Mapping

This section deals with the specific command mappings for the .ART Registry EPP extension for auctions.

5.2.3.1 EPP Query Commands

There are four EPP commands to retrieve object information: <check> to find out whether an object is known to the server, <info> to ask for detailed information associated with an object, <poll> to discover and retrieve queued service messages for individual clients and <transfer> to get transfer status

information for an object.

5.2.3.1.1 EPP <check> Command

This extension does not add any elements to the EPP <check> command or to the <check> response described in the EPP domain mapping (s. RFC 5731).

5.2.3.1.2 EPP <info> Command

This extension does not add any elements to the EPP <info> command described in the EPP domain mapping. Additional elements are defined for the <info> response.

When an <info> command has been processed successfully, the EPP <extension> element in the response, if present, contains a child <auction:infData> element that identifies the registry auction namespace and the location of the registry auction schema. The <auction:infData> element contains an <auction:bid> element, which informs about the amount and currency of the currently set bid as described above.

An example of an <info> response can be found in attachment Q25-Ext-Auction.pdf, Section 2.1. EPP <info> command, since the TLD Application System (TAS) is not well suited to pre-formatted text. The included example simply retrieves the current bid for the given domain name.

5.2.3.1.3 EPP <poll> Command

This extension does not add any elements to the EPP <poll> command or to the <poll> response described in the EPP domain mapping (s. RFC 5731).

5.2.3.1.4 EPP <transfer> Command

This extension does not add any elements to the EPP <transfer> command or to the <transfer> response described in the EPP domain mapping (s. RFC 5731).

5.2.3.2 EPP Transform Commands

There are five EPP commands to transform objects: <create> to create an instance of an object, <delete> to delete an instance of an object, <renew> to extend the validity period of an object, <transfer> to manage object sponsorship changes and <update> to change information associated with an object.

5.2.3.2.1 EPP <create> Command

This extension defines additional elements to extend the EPP <create> command described in the EPP domain mapping for auction processing. No additional elements are defined for the <create> response.

The EPP <extension> element of the <create> command contains a child <auction:create> element to indicate that auction information should be

submitted. It identifies the registry auction namespace and the location of the registry auction schema. The <auction:create> element must contain an <auction:bid> element, which specifies the amount and currency as described above.

An example of a <create> command can be found in attachment Q25-Ext-Auction.pdf, Section 2.2. EPP <create> command, since the TLD Application System (TAS) is not well suited to pre-formatted text. The included example sets the bid when applying for the given domain name to the specified amount.

5.2.3.2.2 EPP <delete> Command

This extension does not add any elements to the EPP <delete> command or to the <delete> response described in the EPP domain mapping (s. RFC 5731).

5.2.3.2.3 EPP <renew> Command

This extension does not add any elements to the EPP <renew> command or to the <renew> response described in the EPP domain mapping (s. RFC 5731).

5.2.3.2.4 EPP <transfer> Command

This extension does not add any elements to the EPP <transfer> command or to the <transfer> response described in the EPP domain mapping (s. RFC 5731).

5.2.3.2.5 EPP <update> Command

This extension defines additional elements to extend the EPP <update> command described in the EPP domain mapping for auction processing. No additional elements are defined for the <update> response.

The EPP <extension> element of the <update> command contains a child <auction:update> element to indicate that auction information should be updated. It identifies the registry auction namespace and the location of the registry auction schema. The <auction:update> element must contain an <auction:bid> element, which specifies the new amount and currency as described above.

Whether all modifications of bids are allowed, only certain ones (e.g. only increases) or none at all depends on the .ART Registry auction policy, which is described elsewhere.

An example of an <update> command can be found in attachment Q25-Ext-Auction.pdf, Section 2.3. EPP <update> command, since the TLD Application System (TAS) is not well suited to pre-formatted text. The included example modifies the bid for the given domain name.

5.2.4 Formal Syntax

The formal syntax of this EPP extension is a complete schema representation of the object mapping suitable for automated validation of EPP XML instances. The schema definition is listed in attachment Q25-Ext-Auction.pdf, Section 1. Schema Definition

(Formal Syntax), since the TLD Application System (TAS) is not well suited to pre-formatted text.

5.3 Extension for Language Information

The CORE Registration System used to operate the .ART Registry provides a proprietary EPP extension for internationalised domain names (IDNs).

5.3.1 Introduction

This part of this answer desribes an extension mapping for version 1.0 of the Extensible Provisioning Protocol (EPP) described in RFC 5730. This mapping is an extension of the domain name mapping described in RFC 5731. It is specified using the Extensible Markup Language (XML) and XML Schema notation.

This extension serves the purpose of supplying and querying information for internationalised domain names. In particular, the language or script used and domain name variants are addressed.

5.3.2 Object Attributes

This extension for IDNs adds additional elements to the EPP domain name mapping. Only new element descriptions are documented here.

5.3.2.1 Languages and Scripts

This extension allows the specification of either a language tag or a script tag when registering a domain name. The language or script defines the characters allowed for use in the domain name as specified in the IDN tables (see Question 44, Support for Registering IDN Domains). It is not allowed to specify more than one language or more than one script.

For the time being, the .ART Registry expects the value of a language tag element to be a an ISO 639-1 language code referring to a supported language. The value of a script tag is expected to be an ISO 15924 script code referring to a supported script.

5.3.2.2 Variants

This extension allows to specify a number of variants of the domain name to be registered together with the supplied domain name. The variants are expected to be submitted in normalised form (see also Q44, Support for Registering IDN domains). The number of variants that can be specified is limited to at most 10.

5.3.3 EPP Command Mapping

This section deals with the specific command mappings for the .ART Registry EPP extension for IDNs.

5.3.3.1 EPP Query Commands

There are four EPP commands to retrieve object information: <check> to find out whether an object is known to the server, <info> to ask for detailed information associated with an object, <poll> to discover and retrieve queued service messages for individual clients and <transfer> to get transfer status information for an object.

5.3.3.1.1 EPP <check> Command

This extension defines additional elements to extend the EPP <check> command described in the EPP domain mapping for IDN processing. No additional elements are defined for the <check> response.

The EPP <check> command is used to determine if an object can be provisioned within a repository. This IDN extension modifies base check processing to support language and script tags.

The EPP <extension> element, if present, contains a child <idn:check> element that identifies the registry IDN namespace and the location of the registry IDN schema. If at least one of the checked domains is an IDN, the <idn:check> element must contain either an <idn:lang> element or an <idn:script> element. The <idn:lang> element contains the language whose characters may be used in the checked domain names; the <idn:script> element contains the script whose characters may be used in the checked domain names. The language or script specification applies to all domain names specified in the command. The results of the check (i.e., the domains names' availability for provisioning) are governed by the validity of the names with respect to the specified language or script.

Examples of <check> commands can be found in attachment Q25-Ext-IDN.pdf, Section 2.1. EPP <check> command, since the TLD Application System (TAS) is not well suited to pre-formatted text. Two examples are included, one with a language tag (Section 2.1.1), one with a script tag (Section 2.1.2).

5.3.3.1.2 EPP <info> Command

This extension does not add any elements to the EPP <info> command described in the EPP domain mapping. Additional elements are defined for the <info> response.

When an <info> command has been processed successfully, the EPP <extension> element in the response, if present, contains a child <idn:infData> element that identifies the registry IDN namespace and the location of the registry IDN schema. The <idn:infData> element contains either an <idn:lang> element or an <idn:script> element. The <idn:lang> element contains the language that is set for the domain name object; the <idn:script> element contains the script that is set for the domain name object.

The <idn:infData> element also contains an <idn:variants> element, which in turn contains a (possibly empty) sequence of <idn:nameVariant> elements. The <idn:nameVariant> elements represent the variants that are registered together with the actual domain name.

Examples of <info> responses can be found in attachment Q25-Ext-IDN.pdf, Section 2.2. EPP <info> command, since the TLD Application System (TAS) is not

well suited to pre-formatted text. Three examples are included, one with a language tag only (Section 2.2.1), one with a script tag only (Section 2.2.2) and one with a language tag and variants (Section 2.2.3).

5.3.3.1.3 EPP <poll> Command

This extension does not add any elements to the EPP <poll> command or to the <poll> response described in the EPP domain mapping (s. RFC 5731).

5.3.3.1.4 EPP <transfer> Command

This extension does not add any elements to the EPP <transfer> command or to the <transfer> response described in the EPP domain mapping (s. RFC 5731).

5.3.3.2 EPP Transform Commands

There are five EPP commands to transform objects: <create> to create an instance of an object, <delete> to delete an instance of an object, <renew> to extend the validity period of an object, <transfer> to manage object sponsorship changes and <update> to change information associated with an object.

5.3.3.2.1 EPP <create> Command

This extension defines additional elements to extend the EPP <create> command described in the EPP domain mapping for IDN processing. No additional elements are defined for the <create> response.

The EPP <create> command provides a transform operation that allows a client to create an instance of a domain object. This IDN extension modifies base create processing to support language tags, script tags and domain name variants.

The EPP <extension> element, if present, contains a child <idn:create> element that identifies the registry IDN namespace and the location of the registry IDN schema. The <idn:create> element must contain either an <idn:lang> element or an <idn:script> element. The <idn:lang> element contains the language whose characters may be used in the domain name; the <idn:script> element contains the script whose characters may be used in the domain name.

The <idn:create> element must also contain an <idn:variants> element, which in turn contains a (possibly empty) sequence of <idn:nameVariant> elements. The <idn:nameVariant> elements represent the variants that are to be registered together with the actual domain name.

Note that the .ART Registry restricts the number of domain name variants given in the <idn:variants> element to at most 10. Submitting an empty <idn:variants> element is allowed; this will not register any domain name variants.

Examples of <create> commands can be found in attachment Q25-Ext-IDN.pdf, Section 2.3. EPP <create> command, since the TLD Application System (TAS) is not well suited to pre-formatted text. Three examples are included, one with a language tag only (Section 2.3.1), one with a script tag only (Section 2.3.2) and

one with language tags and variants (Section 2.3.3).

5.3.3.2.2 EPP <delete> Command

This extension does not add any elements to the EPP <delete> command or to the <delete> response described in the EPP domain mapping (s. RFC 5731).

5.3.3.2.3 EPP <renew> Command

This extension does not add any elements to the EPP <renew> command or to the <renew> response described in the EPP domain mapping (s. RFC 5731).

5.3.3.2.4 EPP <transfer> Command

This extension does not add any elements to the EPP <transfer> command or to the <transfer> response described in the EPP domain mapping (s. RFC 5731).

5.3.3.2.5 EPP <update> Command

This extension defines additional elements to extend the EPP <update> command described in the EPP domain mapping for IDN processing. No additional elements are defined for the <update> response.

The EPP <update> command provides a transform operation that allows a client to change the state of a domain object. This IDN extension modifies base update processing to support domain name variants.

The EPP <extension> element, if present, must contain a child <idn:update> element that identifies the registry IDN namespace and the location of the registry IDN schema. The <idn:update> element may contain an <idn:add> element and an <idn:rem> element. Each of these contain a (possibly empty) sequence of <idn:nameVariant> elements. Similar to the <update> command's elements <domain:add> and <domain:rem>, these are used to specify the domain name variants that are to be added to and removed from the domain object, respectively. If the EPP <extension> element is missing in the <update> command, no change to the domain name variants will be made.

Note that the .ART Registry restricts the number of domain name variants given in the <idn:add> and <idn:rem> elements to at most 10.

An example of an <update> command can be found in attachment Q25-Ext-IDN.pdf, Section 2.4. EPP <update> command, since the TLD Application System (TAS) is not well suited to pre-formatted text. The included example adds some variants to be associated with the given domain name while removing existing ones at the same time (Section 2.4.1).

5.3.4 Formal Syntax

The formal syntax of this EPP extension is a complete schema representation of the object mapping suitable for automated validation of EPP XML instances. The schema definition is listed in attachment Q25-Ext-IDN.pdf, Section 1. Schema Definition

(Formal Syntax), since the TLD Application System (TAS) is not well suited to pre-formatted text.

6. Resourcing plans

6.1 Initial Work

No resources are necessary for the initial implementation, since the CORE Registration System (including the EPP extensions) has already been implemented.

6.2 Ongoing Work

For registrar support regarding the EPP extensions, the following resource allocations are estimated:

First Level Support: 4 man hours per month.

Employees already working for CORE Internet Council of Registrars will be handling these tasks. The numbers above were determined by averaging the effort required for comparable tasks conducted by CORE in the past over the course of 12 months.

26. Whois

Q26 - Whois

1. Overview

The CORE Registration System used by CORE Internet Council of Registrars to operate the .ART TLD will offer Registration Data Directory Services (RDDS) in compliance with Specification 4 of the Registry Agreement, consisting of a Whois Service, Zone File Access and Bulk Registration Data Access.

2. Whois Service

2.1 Interfaces

2.1.1 Port 43 Whois Service

Whois data for .ART will be accessible via an interface on TCP port 43 at whois.nic.ART, using the ”Whois” protocol (as defined in RFC 3912).

While the interface is publicly available, general use is rate limited to prevent data mining and mitigate denial of service attacks. Registrars may request to be exempted from the rate limiting measures by specifying IP addresses or address ranges to be put on a whitelist. Clients sending Whois requests from whitelisted IP addresses have unlimited access to the service.

2.1.1.1 Input Format

The input sent by Whois clients to the port 43 Whois server consists of two parts: the query options (starting with a hyphen character) and the query itself.

By default, the port 43 Whois service searches for domain names and name server names matching the query string. By the following keywords, the search type can be specified explicitly:

* ”domain”: Search for domains with matching names or IDs.
* ”nameserver”: Search for name servers with matching names, IDs or IP addresses.
* ”contact”: Search for contacts with matching IDs.
* ”registrar”: Search for registrars with matching IDs or organisation names.

The remaining tokens in the input are taken as the search parameter. It may contain the percent sign (‘%’) as a wildcard for any number (including zero) of characters or the underscore character (‘_’) for a single character. For data mining prevention and resource protection, the number of objects returned for wildcard searches is limited to 50.

Evidently, the query format resulting from this input format specification is fully compliant with Specification 4, since it allows querying

* domains via: whois example.ART,
* registrars via: whois ”registrar Example Registrar, Inc.”,
* name servers via: whois ”ns1.example.ART” and
* name servers via: whois ”nameserver (IP Address)”.

2.1.1.2 Output Format

The Whois implementation used by CORE follows a template-based approach for its output to achieve maximum flexibility with regard to the desired format. Key-value output templates containing well-defined placeholders (e.g., for domain name, registrar name, name servers, or contact fields) for variable data allow customising the output for each response type to meet ICANN’s demands. To supply values for the placeholders in the templates, the local Whois database is fed with all properties of registrars, domains, contacts and name servers that need to be present in the Whois output. Metadata such as the ”last Whois update” date, is also available for use in templates. Thanks to this template mechanism, adjustments for changing requirements over time may be implemented easily.

Additionally, the Whois implementation supports internationalised output. If a contact uses ”localised” address fields in addition to ”internationalised” data (as supported by RFC 5733), some data fields may contain non-US-ASCII characters. Also, internationalised domain names (IDN) allow the use of non-US-ASCII characters.

The results of a Whois query are encoded using either the US-ASCII character set, or, if a valid character set has been specified via the -C query option, the selected character set. If the output contains characters for which no encoding exists in the selected character set, they are replaced with a question mark, and a warning comment is added to the beginning of the output. Please see the answer to question 44 for more information about IDN support.

The format for values such as dates, times and phone⁄fax numbers in the Whois output conforms to the mappings specified in the EPP RFCs 5730-5734, since the SRS enforces

compliant values for requests from registrars, stores them as received and feeds them to the Whois instances unmodified.

Overall, this means that the response formats for domains, registrars, and name servers, as described in ICANN's Specification 4 of the Registry Agreement, are fully supported by the Whois implementation used by CORE.

2.1.2 Web-based Whois Service

The web Whois service operated at whois.nic.ART shares the same functionality as the port 43 service, but receives query input via an HTML form. The output format is the same as for the port 43 service.

To prevent the Web interface from being abused for data mining, a CAPTCHA test ("Completely Automated Public Turing test to tell Computers and Humans Apart") must be passed upon each web Whois query before any response data is displayed.

2.2 Searchable Whois

CORE's Whois implementation offers search capabilities in accordance with Specification 2, Section 1.8. They allow complex searches for Whois database records based on the content of various data fields, thereby considerably exceeding common Whois query functionality.

This provides powerful means of information retrieval, such as finding all domain names registered by a certain person or company. When made available to unauthorised parties, this data may be abused for undesirable activities such as data mining (e.g. for advertising purposes) or social profiling. Restrictions must be imposed to prevent such abuse.

Consequently, this feature is offered exclusively on the web-based Whois interface (not the port 43 Whois), and is only available to authenticated users after they logged in by supplying proper credentials (i.e., user name and password). The .ART Registry will issue such credentials exclusively to eligible users and institutions that supply sufficient proof of their legitimate interest in extended Whois searches, like e.g. law enforcement agencies. Authorisation policies and procedures are established in close collaboration with ICANN, and in compliance with any privacy laws and policies that may apply.

The search capabilities offered meet and exceed the requirements of Specification 2:

* Searches using the wildcards '%' and '_' (with semantics as described above) are possible on the following fields (thus allowing partial matches):
** domain name
** contact data (across all contact types, including the registrant):
*** name
*** organisation
*** address fields (street, city, state/province, postal code, country code)
* Exact match searches are possible on the following fields:
** registrar ID
** name server name
** name server IPv4 or IPv6 address (if stored in the registry for glue records)
* Multiple such search criteria may be joined by the logical operators (listed in descending precedence):
** NOT

** AND
** OR

The web interface offers a graphical editor for convenient creation of complex searches, allowing to group sets of search criteria in order to override the defined precedence of operators (thus providing the equivalent of parentheses in classic boolean expressions).

The search results are presented as a list of domain names matching the criteria. If more than 50 results are found, only the first 50 matches are presented on the initial result page, along with an indication of the total number of matches. Links allow the user to navigate through pages of search results.

2.3 Whois Data Distribution

The Whois implementation used by CORE is written as an autonomous system component running in its own server instance, i.e. it is not part of the server running the SRS component. Multiple Whois instances, all serving the same SRS data, are run in parallel; these instances may be located in diverse locations (both geographically and in terms of network topology).

All instances of the Whois service operate on their own databases. This ensures a load decoupling between the SRS and the Whois servers - high request rates on the Whois servers will not affect the main registry system's performance, and vice versa.

The database of a Whois server is continuously synchronised with the registry's database via a VPN connection. A special communication protocol ("Whois feed") is used to supply information about objects that have been created, modified or deleted in the SRS to all connected Whois servers.

As soon as changes to the registry's database have been made persistent, these changes are forwarded to all Whois servers. The Whois servers update their own databases with the data and publish the new information. This way, changes to the registry will become visible on the Whois server typically in less than a minute, resulting in an RDDS update time well under the 60 minutes permitted by Specification 10.

The Whois feed protocol has been carefully designed to allow a graceful recovery from temporary SRS/Whois disconnections. In case of a communication problem or a maintenance of the Whois instance, changes that occurred since the last successful update are automatically identified and transferred.

2.4 Network Structure

The Whois network structure (for queries and the feed) is depicted in Figure Q26-F1.

The green path shows how a Whois instance is continuously fed with data from the SRS. To obtain updates, a Whois server instance (D) in the Demilitarised Zone (DMZ) maintains a TCP connection to the EPP backend (B) in the Trust zone through a firewall (C) which separates the two zones. The EPP backend fetches the required data from the primary SRS database (A) and sends a corresponding feed data stream to the Whois instance.

The yellow path illustrates the data flow of Whois queries. A port 43/web query coming in from the Internet enters the Untrust zone via a network router (1) and

passes a firewall (2) into the DMZ. A load balancer (3) dispatches the request to one of the available Whois instances (4), which processes the requests and sends the response back to the Whois client or web browser.

As the server hardware and network setup planned for the Whois subsystem is part of the overall registry infrastructure, it shares its design principles and implementation. Please see the answers to Questions 31 and 32 for further details.

2.5 Inner Workings of a Whois Server Instance

The inner structure of a Whois server instance is depicted in Figure Q26-F2. It shows how incoming port 43 or web traffic from a load balancer (at the top) is processed internally.

Port 43 queries are handled by the RFC 3912 protocol implementation. A rate limiter component ensures that query limits are enforced for connections not originating from whitelisted IP addresses. Non-blocked requests are passed on to a query evaluator component, which parses the request, fetches required data from the instance's local database engine and prepares the response based on the configured output templates. A separate statistics collector module gathers query statistics (such as query type and response time) in dedicated database tables; this data is used to create monthly ICANN reports.

Web-based queries are handled in a similar fashion. Clients connect to the Whois web frontend; if both the CAPTCHA and the rate limiter component are passed, the query from the web form is processed and answered (as well as included in statistics) just like port 43 requests. For this purpose, the web application container hosting the web Whois has direct access to the local database engine, i.e. it does not utilise the port 43 implementation, but processes requests autonomously. In contrast to the port 43 server, the web Whois also contains an LDAP authentication component; it is used to validate the credentials of users logging in for accessing the extended search features described above.

The bottom of the diagram shows the Whois feed client component, which is responsible for maintaining a connection to the Whois feed service of the EPP backend, processing the feed data and updating the local Whois database.

2.6 Whois Data Privacy Measures

The Whois server implementation used by CORE is designed to support various levels of privacy regarding the content of query responses.

2.6.1 Consideration of EPP Data Disclosure Preferences

The EPP 1.0 standard, particularly its contact mapping as described in RFC 5733, provides means for registrars to specify their preferences concerning the handling of contact data submitted to the registry. Using optional <contact:disclose> elements when creating or modifying contacts, the registrar is able to identify contact fields that require special handling regarding their disclosure to third parties.

The Whois service is designed to respect the data disclosure preferences specified by registrars using these mechanisms. Unless registry policy dictates otherwise, contact fields will be included in or excluded from the Whois output according to

the respective disclosure setting. The governing registry policy will be carefully tuned to be in line with applicable data protection laws.

2.6.2 Web Whois

The Whois server's web interface uses the same output restrictions as the port 43 interface.

The CAPTCHA mechanism used to let only humans (as opposed to machines) access the Web whois provides protection against Whois data abuses like data mining or spam. As an additional guard against spam, any e-mail addresses within the Whois output can optionally be displayed as images only (instead of HTML text).

2.7 Support for Emerging Technologies

CORE is aware of the shortcomings in today's RDDS technology. The Whois protocol, as defined in RFC 3912, only defines the basic exchange between client and server, without any specification of input and output formats. This has led to a large number of different output formats among registries, posing problems for automated Whois clients.

In September 2011, ICANN's Security and Stability Advisory Committee (SSAC) published SAC 051, a Report on Domain Name Whois Terminology and Structure. It contains recommendations for a domain name registration data access protocol suitable for replacing the current Whois technology. In February 2012, ICANN published a draft roadmap for the implementation of these recommendations. CORE is committed to participate in this process, and to comply with and fully support any future RDDS technologies (such as an XML-based, RESTful Whois) emerging from it.

2.8 Whois Resiliency and Performance

Thanks to the Whois subsystem's intrinsic ability to run an arbitrary number of Whois instances in geographically diverse locations (all fed from the same data source in a near-realtime fashion), it offers considerable resiliency. In such a setup, the outage of a single Whois instance will not disrupt Whois services for Internet users.

The same feature also guarantees a high level of scalability and performance. Should the monitoring system operated by CORE suggest an increased demand for Whois queries for names in the .ART TLD, additional Whois servers can quickly be added to the existing setup. The decoupling of SRS and Whois services described above ensures that bursts in Whois usage will not impact SRS performance. Using such scaling measures if need be, even unusual peak volumes can be handled.

Please see the answer to question 34 (Geographic Diversity) for details about the locations planned for .ART Whois instances.

In the initial setup, each Whois instance is capable of handling up to 500 queries per second. It is assumed that the average load will be at most 100 queries per second, so there is sufficient headroom for future load increases and bursts.

2.9 Compliance with Specification 10 of the Registry Agreement

The technical features described above ensure that the RDDS (Whois) implementation provided by the CORE Registration System for .ART will be in full compliance with Specification 10 of the Registry Agreement. RDDS availability, query round trip time (RTT) and update time will be maintained well within the permissible limits.

Due to the unpredictable complexity of searches conducted using wildcards or boolean operators, it is assumed that they are not used in queries for measuring RDDS availability and query RTT. Also, the service levels for these two metrics are only guaranteed for queries returning a maximum of 10 results.

3. Zone File Access

CORE will enter into standardised agreement with Internet users seeking access to .ART zone file data by following the procedures laid out in Specification 2, Section 2. For this purpose, the SRS prepares a .ART zone data file compliant with the specified File Format Standard, which is made available at the ICANN-specified and managed URL (i.e. ftp://ART.zda.icann.org). Through facilitation of the CZDA provider, users presenting sufficient credentials will be granted access to this data. Full cooperation and assistance will be provided to ICANN and the CZDA provider in this context.

In addition, bulk access to the zone files for .ART will also be provided to ICANN or its designee, as well as to the Emergency Operators on a continuous basis.

4. Bulk Registration Data Access

As described in the answer to question 38 (Data Escrow), the Escrow module of the CORE Registration System is capable of creating files containing Thin Registration Data, as well as Thick Registration Data restricted to the domain names of a single registrar. Using this facility, CORE will grant ICANN periodic access to Thin Registration Data, as well as exceptional access to a failing registrar's Thick Registration Data, in a format and on a schedule fully compliant with Specification 2, Section 3.

5. Experience in providing ICANN-compliant Whois services

CORE has been operating Shared Registry Systems (SRS) since 1997, which all require a connected port 43 Whois server. In its role as the registry backend operator for .cat and .museum, CORE has continuously provided (and still provides) reliable Whois services for these registries, being in full compliance with RFC 3912 and ICANN registry agreements.

The experience gathered from these previous Whois related activities enables CORE to develop and operate a Whois subsystem for the .ART Registry that is fully compliant with all ICANN requirements.

6. Resourcing Plans

The CORE Registration System already supports the Whois services as described above at the time of writing. Since the system is designed to be highly configurable, the realisation of different privacy policies merely requires changing the respective settings within the system configuration.

This means that no development resources will be needed for the Whois service during the initial setup of the system. However, the staff on duty at CORE will need to define the related policies and configure the system accordingly.

6.1 Initial implementation

For the initial setup, the following resources are allotted:

* Registry Policy Officer: finalising policies, creating documentation: 1.5 man days
* System Administrator: configuring system for policies: 4 man hours
* First Level Support: training: 2 man hours per person

6.2 Ongoing maintenance

For the ongoing system maintenance, the following resources are allotted:

* System Administrator: system maintenance: 0.5 man days per month
* First Level Support: support: 6 man hours per month
* Second Level Support: access authorisation: 5 man hours per month

Employees already working for CORE Internet Council of Registrars will be handling these tasks. The numbers above were determined by averaging the effort required for comparable tasks conducted by CORE in the past over the course of 12 months.

27. Registration Life Cycle

Q27 - Registration Life Cycle

The CORE Registration System used by CORE Internet Council of Registrars to operate the .ART TLD implements a registration life cycle that conforms with best practices and procedures widely used by existing top level domain registries. While the life cycle fully complies with all relevant EPP RFCs, it also simplifies the processing of automatic domain renewals in order to ease domain data management for registrars.

The attached state diagram (Figure Q27-F1) depicts the typical life cycle of a .ART domain during the General Availability phase, from its creation to its release. In the following, the various triggers, states and transitions involved in the registration life cycle (denoted by capital letters in parentheses) are described in detail. Blue boxes denote domain states, yellow boxes denote actions caused by registrar commands, grey boxes denote automatic actions by the system, white boxes denote timed conditions reached at some point in the life cycle.

1. Domain Creation

(A) After receiving a <domain:create> command from the registrar’s EPP client, the specified domain name is checked for availability and compliance with the registry’s rules and policies. If these checks are passed, a corresponding domain object is created in the repository. Its expiration date is set according to the registration period specified in the <domain:create> command (1-10 years) and the EPP command’s time stamp.

With its creation, the domain also enters the Add Grace Period (AGP), which lasts 5 days; during this time frame, the registrar may delete the domain for a full refund of the registration fee (as long as the limits specified by the AGP Limits Policy are not exceeded). Also, a domain deleted during the AGP will not enter the Redemption Grace Period (RGP), but will instead be released immediately. To indicate the AGP, the domain's Grace Period (GP) status according to RFC 3915 is set to "addPeriod"; this status is automatically removed after the end of the AGP.

(B) The domain is registered. Provided that at least two name servers are present in the domain and the domain has not been put into status "clientHold" or "serverHold", it is published in the TLD zone and carries the EPP status "ok". If no name servers are associated with the domain, the domain carries the EPP status "inactive" to indicate that no delegation information is present. Note that a .ART domain may either have zero name servers or 2-13 name servers; the case of exactly one name server is prohibited by server policy. In any case, the domain's current data is published on the Whois server (according to the disclosure settings set by the registrar).

2. Domain Update

(C) After receiving an EPP <domain:update> command, the domain is modified in the repository according to the data specified in the command. The domain returns to the registered state (B). Should the update change the domain's name servers or its "clientHold" status, its publication in the TLD zone is affected according to the condition described in state (B). An update command may set other domain status values, such as "clientDeleteProhibited"; see below for a full list of all supported status values. The TLD name servers and Whois servers are updated to reflect the domain's new data.

3. Domain Renewal (Automatic or Explicit)

(D) If a domain reaches its expiration date, it is automatically renewed; it will not be deleted, but remains in the registered state. Note that, in order to avoid unduly disruption of the domain's operation, this automatic renewal will even take place if the domain carries the status "clientRenewProhibited"; this status will only disallow the explicit renewal of domains.

(E) With reaching its expiration date, the domain enters the so-called "Auto Renew Grace Period" (ARGP), which lasts 45 days. During this time period, the registrar has the opportunity of deleting the domain name without being charged for the renewal. In order to avoid the necessity of a refund in this case, the CORE Registration System only charges the registrar with the renewal fee after the end of the ARGP (i.e., when the renewal is final). If the registrar deletes the domain during the Auto Renew Grace Period, nothing has been charged yet, so no refund is required either. Note that this differs from the commonly used practice of charging the renewal fee already at the beginning of the Auto Renew Grace Period, which requires complicated refunds in case the domain is deleted or transferred in this period. During the Auto Renew Grace Period, the domain carries the "autoRenewPeriod" GP status, which is also displayed in the Whois along with the previous expiration date (now in the past). Only after the end of the Auto Renew Grace Period, the expiration date is increased.

(F) If the end of the ARGP is reached before the registrar deletes the domain, the registrar is charged with the renewal fee. The domain's "autoRenewPeriod" GP status is removed.

(G) After explicit renewal (or final automatic renewal), the domain's expiration date is increased. The domain's Whois output is changed to reflect this.

(H) If the registrar explicitly renews a domain by sending a <domain:renew> EPP command, the CORE Registration System increases the domain's expiration date according to the period value specified in the command. Note that a domain's remaining registration period may not last more than 10 years; renewal requests that would make a domain exceed this limit are rejected. The registrar is charged with the corresponding renewal fee. The domain's "Renew Grace Period" is started, which lasts 5 days; during this period, the domain may be deleted for a full refund of the renewal fee. This is indicated via the "renewPeriod" GP status, which is automatically removed when the Renew Grace Period ends.

4. Domain Deletion

(I) After receiving an EPP <domain:delete> command, the deletion of the domain from the repository is initiated.

(J) If the domain is in its AGP when the delete command is received, it will be released immediately, i.e. it will be available for new registrations right away. The domain will not enter the Redemption Grace Period (RGP) in this case, and the registrar receives a refund of the registration fee (as long as the limits specified by the AGP Limits Policy are not exceeded).

(K) The domain is released (i.e., purged from the repository) and available for new registrations. This marks the end of the domain's life cycle. If the domain was in its Add, Auto Renew, Renew or Transfer Grace Period when the delete command was received, the related charges are refunded to the sponsoring registrar.

5. Domain Restore After Deletion - the Redemption Grace Period (RGP)

(L) If the domain is not in its AGP when the delete command is received, it enters the Redemption Grace Period (RGP), which lasts 30 days. This means that the domain is not released immediately, but is only put into the EPP status "pendingDelete" (which is also displayed in the domain's Whois output) and withheld from DNS publication.

The CORE Registration System fully supports the Redemption Grace Period procedures and protocols, as defined by RFC 3915. During the RGP, the domain may be restored by the previous registrar by sending a <domain:update> command carrying an EPP RGP extension according to the RFC.

(M) The domain is in the Redemption Grace Period (RGP). During this phase, it is not present in the TLD zone. The domain carries the EPP status "pendingDelete" and the RGP status "redemptionPeriod" according to RFC 3915.

(N) If the domain is not restored by the previous registrar before the end of the RGP, the domain will be scheduled for release. The EPP status "pendingDelete" is retained, the domain's RGP status is changed to "pendingDelete".

(O) The domain is no longer restorable by the registrar and due for release. It will remain in this state for a time period defined by registry policy; this could, for example, be a variable time period with a random offset in order to make the release date and time less predictable for domain snipers. Once this time period ends, the

domain is released and put into the final state (K).

(P) If the previous registrar restores the domain before the end of the RGP (by sending a <domain:update> command carrying an EPP RGP extension according to RFC 3915), the domain's RGP status is changed to "pendingRestore". If the registrar also sends the RGP restore report within 5 days (or along with the update command), the "pendingDelete" status value is removed from the domain and the domain will be put back into the registered state (B). If the conditions described under (B) are met, the domain will be re-added to the TLD zone. If, however, the restore report is not received within 5 days, the domain goes back into the RGP (RGP status "redemptionPeriod"), i.e. into state (M); the RGP is not restarted in this case, but is resumed at the point when the restoration was initiated by the registrar.

6. Domain Transfer

(Q) Upon request by a domain's registrant, a registrar (called "gaining" registrar in this case) may request to transfer a domain name currently sponsored by a different registrar (the so-called "losing" registrar) into its own domain portfolio. This is done by sending an EPP <domain:transfer> command with operation "request". After receiving such a command, the domain is marked with a "pendingTransfer" EPP status value. <domain:trnData> EPP poll messages are placed in the message queues of both gaining and losing registrar to inform them about the transfer request. The gaining registrar is charged with the transfer fee.

A request for a domain transfer will only succeed if certain conditions are met. In particular, the provided authorisation information must be correct, and the domain must not have the "clientTransferProhibited" or "serverTransferProhibited" status values set. Note that the status "serverTransferProhibited" is automatically set and maintained for 60 days by the SRS after a domain is first created, as well as after each successful registrar transfer. This is common practice among registries and avoids the problem of "registrar hopping", i.e. frequent registrar changes (after e.g. hijacking a domain name) in order obstruct takedown procedures.

(R) The domain transfer is pending. The CORE Registration System waits for either the transfer to time out (after 5 days), or for the reception of an approval, rejection or cancellation before the time-out. The losing registrar may approve or reject the transfer by sending an EPP <domain:transfer> command with operation "approve" or "reject", respectively. The gaining registrar may cancel the transfer by sending an EPP <domain:transfer> command with operation "cancel".

(S) The transfer was completed successfully, either by approval of the losing registrar or by time-out (which by default automatically approves the transfer; this behaviour is configurable). The "pendingTransfer" EPP status value is removed from the domain. The domain is assigned to the gaining registrar and removed from the losing registrar's portfolio. <domain:trnData> poll messages are placed in the message queues of both gaining and losing registrar. The domain returns to status (B). A successful transfer starts the domain's "Transfer Grace Period" (TGP) which lasts 5 days; during the TGP (which is indicated by the "transferPeriod" GP status), the domain may be deleted by the gaining registrar for a full refund of the transfer fee.

(T) The transfer was unsuccessful, i.e. it was rejected by the losing registrar or cancelled by the gaining registrar. The EPP status "pendingTransfer" is removed from the domain. <domain:trnData> poll messages are placed in the message queues of both gaining and losing registrar. The domain returns to status (B). The transfer fee previously charged to the gaining registrar is refunded.

7. EPP and Grace Period Status Values

As described above, the .ART domain life cycle involves various EPP Domain and Grace Period status values and uses them in compliance with RFCs 5730-5733 and 3915 (note that RFC 5910 does not specify any status values). This section provides an overview of the status values and describes whether and how they are used in the life cycle.

In general, status values starting with ”client” may only be set or removed by the registrar, while all other status values (including those starting with ”server”) may only be set or removed by the registry, either automatically or manually by registry staff.

7.1 EPP Domain Status Values (from RFC 5731)

* clientDeleteProhibited: Indicates that the domain cannot be deleted by a <domain:delete> command.
* clientHold: Indicates that the domain is not published in the .ART zone.
* clientRenewProhibited: Indicates that the domain cannot be renewed by an explicit <domain:renew> command; the status does not prevent automatic renewal.
* clientTransferProhibited: Indicates that the domain cannot be transferred.
* clientUpdateProhibited: Indicates that the domain cannot be modified.
* inactive: The domain has no delegation information, i.e. no name servers are associated. The domain is not published in the .ART zone.
* ok: The domain is active, i.e. it resolves, has no pending operations or prohibitions, and carries no other status values.
* pendingCreate: Indicates that the domain’s creation is pending, i.e. that an asynchronous process is in progress to finish the domain’s creation. This status is supported, e.g. for use during launch phases such as Sunrise and Landrush (to indicate that a domain application’s asynchronous review is pending); please refer to the answer to question 29 (Rights Protection Mechanisms) for more information about the special life cycle support offered by the CORE Registration System for launch phases.
* pendingDelete: Indicates that the domain is being deleted; depending on its RGP status (see below), it may be restorable or not.
* pendingRenew: Indicates that the domain is pending a renewal. While supported by the CORE Registration System, this status not used in the designated .ART domain life cycle.
* pendingTransfer: Indicates that the domain is in the process of being transferred from one registrar to another registrar.
* pendingUpdate: Indicates that an update to the domain is pending, i.e. that an asynchronous process is in progress to finish the domain’s modification. While supported by the CORE Registration System, this status not used in the designated .ART domain life cycle.
* serverDeleteProhibited: Indicates that the domain cannot be deleted.
* serverHold: Indicates that the domain is not published in the .ART zone.
* serverRenewProhibited: Indicates that the domain cannot be renewed by an explicit <domain:renew> command; the status does not prevent auto-renewal.
* serverTransferProhibited: Indicates that the domain cannot be transferred. This status is automatically set and maintained for 60 days by the SRS after a domain is first created, as well as after each successful registrar transfer.
* serverUpdateProhibited: Indicates that the domain cannot be modified.

7.2 EPP Grace Period Status Values (from RFC 3915)

* addPeriod: Indicates that the domain is in the Add Grace Period.
* autoRenewPeriod: Indicates that the domain is in the Auto Renew Grace Period.
* renewPeriod: Indicates that the domain is in the Renew Grace Period.
* transferPeriod: Indicates that the domain is in the Transfer Grace Period.
* pendingDelete: Indicates that a deleted domain is scheduled for release, i.e. it can no longer be restored by the registrar.
* pendingRestore: Indicates that a request to restore a deleted domain has been received, and that the registry awaits the restore report from the registrar.
* redemptionPeriod: Indicates that a deleted domain is in its Redemption Grace Period, i.e. it may be restored by the registrar.

8. Consistence with Commitments to Registrants

The registration life cycle described above is consistent with the registry's commitments to registrants, as laid out in the answer to Question 30a. In particular, the handling of auto-renewals and the Redemption Grace Period ensures the "Protection of Investment" part of that commitment, since it protects the domain from vanishing unintendedly.

9. Resourcing Plans

The CORE Registration System already supports the life cycle described above at the time of writing. Since the system is highly configurable, the adjustment of any variables and flags defining the process (such as name validity policies, or the durations of involved grace periods and time-outs) merely requires changing the respective settings within the system configuration. No coding is required for this, which means that no special developing resources will be needed. However, the staff on duty at CORE Internet Council of Registrars will need to define the related policies and set up the system to support and maintain the desired registration life cycle.

For the initial setup, the following resources are allotted:

* Registry Policy Officer: finalising policies, creating documentation: 3 man days
* System Administrator: configuring system for policies: 4 man hours
* First Level Support: training: 3 man hours per person

For the ongoing maintenance, the following resources are allotted:

* System Administrator: 4 man hours per month

Employees already working for CORE Internet Council of Registrars will be handling these tasks. The numbers above were determined by averaging the effort required for comparable tasks conducted by CORE in the past over the course of 12 months.

28. Abuse Prevention and Mitigation

As the registry backend provider for .ART, CORE Internet Council of Registrars will work in close cooperation with the .ART Registry to establish thorough and effective methods to prevent abuse of .ART domain names, .ART registrant data or the associated infrastructure, as well as to mitigate any impact from such abuse (should

it occur despite the preventive measures). In order to achieve this, the .ART Registry and CORE Internet Council of Registrars are committed to deploy extensive organisational and technical measures; these are described in the following.

1. Rapid Takedown Policy for Cases of Malicious Activity

The .ART Registry (and CORE Internet Council of Registrars as its technical provider) are committed to closely collaborate with law enforcement authorities and security agencies in order to take quick action in case a .ART name is reported to be involved in malicious activity. For this purpose, a ”Rapid Takedown Policy” is established that

identifies cases of malicious activity,

defines ways for the registry to be notified of such activity (e.g. via a dedicated web site, e-mail address or phone hotline),

defines clear and consistent procedures to quickly stop the malicious activity (after the activity was confirmed and impact of the measures has been assessed),

defines related service levels (e.g. with respect to the maximum time the registry may take to respond to takedown requests),

defines rules regarding the notification of involved parties (registrant, administrative contact, technical contact, registrar, informant, the public),

defines ways to appeal against any measures taken,

defines how cases covered by the policy need to be documented and reported.

In this context, cases of malicious activity may include (but are not limited to)

wrong, invalid or harmful DNS setup (e.g. pointers to false IP addresses),

use of trademarked or otherwise reserved names without proper rights,

use of the domain in actions that affect the stability and security of the Internet (e.g. in Denial of Service (DoS), Distributed Denial of Service (DDoS) attacks or botnets),

use of the domain for the distribution of malware (such as computer viruses, worms, Trojan horses, spyware or rootkits),

use of the domain for phishing or scamming,

use of the domain for spamming (affecting e-mail or other forms of electronic messaging),

maintaining invalid registrant contact data in the domain.

Where applicable, the policy includes metrics and thresholds for finding quantitative indications of malicious conduct.

Procedures to stop malicious activity may include (but are not limited to)

notifying the domain’s sponsoring registrar, specifying a deadline until which the activity needs to be ceased,

notifying the domain's registrant, administrative or technical contact directly (again specifying a deadline until which the activity needs to be ceased),

locking the domain and putting it on hold in order to prevent changes to the domain and to remove it from the .ART zone ("takedown"),

deleting the domain name and blocking it from further registration if need be.

Escalation rules (defining which steps are to be taken in which order and conditions for moving on to the next, more drastic measure) are part of the policy.

Since removing a domain name from the .ART zone usually has serious consequences (such as rendering web sites and e-mail addresses utilising the domain name unusable), the .ART Registry (and CORE Internet Council of Registrars as its technical provider) will, in accordance with the policy, exercise extreme caution with regard to any takedown decision. At the same time, the .ART Registry is aware that malicious activity potentially affects a large number of Internet users, which sometimes warrants drastic measures. The Rapid Takedown Policy aims at finding appropriate measures, taking the interests of all involved parties into consideration.

The Rapid Takedown Policy will be announced to both .ART registrars and .ART registrants and be part of the Registry-Registrar Agreement (RRA) and the .ART registration terms.

For cases of phishing, the .ART Registry will work closely with all relevant Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) of the area to develop an anti-phishing-specific simplified Rapid Takedown Policy. The goals will be to:

get all CERTs and CSIRTs of the area (at least, but open to other CERTs) accredited as authorised intervenors,

develop criteria and checklists for domain names eligible for rapid suspension,

develop a secured communications method between the authorised intervenors and the .ART Registry, including an Affidavit form.

Names reported by authorised intervenors will be suspended in less than 4 hours. This system should expand to a global authorised intervenors list. In this regard, the .ART Registry will work with the Anti-Phishing Working Group and other initiatives in order to develop and complete their proposed Accelerated Take Down proposal, which is still in beta stage.

2. Abuse Point of Contact

To ensure that the .ART Registry gets notified of any cases of abuse as quickly and easily as possible, an area of the public web site operated by the .ART Registry for the .ART TLD will be dedicated to the reporting of such cases. The respective web pages establish a single point of contact where abuse cases can be reported via a simple web form. An e-mail address and a phone number will also be provided as alternative means of communication.

Every case reported will raise a high-priority ticket within the .ART support staff's ticket system, examined immediately and treated in accordance with the Rapid Takedown Policy.

3. Prevention of Domain Name Tasting and Domain Name Front Running

The life cycle of a .ART domain name includes a 5-day Add Grace Period (AGP) during which a newly created domain name may be deleted with a refund of the domain fee. This is common practice and corresponds to the policies of almost all existing generic top level domains.

However, in the past the Add Grace Period has been abused for practices such as domain name tasting and domain name front running. Domain name tasting means that domains were created simply for the purpose of testing whether revenue can be generated by e.g. creating a web page with advertisements for the domain; if this was found feasible within the first few days, the domain was retained, otherwise it was deleted within the add grace period for a full refund, i.e. the domain was ”tasted” for potential revenue without any payment to the registry. Domain name front running refers to the practice of pre-registering domain names somebody has merely expressed interest in (e.g. by searching for them on the Whois web frontend of a registrar) with the purpose of reselling the domain to that person (at an inflated price) afterwards; again, the Add Grace Period has been abused for this purpose, since a registrar could do that without any cost (if the unsold domain was deleted before the end of the add grace period).

In 2008, ICANN introduced the so-called ”AGP Limits Policy” (http://www.icann.org/en/tlds/agp-policy-17dec08-en.htm) which addresses these and other issues resulting from the Add Grace Period. As the registry operator for the .ART TLD, CORE Internet Council of Registrars will fully implement this policy by restricting Add Grace Period refunds to registrars according to the limits specified by the policy. At the end of every month, the registration system’s billing module will determine every registrar’s net domain adds and check whether the add grace period refunds granted during that month exceed the permissible number according to the policy; if this is the case, additional charges to the registrar’s account will be initiated to effectively revert the excessive refunds.

Any exemption requests by registrars, whether they were granted (as permitted by the policy) or rejected, are documented, and such documentation will be maintained and made available for review by ICANN on request. The registry’s monthly report to ICANN will contain per-registrar information on the granted add-deletes, as well as additional columns regarding the exemption requests.

The related report columns are (with column header names in parentheses):

number of AGP deletes (”domains-deleted-grace”)

number of exemption requests (”agp-exemption-requests”)

number of exemptions granted (”agp-exemptions-granted”)

number of names affected by granted exemption request (”agp-exempted-domains”)

4. Prevention of Domain Name Sniping (Grabbing)

Domain name sniping (also known as ”grabbing”) is another common abuse pattern; the name refers to the practice of trying to re-register potentially interesting domain names immediately after they are deleted (sometimes by accident, or because a registrant failed to renew the domain with his registrar in time).

Since .ART domains are (per registry policy) automatically renewed when they reach their expiration date, no explicit renewals by registrars are required to prevent a domain name from being deleted when they expire. Registrars need to explicitly delete domains in order to release them for re-registration. This substantially

reduces opportunities for domain name sniping.

However, registrars may still send unintended domain deletions, i.e. due to clerical errors or miscommunication with the registrants. Even for these cases, measures against domain sniping are in place. Starting in 2002, registries have begun to implement an ICANN proposal, the so-called ”Redemption Grace Period” (RGP, http://www.icann.org/en/registrars/redemption-proposal-14feb02.htm). The proposal recommends to introduce a 30-day period after a name’s deletion during which the name is removed from the TLD zone (in order to give the registrant the chance to take notice of his name’s deletion) but is still eligible for being restored by the previous registrar/registrant. Supporting the RGP significantly reduces chances for domain grabbers to obtain inadvertently deleted domains, since a registrant gets 30 days to notice the mistake and to restore the domain before it becomes available for re-registration.

The CORE Registration System used by CORE Internet Council of Registrars to operate the .ART TLD supports the Redemption Grace Period as proposed by ICANN and implements it in full compliance with RFC 3915 (”Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (EPP)”).
5. Prevention of Orphaned Glue Records

According to the definition found in the ”SSAC Comment on the Orphan Glue Records in the Draft Applicant Guidebook” (http://www.icann.org/en/committees/security/sac048.pdf), a glue record becomes an ”orphan” when the delegation point NS record (the ”parent NS record”) that references it is removed while retaining the glue record itself in the zone. Consequently, the glue record becomes ”orphaned” since it no longer has a parent NS record. In such a situation, registrars and registrants usually lose administrative control over the record, and the record’s attribution to a certain registrar may become unclear, which makes it a potential vector for abuse.

The glue record policy in effect for the .ART TLD avoids this situation entirely by disallowing orphan glue records altogether. This corresponds to policy #3 mentioned in Section 4.3 (page 6) of the SSAC document mentioned above. The technical implementation within the CORE Registration System and its associated zone generation process ensures this by the following measures:

As a general principle, glue records are only created if they are really necessary, i.e. only in the case where a name server (e.g. ”ns.example.ART”) is used for the delegation of a superdomain of its own name, e.g. ”example.ART” in this example. If the same name server is used for e.g. ”example2.ART”, no glue record is created.

A host object within the .ART TLD (like ”ns.example.ART”) cannot exist without its parent domain (”example.ART”). Any attempt to create the host ”ns.example.ART” will be rejected by the SRS if the domain ”example.ART” doesn’t already exist or is not sponsored by the registrar creating the host. Likewise, the domain ”example.ART” cannot be deleted by the registrar if subordinate hosts like ”ns.example.ART” still exist. These subordinate hosts have to be deleted before the domain itself may be deleted; if such hosts are used in delegations for other .ART names, these delegations in turn have to be removed before the host may be deleted.

If a domain name is put on hold (e.g. as a consequence of the Rapid Takedown Policy described above), this not only means that the delegation for the name itself is removed from the zone; it also means that any occurrences of NS records referencing a name server that is subordinate to the domain are also removed from other .ART domains, along with any accompanying glue records. The same of course

holds true should the domain name have to be deleted entirely by the registry.

Consequently, no glue records can exist for a certain domain in the .ART zone after that domain is put on hold or deleted as part of abuse prevention or mitigation procedures.

It should be noted that this policy may lead to other domains (not directly involved in the abuse case) being affected by the takedown if they were delegated to a name server subordinate to the offending domain. Depending on their overall DNS architecture, such domains may become unreachable or less reachable after the delegation point is removed. While this could in theory be avoided by a less rigid orphan glue record policy, the overall benefit of adopting the strict policy described above is deemed higher than the potential damage to domains using a DNS infrastructure depending on an offending domain name.

6. Preventing Use of Trademarked, Reserved, Invalid, Illegal or Otherwise Unsuitable .ART Names

As laid out in the answer to Question 29 (Rights Protection Mechanisms), the .ART Registry takes extensive measures to protect the legal rights of others (such as trademark holders) with regard to .ART domain names. This includes

conducting a Sunrise phase to allow trademark holders to secure names related to their trademarks prior to GA,

accessing a Trademark Clearinghouse to validate trademarks presented by registrants,

offering a Trademark Claims Service, at least during the first 60 days of general availability,

taking precautions against phishing and pharming and

committing to full compliance with established Dispute Resolution and Suspension Procedures, including the Uniform Rapid Suspension (URS), the Trademark Post-Delegation Dispute Resolution Procedure (Trademark PDDRP), and the Uniform Domain Name Dispute Resolution Policy (URDP).

Please refer to the answer to Question 29 for more detailed information on these measures.

In addition to these specific rights protection measures, the CORE Registration System provides the following general means to make sure that no .ART names are registered which are for other reasons deemed invalid, reserved, illegal, offensive or unsuitable.

6.1 Rule Engine

For the most part, this is achieved by the deployment of a complex rule engine that checks each registered name at the time of registration for compliance with a configurable set of rules. Among other things, these rules include

a test to ensure that the domain name has the proper number of labels (which is two for a traditional registry that allows only second level domains to be registered),

a test to ensure that no hyphens occur in position 3 and 4 of any of the domain's U-labels (to protect "xn--" and future ACE prefixes),

a test to disallow hyphens at the beginning or end of the name,

a test to disallow ASCII characters which are neither a letter, nor a digit or a hyphen,

a test to find invalid IDN characters, i.e. characters not contained in any of the supported IDN tables,

a test to disallow reserved geopolitical names,

a test to disallow registry reserved names,

a test to disallow ICANN reserved names,

a test to disallow otherwise reserved or unsuitable names.

Please refer to the answer to Question 44 (Internationalised Domain Names) for more information on the rules governing valid IDNs in the .ART TLD.

For the tests checking for reserved names, custom lists of labels can be conveniently maintained by the .ART Registry to define the disallowed names for each category. Additional categories can also be added as required for enforcing specific policies of the .ART TLD.

The rules are stored in database tables (rather than static configuration files), which means rules can be added, deleted or altered by authorised registry personnel without requiring a shutdown or restart of the .ART SRS.

Should eligible parties approach the .ART Registry (via a registrar) providing sufficient evidence of their eligibility for a specific reserved domain name, the .ART Registry can enable the chosen registrar to register the domain name for that specific registrant only (circumventing the rule engine check that would otherwise prevent the registration). Technically, this is done via the registry issuing a special authorisation code to the registrant, who supplies this authorisation code to the registrar of his choice. The registrar then needs to use this specific code as the domain authinfo in the EPP 〈domain:create〉 request, which will let the request bypass the rule engine's blocking mechanism and permit the registration.
6.2 Compliance with Specification 5 of the Registry Agreement

The rule engine is the central system component ensuring that the .ART Registry will operate the .ART TLD in full compliance with Specification 5 ("SCHEDULE OF RESERVED NAMES AT THE SECOND LEVEL IN GTLD REGISTRIES") of the Registry Agreement. Unless the .ART Registry is otherwise authorised by ICANN and the Government Advisory Committee (GAC) in writing, the rule engine for .ART will be set up to prohibit the registration of the labels and label types listed in Specification 5 by registrars.
6.3 Pattern Matching and Fuzzy String Comparison

In addition to the pre-registration checks described above, the rule engine also supports testing registered domain names against a set of configurable string patterns, as well as for their similarity to a set of disallowed strings. The former is implemented by matching names against regular expressions, the latter by calculating the so-called "Levenshtein distance" between the registered name and a given disallowed string (which is a measure for their similarity). Prior to performing any of these checks, the registered name is subjected to a number of normalisations in order to maximise its comparability; this includes the mapping of IDN characters with accents to their ASCII counterparts where feasible, the removal of hyphens and the removal of digits.

If a name matches a regular expression, or if the calculated Levenshtein distance falls below a certain threshold, the name is still normally registered, however it is also internally flagged for review. Due to the fuzzy nature of the pattern and Levenshtein matching, a name flagged via these checks may not necessarily be invalid or illegal; this is why the flagged names need to be reviewed manually by the .ART support staff. Flagged names automatically create tickets within the support team's issue system, which starts a workflow that ultimately decides whether the name is permissible (in which case the flag is removed) or invalid/illegal (in which case the name is deleted and the registrar gets notified).

6.4 Handling of IDNs

In the context of abuse prevention, the proper handling of Internationalised Domain Names (IDNs) becomes an important aspect.

If different IDN scripts were allowed to be mixed within one domain name, so-called homographs could be used to make users believe they are looking at a certain web site while it is actually a different one which name just has an identical or very similar visual representation. For example, since the Cyrillic letter "Er" ("p" in Cyrillic script) in lower case has the same visual appearance as the Latin lower case letter "p", mixing Latin and Cyrillic scripts would allow the creation of a domain name like "paypal.ART", a homograph of the Latin-only name "paypal.ART" which, despite being a different word, looks exactly the same. Such a domain name could thus e.g. be used for spoofing or phishing attacks. The .ART Registry prevents such abuse by implementing an IDN policy that disallows the mixing of scripts; within each label of a registered .ART, only characters from a single script may be used.

Likewise, the Cyrillic-only second level domain "pop.ART" looks identical to its Latin-only counterpart "pop.ART". If only the rule described above (no mixing of scripts) would apply, these two names could coexist for different registrants, and could thus be abused to confuse users. However, the special way the .ART Registry handles such IDN variants while considering respective IDN tables and canonical forms of domain names, as described in detail in the answer to Question 44 (Support for Registering IDN Domains), prevents this situation; only one of these two domains may exist at the same time.

7. Domain Data Access Control

One important point of attack that may lead to abuse of .ART domains and their associated data is the unauthorised or excessive access to data stored within the .ART repository. This applies to both read access (e.g. via public interfaces such as the port 43/web Whois) and write access (such as registrar interfaces like EPP or the web-based Control Panel). The measures taken in the .ART TLD to properly restrict access are laid out in the following.

7.1 Prevention of Whois Data Mining

The port 43/web Whois interfaces grant public access to domain, host and contact data. As such they are a potential target for data mining, i.e. the retrieval of large amounts of postal or e-mail addresses for e.g. the purpose of advertising.

As explained in detail in the answer to Question 26 (Whois), the Whois implementation provided by the CORE Registration System prevents such data mining attempts, most importantly by the following measures:

Access to all Whois interfaces is rate-limited (when accessed from IP addresses not whitelisted for unlimited access).

Web interface users are required to pass a CAPTCHA before access is granted.

Web interface users seeking access to extended Whois search capabilities are required to authenticate by entering login credentials (which are only issued to eligible parties).

For improved spam protection, E-mail addresses may be displayed as images only in the web-based Whois.

Contact disclosure flags as specified in RFC 5733, the Extensible Provisioning Protocol (EPP) Contact Mapping, are fully supported. This gives registrants enhanced control over the contact fields they want to disclose in the Whois. In this respect, the system is configurable and allows restricting the use of EPP contact disclosure settings via rules defined by specific registry policies or legal requirements.

7.2 Prevention of Unauthorised Data Modifications

Domain data within the .ART is exclusively provisioned by registrars, i.e. registrants have no direct write access to their data within the repository; all their modifications have to be done via the registrar sponsoring the respective domain. In this constellation, registrants needs to trust their registrar and will expect that the management of their domain is conducted in a diligent and correct manner.

This means that the registry's interfaces used by registrars need to be secured in order to only allow the sponsoring registrar of a domain (and nobody else) to modify domain data.

The EPP interface provided by the CORE Registration System does this by

requiring SSL⁄TLS on the transport layer,

requiring a strong EPP password (minimum length, mandatory digits and non-alphanumerical characters),

requiring changing the EPP password on a regular basis,

requiring registrars to supply lists of IP addresses or subnets from which exclusive access will be granted,

requiring registrars to use SSL client certificates known to and trusted by the registry, thus providing an additional means of authentication beyond the EPP password.

Likewise, the web-based Control Panel

requires SSL⁄TLS on the transport layer,

requires registrars to log in with a user name and password (for which the same rules regarding minimum length, mandatory digits and non-alphanumerical characters apply),

requires changing the password on a regular basis,

requires registrars to supply lists of IP addresses or subnets from which exclusive access will be granted,

requires registrars to install SSL client certificates known to and trusted by

the registry in their web browsers, thus providing an additional means of authentication beyond the web password.

8. Whois Accuracy

Since .ART is operated as a so-called ”thick registry”, the .ART Whois displays information about the registrant, as well as the administrative, technical and billing contacts of every .ART domain. In cases of malicious or abusive activity involving a .ART domain, this Whois contact information usually is the first and most important source of information, e.g. for law enforcement authorities, to determine the people or organisations responsible for the domain in a timely manner. Consequently, it is deemed very important to maximise the accuracy of contact information stored in the registry repository.

The .ART Registry (and CORE Internet Council of Registrars as its technical provider) are therefore committed to take diligent measures to promote Whois accuracy, including (but not limited to) the following:

Contact data completeness policy: The thick registry model used for .ART mandates the association of each .ART domain with exactly one registrant, one administrative contact, one technical contact and one billing contact. The data of all used contacts is stored in the registry repository. While RFC 5733, the Extensible Provisioning Protocol (EPP) Contact Mapping, merely requires contact data to contain a name, a city, a country code and an e-mail address for a syntactically complete EPP request, the .ART TLD policy for contact data mandates the specification of at least one address line (street), a voice phone number and a postal code in addition. This means that, in addition to the XML schema validation conducted by the .ART SRS for every EPP request received from the registrar (which ensures the presence of all RFC-mandated contact data), the SRS also requires these essential fields to be present and will reject requests lacking them with a ”parameter value policy error” message. The validation done by the SRS also goes beyond validating against the EPP XML Schema Definitions (XSDs) with respect to field content. For instance, contact e-mail addresses are required to contain an ’@’ character and a valid domain name; this is not mandated by the XSDs specified in RFC 5733.

Contact data monitoring: On a regular basis, the registry will run automated plausibility audits on the contact data submitted by registrars. Using publicly available databases, contact address lines will e.g. be mapped to cities and zip codes, which are then compared to the ones provided by the registrant. Likewise, phone and fax numbers will be checked for plausibility.

Domain data change notifications: The CORE Registration System used to operate the .ART TLD can be configured (on a per-registrar basis) to automatically notify certain contacts of a domain (e.g. both the registrant and the administrative contact in order to reach multiple people concerned with the domain) after every change made to the domain (i.e. alterations of associated contacts or name servers). When enabled, this feature allows unauthorised or unintended changes to domain and contact data to be detected immediately. This functionality will however need to be deployed after consultation with .ART registrars, since many registrars do not endorse direct communication between the registry and registrants, i.e. their customers.

WDRP auditing: In 2003, ICANN adopted the so-called ”Whois Data Reminder Policy” (WDRP, http://www.icann.org/en/registrars/wdrp.htm) which obliges ICANN-accredited registrars to send yearly Whois data reminder notices to registrants. These notices contain the Whois data currently on file for the respective domain, as well as

instructions for the registrant about ways to correct the data if required. While the .ART Registry does not intend to replicate this reminder procedure on the registry level, it will establish an auditing process that monitors the WDRP activities of .ART registrars to make sure that WDRP responsibilities are honoured.

9. Resourcing Plans

The CORE Registration System already supports the technical abuse prevention and mitigation measures above at the time of writing. No additional coding is required for this, which means that no special developing resources will be needed. Continuous audits and monitoring, as well as timely reactions to reports of malicious activity will be provided by the staff on duty at CORE Internet Council of Registrars.

For the initial setup, the following resources are allotted:

Registry Policy Officer: finalising policies, creating documentation: 7 man days

System Administrator: monitoring setup: 3 man days

First Level Support: training: 1 man day per person

Second Level Support: training: 1 man day per person

For the ongoing maintenance, the following resources are allotted:

First Level Support: 10 man hours per month

Second Level Support: 20 man hours per month

System Administrator: 3 man hours per month

Employees already working for CORE Internet Council of Registrars will be handling these tasks. The numbers above were determined by averaging the effort required for comparable tasks conducted by CORE in the past over the course of 12 months.

29. Rights Protection Mechanisms

Q29 - Rights Protection Mechanisms

Whenever a new TLD is introduced, the protection of intellectual property, legal rights and trademarks (TMs) is an important objective. Using suitable technical means and appropriate policies and procedures, rights owners and trademark (TM) holders must be protected from abusive domain registrations throughout a TLD's launch phase(s), as well as during the period of general availability (GA) which follows theselaunch phase(s).

The .ART Registry(and CORE as its technical provider) are committed to make all necessary technical and organisational provisions in order to achieve this objective. This includes, but is not limited to, full compliance with all respective specifications, agreements and ICANN policies. Details about the measures put in place are laid out in the following.

1. Sunrise Period

A proven way to allow eligible rights owners to secure domain names related to their registered TMs is to conduct one or more so-called ”Sunrise” phases prior to the TLD’s GA launch. During Sunrise, domain names are awarded only to registrants supplying appropriate and valid data manifesting their ownership of a TM that matches the desired name.

Technically, Sunrise phases differ from the GA period in some important aspects:

* In addition to the usual domain data, registrars need to collect TM information (such as TM name, number, type, application⁄registration dates) from the registrants and submit this data to the registry when applying for domain names.

* The specified TM information needs to be validated. This involves verifying the data with the help of a so-called ”Trademark Clearinghouse” (TCH), a central repository authenticating, storing and disseminating TM information (providers for this service are to be designated by ICANN). In addition, manual reviews may be part of the validation process, for which appropriate tools should be in place.

* The results of the TM validation need to be received and properly processed. This includes notifying all involved parties (such as the registrar and registrant).

* It is possible that multiple applications for the same domain name are received. To distinguish these applications, a unique ”application ID” is assigned to each of them. If more than one of the applications for a domain name carry valid TM data, contention resolution measures need to be taken in order to determine the registrant to whom the domain is awarded.

The CORE Registration System used by CORE to operate the .ART TLD fully supports these and other requirements of Sunrise phases via features described in the following.

1.1 Sunrise EPP Extension Support

The system supports an EPP extension for submission of TM data along with domain applications during launch phases such as Sunrise. For multi-phase Sunrise periods, the extension also supports the specification of the phase for which an application is submitted.

Moreover, the extension offers the possibility to submit additional textual information along with an application, such as e.g. the intended use for the domain name, or a URL demonstrating the previous use of the domain name under other TLDs. The registry’s Sunrise policy governs whether specifying this information is required, which kind of data this information needs to provide, and how this information affects the decision about whether or not a domain name is awarded.

Please refer to the answer to Question 25 for more information about the launch phase EPP extension.

1.2 Sunrise Whois Support

CORE provides special Whois services during launch phases like Sunrise. This allows

registrants to check the status of their applications independently from information they may obtain from their registrars.

However, the Whois search options and the information returned during Sunrise differs from GA (as described in the answer to Question 26). Only the search for application IDs is enabled, without any support for wildcards. If an application ID exactly matches the Whois client's query string, the application's data (domain name, registrar, application date, contact data and TM information) is returned, along with information about the application's status (such as "approved" or "under review"). See the Sunrise/Landrush life cycle specification below for details about possible application states.

1.3 Registration Life Cycle Support for Sunrise (and Other Launch Phases)

The system supports the special steps of the registration life cycle that occur during Sunrise, i.e. the initial asynchronous TM validation and/or selection processes.

The registration life cycle described in the answer to Question 27 applies to the GA phase of the .ART TLD, i.e. the normal "First-Come, First-Served" (FCFS) period that usually starts after a TLD has finished its initial launch phase(s). Launch phases like Sunrise and Landrush usually involve a special life cycle that adds some complexity to the initial domain creation step.

During Sunrise phases, this step comprises the validation of TM data and the determination of the winning application if multiple ones were received. Depending on the concrete registry policy in place, one or multiple Sunrise phases may be conducted.

So-called "Landrush" phases are usually conducted after (or in parallel to) Sunrise phases in order to limit the load on the Shared Registration System (SRS) that usually occurs during the initial run on popular, generic names. Their goal is to replace the brute-force FCFS approach of the GA by a fair, controlled domain assignment process that does not encourage registrars to flood the SRS with requests when GA starts. Similar to Sunrise, most Landrush approaches let registrars submit multiple applications for the same domain name, among which a winner is determined by asynchronous contention resolution measures as defined by the registry's policies. In contrast to Sunrise, usually no special proof of eligibility needs to be supplied by registrars or validated by the registry during Landrush.

1.3.1 Life Cycle Support for Sunrise

During both Sunrise and Landrush, the first step of the normal domain life cycle ("create domain", position (A) in the GA life cycle diagram
Q27-F1 from the answer to Question 27) consists itself of a number of individual steps representing the registry's rights protection workflow.
The steps during Sunrise are depicted in Figure Q29-F1:

(A1) Registrars are required to submit Sunrise applications for domain names by sending EPP <domain:create> commands containing a special EPP extension for the specification of relevant TM data. In addition, a second EPP extension may be used to specify data required to resolve a potential contention with regard to the domain name (e.g. the registrant's bid for the case that an auction should be held to decide the final assignment of the domain name).

Application data is stored in the registry database. Checking this data for validity may involve manual evaluation that needs to be done

asynchronously. Also, multiple valid applications for the same domain name may be submitted during Sunrise, which is why applications are collected until the end of the Sunrise submission period, after which evaluations (and, if required, contention resolution) take place to determine the final outcome. The final result of the application is later communicated to the registrar via an EPP poll message.

(A2) The registry system accesses the API of the connected TCH in an attempt to validate the submitted TM information in relation to the desired domain name.

(A3) If the check with the TCH fails, i.e. the provided TM information is found to be evidently invalid, the application is rejected immediately without further manual review. An EPP poll message is placed in the registrar's message queue to inform the registrar about the negative outcome of the application. The application's status is now "invalid", which is also displayed in the special launch phase Whois output when the application ID is queried.

This step in the life cycle may also be reached later in the validation process, i.e. after the application was found invalid during a manual review, or when a contention resolution for a name with multiple valid applications was lost by the registrant. In the latter case, the application's status is "rejected".

(A4) If the check with the TCH succeeds, i.e. the provided TM information is found to be (at least tentatively) valid, the application is added to the pool of automatically validated applications for the given name. The application's status is now "pending". Such applications are collected in the registry database until the end of the Sunrise submission period. The registrar may withdraw the application by sending an EPP <domain:delete> before the Sunrise submission period ends.

(A5) At the end of the Sunrise submission period, the application may be further evaluated, potentially involving manual checks. If the outcome of this evaluation is that the application is invalid, the application is rejected by going to step (A3).

(A6) All remaining, valid applications for the given name are examined. If there is only one valid application (left) for the given name, this application may be approved in step (A7). Otherwise, a contention resolution needs to be conducted to determine the final assignee for the application, which is done in step (A8).

(A7) The application is approved, the domain is allocated and assigned to the registrar. An EPP poll message is placed in the registrar's message queue to inform the registrar about the positive outcome of the application. The domain proceeds into the registered state. The application's status is now "allocated".

(A8) Since multiple valid applications for the same name were submitted, a contention resolution is required to determine the registrant to which the domain is awarded (the actual contention resolution used for .ART is described below). If the resolution is won, the next step is (A7); if it is lost, the next step is (A3). During the contention resolution, the application's status is "validated".

1.3.2 Life Cycle Support for Landrush

The steps during a Landrush phase are quite similar to the ones for Sunrise. As depicted in Figure Q29-F2, the basic approach is the same, except that no TM information is submitted or reviewed in the process; the only aspects governing the assignment of the domain name during Landrush are

* whether more than one application was received for the name and

* if this should be the case, which of these applications wins the contention resolution.

The availability of Landrush support in the CORE Registration System does not imply that dedicated Landrush phases must be held. While they are technically feasible, registry policy may also dictate that Sunrise and Landrush are conducted in a single phase, or in overlapping phases. The CORE Registration System is prepared for such cases. A combined Sunrise⁄Landrush phase is e.g. possible by allowing applications during Sunrise to be submitted without carrying any TM data (which marks them as Landrush applications). During the selection process, applications carrying TM data (i.e. proper Sunrise applications) then always take precedence over ones that were submitted without such data; only if no valid Sunrise applications are received for a name, the Landrush applications for the name are considered, and the winning one is determined in accordance with the registry's contention resolution policies.

Another alternative to a dedicated Landrush phase is the use of a FCFS approach for GA with staggered pricing; in this approach, a domain's initial registration price is relatively high when GA starts, but is decreased over time. Registrants willing to pay the high price may register the domain early on, others will try waiting until the price goes down. Despite the FCFS principle, such staggered pricing will usually prevent a flood of requests from registrars at the beginning of GA. The CORE Registration System supports this approach by its flexible billing module, which allows the definition of specific prices for certain time periods, e.g. the first day after the start of GA, the second day and so forth.

The billing module, in conjunction with the rule engine described in the answer to Question 28, may also be used to charge individual, higher prices for attractive, generic names ("premium" domains).

See below for more information on the GA approach designated for .ART.

1.4 Trademark Clearinghouse (TCH) Support

The CORE Registration System is prepared for accessing APIs of the TCH in order to validate the TM information submitted by the registrar during Sunrise. In addition, the system also contains provisions to make use of the TCH APIs for providing a Trademark Claims Service as soon as .ART enters a period of general availability (see below for more information on this service).

Since TCH Service Providers have not been assigned by ICANN at the time of writing, the full technical specifications for these APIs are not yet known. While basic provisions have been made in the CORE Registration System to connect to these providers, the details will therefore have to be finalised once the service providers have been announced and API specifications are available. As described below, appropriate developer resources are allocated to perform this task.

1.5 Support for Multiple Applications for the Same Domain Name

The CORE Registration System is designed to maintain multiple domain objects representing the same domain name at a given point in time. This feature is required to store multiple applications for the same name during launch phases like Sunrise.

To distinguish between the various applications for the name in the database (as well as in external APIs), each application is assigned a unique application ID. These application IDs are returned to registrars in the responses to domain

applications via EPP and may subsequently be used, among other things, to enquire an application's review status. Also, review results are reported back to registrars via poll messages carrying the unique application ID. Registrars can utilise the ID to clearly associate results with their various applications. Registrants may query the status of their applications from the .ART Whois server using the ID.

1.6 Issue System

When manual reviews of Sunrise applications are required, this typically involves a specific support team workflow that, among other things, consists of

* storing application data in a database,
* making application data available to the support staff via a web interface,
* assigning the task of reviewing applications for a certain domain name to a specific support member (for the purpose of clear responsibilities),
* having the application reviewed by the assigned person, who in the process may

o request additional information or documentation from the registrant,

o add such documentation, as well as comments concerning the review, to the application,

o make a decision about the application's outcome or

o forward the task to a different support person with better insight or higher decision privileges (who may then make the final decision).

To support this workflow, the CORE Registration System is equipped with a built-in Issue System that offers registry personnel a convenient web interface to review domain name applications and approve or reject them accordingly.

The Issue System

* offers an SSL-secured web interface accessible by .ART registry staff only;

* allows searching for applications by various criteria (e.g. domain name or current workflow⁄approval state);

* allows a registry support person to find newly submitted or otherwise unassigned applications and to take responsibility for them;

* offers a two-level review workflow that allows the delegation of pre-selection tasks to the first level support staff, after which a final decision - if still required - can be made by second level personnel;

* conveniently displays all application details, including registrant information, the supplied TM information, as well as the results of the verification of that TM data with the TCH;

* fully tracks and documents application status and history, allowing for a complete audit in case of disputes or legal enquiries and

* is fully integrated with the registry backend, i.e. it automatically notifies the SRS about the reviewers' decisions and immediately activates the respective domain in case of an approval. The Issue System also triggers the creation of appropriate EPP poll messages in order to keep registrars informed about the outcome of their applications.

The Issue System was first employed using puntCAT's elaborate multi-phase Sunrise period in 2006 and proved to be an invaluable tool for efficiently organising a TLD roll-out process. It ensures that the registry staff reviewing Sunrise applications finds all information relevant to a domain name in one place and comes to well-founded decisions in a timely manner. The experience gathered from developing and operating the Issue System in that context helped to develop a second-generation version that is now part of the CORE Registration System.

1.7 Support for Resolving Contention

If multiple valid and eligible applications for a domain name are received, a well-defined and deterministic process is required to nominate the winning application. The details of this contention resolution procedure highly depend on a specific TLD's policies. However, even after such policy-based considerations, multiple candidates for the winner of an application may be left in contention. In such a situation, different tie-breaker rules can be applied to make a decision.

1.7.1 First-Come, First-Served (FCFS)

The obvious tie-breaker rule is to simply award the domain to the first application submitted, i.e. the one that carries the earliest time stamp among the ones in the contention set. Since the CORE Registration System assigns a unique time stamp to each received application in a fair, unbiased manner and makes it available to the review staff of the .ART Registry, this FCFS strategy is a viable, technically supported way to resolve contentions.

1.7.2 Auctions

However, FCFS selection processes based on application submission times have the drawback of potentially encouraging registrants and registrars to submit all their requests as soon as the registry starts accepting applications, which imposes time pressure on the involved parties, puts a considerable load on the involved systems and may cause an unfair advantage for registrars with better connectivity to the SRS.

Therefore, the CORE Registration System also supports a simple auction-based tie-breaker approach out-of-the-box. It allows the registrar to submit a single, blind bid amount along with the Sunrise or Landrush application (via a special EPP extension). In the case of a contention, the application that was submitted with the highest bid wins. In the unlikely event that two applications were submitted with the exact same bid amount, the one with the earlier time stamp wins. Only the winning applicant pays his bid, i.e. there is no extra fee for placing a bid; this ensures that the process cannot be regarded as a lottery. If no contention should arise (i.e. there is only one applicant left before bids would be considered as a tie-breaker), the bid amount is irrelevant and only the standard application fee is paid.

2. Compliance with Specification 7 of the gTLD Applicant Guidebook

The .ART Registry will fully comply with the rules defined in Specification 7 of ICANN's gTLD Applicant Guidebook ("Minimum Requirements for Rights Protection Mechanisms"). The details of this compliance is outlined in the following.

2.1 Implementation of All Mandated Rights Protection Mechanisms

In particular, this means that the .ART Registry will include all ICANN mandated and

independently developed Rights Protection Mechanisms (as described here) in the registry-registrar agreement (RRA) to be signed by all registrars authorised to register names in the .ART TLD. The .ART Registry will also, in accordance with requirements established by ICANN, implement each of the mandatory Rights Protection Mechanisms set forth in the ICANN-designated TCH.

During the conducted Sunrise phase, which will at least be offered for 30 days prior to entering a GA period, the .ART Registry will consult the ICANN-designated TCH in order to verify TM data submitted by registrants. Details about this process are depicted above.

2.2 Trademark Claims Service

For further compliance with Specification 7, the .ART Registry will implement a continuous Trademark Claims Service (TCS) to ensure that even after Sunrise, registrants are notified whenever their registered domain name potentially violates a TM holder's rights as stored in the TCH. Likewise, the service makes the TM holder aware of any domain registrations that potentially infringe on his TMs registered with the TCH.

As required by ICANN, the TCS of .ART will at least cover the first 60 days of GA; it is considered that the TCS will be provided indefinitely, i.e. on a continuous basis beyond the first 60 days of GA.

When a match of a registered name is found via the API provided by the TCH, the TCS is supposed to provide clear notice to a prospective registrant of the scope of the mark holder's rights. The registrant will in turn be required to provide statement that

* he received notification that the mark is included in the TCH,

* he received and understood the notice and

* his registration and use of the requested domain name will not infringe on the rights that are subject of the notice.

The registrant will be directed to the TCH Database information referenced in the Trademark Claims Notice to enhance understanding of the TM rights being claimed by the TM holder.

Also, if a domain name is registered in the TCH, the registry will, through an interface with the TCH, promptly notify the mark holders(s) of the registration after it becomes effective.

2.3 Prevention of Otherwise Unqualified Registrations

In addition to protecting the rights of TM holders as described above, the .ART Registry will also ensure that no registrations will be allowed which are in violation of the registry,Äôs eligibility restrictions or policies. Technically, this is achieved by utilising the advanced domain name rule engine that is part of the CORE Registration System and described in detail in the answer to Question 28. As laid out there, the underlying set of checks can be tuned to block registrations of .ART names based on various syntactic rules, multiple reserved names lists, and patterns. Prior to the launch of the .ART TLD, the rule engine will be configured in accordance with the policies of the .ART Registry. Reserved names lists will be populated as governed by all eligibility restrictions that need to be enforced, which means that such names are not available for registration by registrars.

However, should eligible parties approach the .ART Registry (via a registrar) providing sufficient evidence of their eligibility for a specific reserved domain name, the .ART Registry can enable the chosen registrar to register the domain name for that specific registrant only (circumventing the rule engine check that would otherwise prevent the registration).

2.4 Reducing Opportunities for Phishing and Pharming

The abusive behaviours of phishing and pharming constitute a severe violation of the legal rights of others. Both practices are usually applied to make users enter confidential information on fake web sites pretending to be operated by a certain company or institution. In the case of phishing, the attack is usually done by trying to conceal the real domain name in the URL, or by using a domain name very similar to the one the user originally meant to visit. In the case of pharming, the attack happens on the DNS level, i.e. while the user still sees the correct domain name of the site he meant to visit, the IP address his resolver determined for the domain name somehow gets manipulated to point to the fake web site.

Due to the way these attacks are conducted, neither phishing nor pharming can be entirely prevented on the registry level. However, the registry can put mechanisms and policies in place that will make such exploits harder or limit their duration and impact.

2.4.1 Phishing

One important tool to rapidly address phishing activities shown by a web site operated under the .ART TLD is the Rapid Takedown Policy described in the answer to Question 28. It allows a fast takedown of an offending site after respective activities were reported and confirmed.

In addition, the flexible rule engine used by the CORE Registration System to validate permissible .ART domain names can be utilised in the context of phishing. Should a certain .ART domain name (or a pattern of such names) be repeatedly involved in attempts to mimic a rights holder's legitimate .ART name for phishing purposes, the set of registration validation rules can be easily augmented to prevent the offending domain name (and, if need be, even an entire pattern of names deemed too similar to a rights holder's legitimate domain name) from being registered again after takedown. Of course, this practice will be exercised in close collaboration with ICANN and other parties potentially involved in the definition of names deemed not eligible for registration within the .ART TLD.

As described in the answer to Question 28, the sophisticated IDN handling implemented by the CORE Registration Systemis designed to provide protection against the most common cases of IDN-based phishing attempts, such as IDN homograph attacks. Please refer to the answers to Question 28, as well as Question 44, for more information on this topic.

2.4.2 Pharming

With regard to pharming, neither the quick takedown of offending domain names nor the blocking of such names are suitable as countermeasures. Due to the nature of the attack, the registry's approach needs to aim at a robust DNS infrastructure for .ART, which ideally should guarantee the integrity and authenticity of DNS lookup results all the way from the registry-operated TLD name servers to the user's local resolver.

As described in detail in the answer to Question 35, the .ART Registry will deploy a

highly reliable and secure DNS subsystem for the .ART TLD, which is powered by the elaborate DNSSEC setup laid out in the answer to Question 43. The .ART Registry is therefore able to safeguard against any attempts to perform DNS manipulation on the level of the name servers operating the .ART zone.

However, due to the way the domain name system (and DNSSEC in particular) works, preventing manipulations of the .ART TLD name servers
alone is not sufficient to avoid pharming attacks. In order to provide complete protection, DNSSEC support is required on every level of the domain resolution process, from the root zone via the TLD name servers and the delegated name servers down to a user's resolver. This means that registrars need to sign the zones they host on their name servers (and offer this service to their registrants), and resolvers (or other clients looking up .ART domain names) need to verify the signatures and notify their users when inconsistencies are detected. Consequently, the .ART Registry will encourage and advertise the widespread support and use of DNSSEC among registrars, registrants and end users. Once DNSSEC has been widely adopted, web browsers, e-mail clients and similar applications will increasingly support the verification of the related signatures out-of-the-box (rather than via the extensions available today), which will drastically diminish opportunities for pharming.

2.5 Compliance with Dispute Resolution and Suspension Procedures

In case of complaints put forward by rights holders with regard to domain names registered under .ART, the .ART Registry will fully comply with all resolution procedures endorsed or mandated by ICANN. In particular, this includes supporting the Uniform Rapid Suspension (URS) procedures and the Trademark Post-Delegation Dispute Resolution Procedure (Trademark PDDRP). Since .artis a community-based gTLD, thisalso includes the Registry Restrictions Dispute Resolution Procedure (RRDRP).

The .ART Registry is committed to implement decisions rendered under the URS. In particular, the .ART Registry will

* readily receive notifications about complaints (Notice of Complaint) from URS providers,

* lock the affected domain within 24 hours of receipt of the Notice of Complaint from the URS Provider, blocking all changes to the registration data, including transfer and deletion of the domain name (while retaining the domain name in the .ART zone, i.e. the name will continue to resolve),

* notify the URS Provider immediately upon locking the domain name (Notice of Lock).

Once the complaint was decided upon, the following steps will be taken:

* If registrant was relieved, the .ART Registry will unlock the domain and return full control to the registrant.

* In case of a determination in favour of the complainant, the .ART Registry will, in accordance with the URS rulings, immediately suspend the domain name and keep it suspended for the remainder of its registration period; this means that the domain will remain locked and that the domain's name servers are redirected to an information web page supplied by the URS provider. In this situation, .ART Registry will also make sure that the Whois output

for the domain keeps displaying the original data (except for the altered name servers) and reflects that the domain name will not be able to be transferred, deleted or modified for the remainder of its registration period.

* The successful complainant will get the option to extend the registration period for one additional year at commercial rates.

In addition to these URS related procedures, the .ART Registry is also committed to take any necessary steps required to support decisions emerging from the Uniform Domain Name Dispute Resolution Policy (UDRP). After a respective complaint has been filed in a court of proper jurisdiction or with an approved dispute resolution service provider, the .ART Registry will implement all required measures arising from its function as a registry, including an immediate transfer of the domain to the legitimate rights holder (if the case's determination is in the complainant's favour).

In case the .ART Registry becomes involved in a Trademark Post-Delegation Dispute Resolution Procedure (Trademark PDDRP), it will fully adhere to the general rules of the procedure as set out by ICANN, as well as the individual requirements defined by the Trademark PDDRP Provider. However, it should be noted that the .ART Registry has taken (and will continue to take) thorough precautions to ensure that a Trademark PDDRP will not become necessary. Nevertheless, should it become necessary, the .ART Registry will abide by the remedies recommended by the Expert Panel, and potential fees imposed.

Since .artis a community-based gTLD, the .ART Registryalso agrees to participate in the Registry Restrictions Dispute Resolution Procedure (RRDRP) and to comply with any determinations resulting from that procedure. This includes, but is not limited to, filing a compliant response to each complaint within 30 days after receiving it from the RRDRP provider, attending hearings related to the complaint, adhering to the recommendations of the Expert Panel upon determination, and abiding with imposed fees.

3. Sunrise and Landrush Policies for the .ART TLD

Please see description of .ART Launch phases in response to Question 18.3.3 above

4. Resourcing Plans

The CORE Registration System already supports the rights protection features described above at the time of writing. No coding is required for this, which means that no special developing resources will be needed. The staff on duty at CORE will be in charge of performing manual reviews of TM data where required.

Since the TCH API is not fully defined at the time of writing, some software development will have to be done in order to integrate it into the Sunrise workflow and the TCS.

For the initial setup, the following resources are allotted:

* Registry Policy Officer: finalising policies, creating documentation: 5 man days

* System Administrator: configuring system for policies: 1 man day

* First Level Support: training: 4 man hours per person

* Software Developer: integration of TCH API: 10 man days

For the Sunrise phase, the following resources are allotted:

* First Level Support: 30 man days per month

* Second Level Support: 30 man days per month

For the ongoing maintenance, the following resources are allotted:

* System Administrator: 1 man day per month

Employees already working for CORE Internet Council of Registrars will be handling these tasks. The numbers above were determined by averaging the effort required for comparable tasks conducted by COREin the past over the course of 12 months.

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

Q30 a) - External Technical & Operational Capability

This chapter presents an abstract, high-level description of the security principles governing the operation of the .ART TLD by the .ART Registry. Since this part of the response is published, detailed information is not included in this part of the answer, however an exhaustive description of the employed security measures is presented in the answer to Question 30 b).

Knipp Medien und Kommunikation GmbH, the technical provider for CORE Internet Council of Registrars, is currently in the process of being certified according to the ISO 27001 standard. The completion of the certification process is estimated for Q4⁄2012.

1. Security Policy

As .ART Registry does not perform the technical operation of the registry itself, but has contracted CORE Internet Council of Registrars for that purpose, .ART Registry defines a general security policy framework that is imposed on itself, CORE and all further contractors and subcontractors. All participating entities have to ensure that their security policies meet the requirements of the framework.

The security policy framework has the following key objectives:

* confidentiality
* access
* accountability
* availability

These objectives are further explained in the following.

1.1 Confidentiality

Confidentiality means the protection of private, proprietary and other sensitive information from entities that neither have a right or a need to gain access to it. Information includes, but is not limited to, registration data, registrar data, financial data, contracts, human resources data, and other business and technical data. To achieve this, all managed data are categorised into the classes ”highly sensitive”, ”confidential” and ”public”, which then define the base levels for the respective protective measures. With respect to the determined classification, for each set of data it is defined

* where the data is stored,
* how it is backed up,
* what protective measures are taken both for the data itself and its backups,
* how long the data is retained and how it is safely destroyed once the information is no longer required,
* how it is protected from illicit access,
* how legitimate access and modification is controlled,
* to which extent the data has to be auditable and
* which regular audits are performed.

1.2 Access

Access defines the rights, privileges and the mechanisms by which assets of the .ART Registry are being protected. Assets may refer to physical items like desktop computers, notebooks, servers, network devices and other equipment, or to logical items like registration data, e-mails and communication logs, passwords or cryptographic key material. For each entity (i.e., person or machine) that is granted access, it is clearly defined

* for which purpose the access is granted,
* to which level the entity can view or change the data, partially or in whole,
* which obligations are imposed on the holder of the access rights,
* at which frequency the grant is revisited, i.e. checked whether it is still required to uphold the grant.

1.3 Accountability

Accountability defines the responsibilities of staff members and management with respect to security aspects. This includes

* handling of passwords and security tokens,
* reviewing audit logs and identifying potential security violations,
* management of security and access control and
* reporting of potential security breaches.

Staff members are made aware of their responsibilities on the assignment of duties and on a regular basis.

1.4 Availability

For each facet of the registry operation, beyond the requirements of ICANN, it is determined which service level is required, i.e.

* the availability requirements, defining the desired relative availability over a period of time (typically one month), including the allowed maximum planned and

unplanned outage times,
* the recovery time objective and
* the recovery point objective, if applicable.

1.5 Security Role Concept

For the .ART Registry, the considerations above manifest themselves in an exhaustive security role concept, which defines roles carrying certain access privileges and responsibilities. Employees at the .ART Registry are assigned one or multiple roles identified by this concept, which clearly defines their duties and access rights.

2. Security Commitments to Users of the .ART TLD

2.1 Abuse Prevention and Mitigation

As discussed in detail in the answer to Question 28, the registry has taken various precautions to reduce the probability that the domain names within .ART are being used in connection with abusive or criminal activities.

2.2 Reliability and Availability of DNS

Various technical measures ensure a 100% availability of the DNS, as well as reliable, accurate and fast responses. A highly protected DNSSEC infrastructure ensures that the digital signatures contained in the DNS are trustworthy.

2.3 Technical Progress

The .ART Registry is committed to employ state-of-the-art security measures on an ongoing basis. This includes, for example, the use of current and secure software, fast patches of security affecting bugs, and the adoption of new security related technologies as they become available.

3. Security Commitments to Registrants

3.1 Protection of Investment

With the commercialisation of the Internet, domain names have become valuable assets. Domain names are no longer simply a more or less convenient handle for cryptic IP addresses, but as brands they have become the base for whole businesses worth millions to billions. Also, with domain names, lifestyles (”twitter”, ”facebook” generations) and communities are associated. Therefore, the loss, abuse or unavailability of a domain name, be it temporary or permanently, may cause significant damage to the domain name registrant.

The .ART Registry fully recognises this. With its highly developed technical and administrative security framework, .ART Registry has taken the necessary measures to protect the investments of registrants in their names. Due to the domain auto-renew mechanism, a valid domain is never deleted by the registry itself. In addition, the Redemption Grace Period provides extra protection if a request to delete the domain is inadvertently issued by the registrant himself or by the entrusted registrar.

Also, if it can be proven that a domain has been illegally moved to a different registrant, this is reverted by the registry to original state.

3.2 Adherence to Registration Policy

The registration policy clearly defines the conditions by which potential registrants may register domain names. The registrants can rest assured that the registry strictly adheres to these rules. In detail,

* The registry guarantees equal opportunity if multiple registrants meet the registration conditions in the same way.
* The registry applies a clear procedure for handling violations of the registration policy. The registrant has the ability to correct the violations before further actions are taken by the registry; he has also the right to appeal if he believes that the grounds for the registry's decisions are invalid.
* The registry maintains its neutrality in conflicts, unless forced by ICANN's Uniform Dispute Resolution Policy (UDRP), Uniform Rapid Suspension (URS) and Registry Restrictions Dispute Resolution Procedure (RRDRP).

3.3 Privacy of Registrant Data

While the registry is strongly committed to data protection and privacy, only limited commitments can be made with respect to registrant data. This is owed to various requirements imposed by ICANN for the right to operate the registry.

First, the registry is required to provide so-called Registration Data Directory Services (RDDS). On the one hand, this allows the anonymous public to retrieve information on the registrant of a domain name. The registry tries to mitigate the impact by taking measures against data mining and by fully supporting EPP's disclosure settings, which allow the registrant (via the registrar) to restrict the exposure of specific data fields (within the limits of ICANN requirements).

On the other hand, as part of the RDDS, the registry is also required to grant access to the data to eligible users and institutions with legitimate interest, not limited to law enforcement agencies. The registry will monitor the activities of these entities and will withdraw the access if there are indications of excessive or abusive use.

Second, the registry has to give access to the registrant data to ICANN as part of the escrow requirement. While the data is encrypted by a public key of ICANN and thus safe from access by third parties, no guarantees can be given about the data handling by ICANN.

The registry adds a declaration about the data handling to the registration agreement in order to make a potential registrant aware of the limited privacy.

Annex B

7095 HOLLYWOOD BLVD #788
HOLLYWOOD, CA 90028

P 323.645.6000
F 323.645.6001

April 11, 2012

RE: Endorsement of the ".ART" gTLD application by Dadotart, Inc.

To the Members of the Board of Directors of ICANN

DeviantART, Inc. writes to express its unconditional endorsement and support to the Dadotart, Inc. application to own and operate the .ART gTLD. We believe that the .ART gTLD, as conceived and proposed by Dadotart, fully aligns with the interests of the economic, philanthropic, and educational needs of the world community dedicated to the Arts.

We have learned through the work of deviantART.com in aggregating over 20 million registered members dedicated to the making or appreciation of art that the Internet is an invaluable resource for communication, learning, and commerce related to the arts. The primary mission and purpose of the .ART gTLD is to provide a trusted, hierarchical, and intuitive online marketplace for Internet users seeking to share works of art or to exchange ideas about art and to access resources for the arts and about the arts. Under the Dadotart stewardship, the .ART gTLD will be reserved for the use of members of the artistic community and will give them a much needed identity of their own within the culture that is the Internet.

We strongly believe that the .ART gTLD will be best represented through the oversight of Dadotart which can provide leadership for the all of the thousands of art-related organizations, associations and institutions as well as the millions who function as artists. The .ART gTLD can become a beacon of culture and assurance of quality and relevance to Internet users worldwide and expand the relevancy into the arts of new technologies for distribution and production.

With our large registered membership, over 60 million monthly unique visitors and nearly 200 million works of art from our members, deviantART is not just the largest arts-related aggregation on the Internet but also the largest aggregation in history of people with a love and attraction to the arts. Members and visitors to deviantART come from all over the world. Only 39% of our traffic is from the United States. We understand the connection of technology to the arts. And, we urge you to support the application of Dadotart in order to continue the advance of the arts to new levels of relevancy in world culture.

Thank you for accepting this letter of endorsement and support for the Dadotart, Inc. gTLD application for the .ART gTLD.

Best Regards,

Angelo Sotira
Co-Founder and CEO
DeviantART, Inc.