February 8, 2013

Mr. Fadi Chehadé
President and CEO
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA

Dear Fadi and Akram,

On behalf of the members of the Registries Stakeholder Group (RySG) and the New TLD Applicant Group (NTAG), I respectfully submit this letter to you for your review, consideration and action. This letter is the result of several weeks of detailed discussion and deliberation around key technical and/or operational implementation details that have yet to be finalized and/or require refinement, and will have a significant impact on the introduction of new gTLDs. The RySG and NTAG look forward to working with ICANN to resolve these issues.

The Registry Stakeholder Group (RySG) has been discussing a number of technical issues outlined in the Draft New gTLD Registry Agreement (draft RA) and the Applicant Guidebook (AGB) from an implementation perspective. This process has identified concerns with some of the technical requirements specified in the draft RA and the AGB. The purpose of this correspondence is to bring these concerns to your attention and to seek your consideration of some proposed modifications to the draft RA and AGB, which would alleviate the concerns of the RySG.

It is our view that the proposed modifications only relate to technical implementation and are not related to policy discussions. Nor will these proposals compromise the quality of service provided by registries. However, we acknowledge that if the modifications as proposed are accepted, changes will be required to the draft RA.

There are seven issues we wish to raise that fall under the following categories:

- Data Escrow;
    - Deposits,
    - Format, and
    - Criteria for escrow contract and provider;
- Zone File Access Format;
- IDN Tables;
- ICANN reporting;
- Pre-delegation Test Elements – DNS Infrastructure;

Each issue will be addressed separately, identifying the issue/concern and proposing modifications for consideration and discussion.

Pre-Delegation Testing Timing

ICANN's October 2012 '*Use of a Drawing for Prioritizing New gTLD Applications'* proposal calls for the conclusion of Pre-delegation testing prior to the execution of the Registry Agreement. This is inconsistent with the Transition to Delegation phase documented in Module 5 of the Applicant Guidebook, which indicates that Pre-delegation testing will occur following execution of the Registry Agreement.

RySG Recommendation

The RySG seek clarification on the timing of the specific Pre-delegation testing requirements taking into account the complexities that arise owing to the absence of an executed Registry Agreement during Pre-delegation testing.

RATIONALE:

The absence of an executed Registry Agreement during Pre-delegation testing presents additional complexities for both ICANN and applicants. The origin of these complexities essentially relates to the fact that it is now an *applicant,* and **not** a Registry Operator, that is required to undergo Pre-delegation testing.

The Pre-delegation testing requirement as specified in Module 5 of the Applicant Guidebook to provide an executed agreement between the selected escrow agent and the applicant inequitably requires applicants to enter into an agreement with a third party without the certainty of having executed a Registry Agreement with ICANN. Delaying the fulfilment of this requirement to a point in time after the execution of the Registry Agreement provides for a more equitable solution.

The absence of an executed Registry Agreement during Pre-delegation testing renders section 4.3(b) of the Registry Agreement (Termination) irrelevant. ICANN essentially loses the operational advantage to insist that Pre-delegation testing is completed within 12 months which may compromise the desire to ensure that all new gTLDs are operational. This issue also raises the wider question of what contractual nexus ICANN believe exists between an applicant and ICANN during this interim Pre-delegation testing period.

Data Escrow Deposits

Specification 2, Data Escrow Requirements, of the draft RA, Part A – Technical Specifications stipulates that the Registry Operator must submit Full and Differential Deposits, whereby:

a. Full Deposit will consist of data that reflects the state of the registry as of 00:00:00 UTC on Each Sunday.
b. Differential Deposit means data that reflects all transactions that were not reflected in the last previous Full or Differential Deposit, as the case may be. Each Differential Deposit will contain all database transactions since the previous Deposit was completed as of 00:00:00 UTC of each day, but Sunday. Differential Deposits must include complete Escrow Records as specified below that were not included or changed since the most recent full or Differential Deposit (i.e., newly added or modified domain names).

RySG Recommendation

The RySG is seeking to have this requirement changed to a Full Deposit every Sunday and either a Full or Differential Deposit every day except Sunday.

RATIONALE:

We believe the current requirement is founded on the assumption that that there will be a large number of Domains Under Management (DUMs) in each registry, presumably in the order of many millions. Where this is the case, we agree that Differential Deposits prove to be a viable option. However, for smaller registries that have a lower number of DUMs we believe that submitting Full Deposits each day is more practicable.

Allowing registry operators to provide Full or Differential Deposits every day except Sunday enables those with a lower number of DUMs to submit Full Deposits leading up to the point where doing so is not optimal due to the increase in the number of DUMs. At this point, the Registry Operator can develop the technology required to generate Differential rather than Full Deposits on a daily basis and Full Deposits on Sunday.

In cases where the number of DUMs is small enough to make daily full deposits practical, the main benefits to our proposal are as follows:

1. If the escrowed data is ever needed for the purposes of re-establishing a registry through an Emergency Backend Registry Operator (EBERO), the workload of the EBERO provider will be reduced by allowing them to utilise one Full Deposit rather than undertaking the complex task of applying any Differential Deposits.

2. The risk of not having a complete data set following the application of the Differential Deposits to the Full Deposits is eliminated until such time as Differential Deposits become necessary for the TLD.

3. It is simpler and more cost effective to produce and verify Full Deposits.

Data Escrow Format

The data escrow format defined in Specification 2 of the draft Registry Agreement http://tools.ietf.org/html/draft-arias-noguchi-registry-data-escrow-04 defines the base framework for data escrow deposits, but does not define the format of the registry data objects. There are two competing Internet-Drafts (I-D) for the format of the registry data objects that both comply with draft-arias-noguchi-registry-data-escrow. One defined by ICANN that uses XML, http://tools.ietf.org/html/draft-arias-noguchi-dnrd-objects-mapping-01 and one defined by Verisign (in consultation with other registries) that uses Comma-Separated Values (CSV), http://tools.ietf.org/html/draft-gould-thippeswamy-dnrd-csv-mapping-01. The agreement indicates to follow the 'draft version published at the time of signing the agreement', which at this point is only draft-arias-noguchi-registry-data-escrow, without reference to the format of the registry data objects. Considering the competing drafts for the registry data objects and the process required to define consensus within the IETF for following the standards track, the current language in the draft

Registry Agreement needs to be updated to reference the three Internet-Drafts, and be flexible to account for the IETF standards process.

RySG Recommendation

The RySG is seeking to have Specification 2 of the draft Registry Agreement updated to reference draft-arias-noguchi-registry-data-escrow along with the option of using either draft-arias-noguchi-dnrd-objects-mapping or draft-gould-thippeswamy-dnrd-csv-mapping, and to form a working group (IETF or open) that includes representatives from Registries (both new and existing) to define the data escrow drafts that will follow the IETF standards track.

RATIONALE

The proposed data escrow format is being actively debated and discussed by registry providers and others in the technical community. There is no defined community consensus for the existing drafts to follow the standards process to RFC, so locking into one or a set of Internet Drafts within the Registry Agreement prior to the community process will result in a fractured and unworkable solution for the registry providers and the EBERO providers. Referencing the drafts that exist with flexible language in the Registry Agreement along with driving to community consensus will help to address this issue.

Data Escrow – Criteria for acceptance of Escrow Contract and provider

Specification 2, Part B, paragraph 1 of the Registry Agreement states:

"Escrow Agent. Prior to entering into an escrow agreement, the Registry Operator must provide notice to ICANN as to the identity of the Escrow Agent, and provide ICANN with contact information and a copy of relevant escrow agreement, and all amendment thereto. In addition, prior to entering into an escrow agreement, Registry Operator must obtain the consent of ICANN to (a) use the specified Escrow Agent, and (b) enter into the form of escrow agreement provided. ICANN must be expressly designated a third-party beneficiary of the escrow agreement. ICANN reserves the right to withhold its consent to any Escrow Agent, escrow agreement, or any amendment thereto, all in its sole discretion."

RySG Recommendation

The RySG urgently requests from ICANN the criteria it will be using to determine whether to consent to an escrow provider as well as what is specifically being looked for in the Escrow agreement. Furthermore, the RySG is of the opinion that, as a third-party beneficiary, ICANN shall also be required to sign any contractual instruments associated with the provision of escrow services by a selected Escrow Agent.

RATIONALE:

In order to facilitate the Registry Operator's fulfillment of this clause and particularly given that such fulfillment must occur prior to the execution of the Registry Agreement, we believe it is critical for all Registry Operators to understand the criteria ICANN will be using to determine whether consent is granted in relation to the Registry Operator's use of a specified Escrow Agent and the Registry

Operator's entry into a particular form of escrow agreement. This request is particularly urgent as, in accordance with section 5.2.1 of the AGB, the Registry Operator is required to provide an executed Escrow Agreement to initiate the Pre-delegation test. Failure to provide the requested criteria decreases the likelihood that the applicant will present an Escrow Agreement that is acceptable to ICANN and may compromise the applicant's ability to undergo Pre-delegation testing as soon as possible. Finally, it must be clearly indicated also that, as a third-party beneficiary, ICANN is required to sign the escrow agreement (as well as any amendment thereto) with the Registry Operator, the Escrow Agent and, as the case may be for the Sponsoring entity.

Zone File Access Format

RySG Recommendation

We request that ICANN expand the requirement to reference the format described in in Section 3 of RFC 5936 (and the RFC references therein), with the one restriction that the $INCLUDE directives must not be used.

RATIONALE :

The Zone File Access Format outlined in Specification 4, Section 2.1.4 of the draft RA attempts to further restrict a technical format that is already adequately defined in RFCs. A new format requires new development by the registries to meet criteria that remains undefined to this day. It also causes a negative chain reaction of increased work---DNS zone file consumers must now alter their platforms to accept a new format. This unnecessary restriction of an already defined technical format increases the likelihood of complications and creates additional complexity for all parties involved, including consumers of the Zone File Access service.

Consumers of the Zone File Access service should be able to parse zone files in RFC compliant Master File format, or in an RFC compliant AXFR format. We do not understand the rationale for further restricting the format. As it stands, to implement the format requested by ICANN requires obtaining either a master file or AXFR from name servers, and then writing code to 'post process' the file into the format requested. Those involved in delivering and accessing Zone Files should be able to make use of existing tools that have been in place and proven for many years.

Some examples of the post processing that would be required include:

- Class and type in a standard AXFR are upper case; ICANN has requested them in lower case.
- Domain names follow the case as entered in the zone file.
- The BIND AXFR format uses spaces rather than tabs.
- $TTL is used extensively.
- Zone files are not always sorted alphabetically.

IDN Tables Format

RySG recommendation

Given the complexities that surround IDN variants, and the fact that ICANN's own IDN Variant Issues Project (VIP) group has not yet completed its work, we suggest that the requirement relating to the format of IDN tables be expanded to include additionally a format that has been previously accepted by IANA or is currently demonstrated to be in use by an existing TLD (ccTLD or gTLD), as an interim solution until a standard method for dealing with IDN variants is developed.

RATIONALE :

A number of new gTLD applicants have been requested by ICANN to resubmit IDN tables provided as part of the new gTLD application in a format that is consistent with either RFC4290 or RFC3743 (even though this requirement did not exist in the Applicant Guidebook). Additionally, the requirements in the Pre-Delegation Testing Provider RFP include verifying compliance with these RFCs.

It should be noted that these RFCs are 'informational' RFCs only, and are not 'standards track'. These RFCs are not ones developed by a working group of the IETF nor do they have community consensus. We are concerned that ICANN staff/consultants may be trying to shoe-horn registry operators into a standardized IDN implementation when no one-size-fits-all IDN implementation could be developed. In reality many registries have IDN tables that are implemented differently to these RFCs (based on different local language community requirements) but are nevertheless just as valid in making IDNs function (ARI Registry Services is using them for a number of IDN TLDs presently, امارات. (.emarat), قطر. (.qatar) and عمان. (.oman), and Neustar for at least .biz). ARI Registry Services' IDN tables are already in the IANA IDN table repository and have been previously accepted by IANA.

ICANN Reporting

In the coming months back end registry operators or 'technical' registry operators (TROs), have the challenge of operating many TLDs (hundreds of TLDs) on their registry infrastructure. There are three (3) main ways they may successfully manage multiple TLDs (of course combinations of each could be used):

1. Option 1 – Deploy different 'instances' of their registry, with an independent data store for each TLD. This is a different EPP interface for each TLD operated by the TRO with Registrars needing to connect to the right interface for each TLD;
2. Option 2 – Deploy a single 'instance' of their registry, with an independent data store for each TLD, then use an EPP extension like the Verisign's namestore extension to distinguish commands between each data store. This is a single EPP interface for all TLDs operated by the registry where Registrars are then asked to send through an 'identifier' with each command to distinguish which 'data store' the command is to operate on; or
3. Option 3 – Deploy a single 'instance' of their registry, with a single data store for all TLDs. This is a single EPP interface for all TLDs operated by the registry, where Registrars can create objects (including domains in the single data store)

As it currently stands, the reporting requirements of ICANN, as stipulated in Specification 3 of the RA, do not lend themselves cleanly to a Registry using Option 3. The current ICANN reporting assume a one to one mapping between registry (using registry to mean a repository of domains, hosts and contacts) and a TLD. For example, one of the reporting lines is the number of Contact objects that were created in the month. For example, in a single data store model, when a contact is created, it is unclear which TLD to attribute the contact create command to.

RySG Recommendation

Given the number of TLDs is now significantly higher than the number of back-end registry operators, and that in the majority of cases those back-end registry operators will operate more than one TLD from the one 'registry', the basis of this one-to-one assumption is no longer valid. These reporting requirements are therefore not pragmatic and should be revisited in conjunction with registries.

RATIONALE:

The one-to-one assumption raises a multitude of issues with respect to the mandatory reporting requirement. For example, where the back-end registry operator is providing services for two (2) TLDs, .tld1 and .tld2, which TLD's report shall a contact object be attributed to when it is created? A back-end registry operator currently only has two ways to address these issues (option 1 and option 2 above).

Both of these ways have drawbacks when compared to a single registry that stores registry data for all TLDs. Specifically;

1. Option 1 requires the deployment and management of potentially hundreds of instances of registry software, or development to fix as such. Additionally this option requires registrars to integrate with each TLD independently.
2. Option 2 requires registrars to implement a custom extension thus complicating their integration effort.

Several registries including Afilias, ARI Registry Services and Demand Media have indicated their desire to implement (or have implemented) option 3. Additionally a number of Registrars have indicated a preference to having registries use option 3. It is important to note that the issues associated with the one-to-one assumption only arise as a result of the requirement for registry operators to report on 'non-meaningful metrics' such as the number of contacts and hosts created in a TLD. Whilst we recognise the value in reporting on the number of domains and the transactions associated with those domains, we question the purpose and value in reporting on these non-meaningful metrics – especially considering the complexities and difficulties inherent in facilitating compliance with requirements that are not pragmatic any longer.

We therefore offer the following solution:

1. ICANN revisits the registry reporting requirements to reach a more pragmatic solution that takes into account the realities associated with the present day provisioning of back-end registry services. Such consideration should identify whether there is a

legitimate need and use for the information requested, and should recommend the elimination of a requirement to provide information that fails to meet this threshold.

Note: Neustar and the UPU have expressed objections to registries using option 3 as an implementation method, considering that they believe that the TLD data needs to be separable. In that regard, they are concerned that having an implementation method that combines all objects in one registry may present issues, particularly if one of the TLDs needs to be transitioned. Therefore, if Option 3 is to be selected, registries must ensure that each TLD is legally, logically and operationally separable from the others they operate in cases of an emergency or other transition, and in order to take into account specific conditions and requirements applicable to each TLD.

Pre-delegation Test Elements – DNS Infrastructure

We have identified a number of issues regarding the first set of test elements on DNS Infrastructure. These issues are described below.

Issue 1 - "Load capacity" testing against "randomly selected subset of servers"

The AGB states in Section 5.2.2 that:

*"**Load capacity** shall be reported using a table, and a corresponding graph, showing percentage of queries responded against an increasing number of queries per second generated from local (to the servers) traffic generators. The table shall include at least 20 data points and loads of UDP-based queries that will cause up to 10% query loss against a **randomly selected subset of servers** within the applicant's DNS infrastructure."*

RySG Recommendation

We hereby seek the following clarification:

A. Please define clearly what is meant by a 'subset of servers';
   - How many of them?
   - A small number of them or closer to 99% of them?
   - Is a subset consisting of a single server sufficient?

B. What is the target load capacity and who determines that? (expected capacity, peak capacity, etc.)

C. The reference to the 20 data points is undefined. Who defines the 20 data points and based on what? What do you do for very small TLDs, where 20 data points might be too many for the size? For low volume brand gTLDs, having 20 different data points isn't practical. Even for larger gTLDs, 20 is probably overkill. This number should be scaled back to a more manageable number with allowances for TLDs with low expected volume.

D. With the advent of Response Rate Limiting (RRL), there is no longer a one-to-one correspondence between query and response. This could be viewed as "Query Loss", when in fact the system is working correctly. If the queries for this test come in from a very small set of IP address blocks, RRL will indeed occur, radically skewing the "Query Loss" data. It may not be possible in a production ready environment (i.e. one where excessive diagnostic logging is not deployed for the reason of performance) to tell when a query is dropped due to actual Query Loss, or due to RRL. How should this be accounted for?

Issue 2 - "Reachability" documentation

The AGB states in Section 5.2.2 that:

"Reachability will be documented by providing information on the transit and peering arrangements for the DNS server locations, listing the AS numbers of the transit providers or peers at each point of presence and available bandwidth at those points of presence."

RySG Recommendation

We are particularly concerned with the disclosure of Reachability Information and Documentation. Many of us are not in a position to release it. In many cases, this is proprietary and confidential information that is part of agreements between registry service providers and third parties.

What is being requested to reveal is also sensitive network information, which if disclosed, exposes registry service providers to considerable security risk. Moreover, transit and peering arrangements are subject to change for business and technical reasons without notice.

The RySG recommends less stringent tests that demonstrate registry service providers' possess the technical competence required to effectively run registries.

Issue 3 - TCP and DNSSEC Capabilities

The AGB states in Section 5.2.1 that:

"The applicant may initiate the pre-delegation test by submitting to ICANN the Pre-Delegation form and accompanying documents containing all of the following information:

- *All name server names and IPv4/IPv6 addresses to be used in serving the new TLD data;*
- *If using anycast, the list of names and IPv4/IPv6 unicast addresses allowing the identification of each individual server in the anycast sets;"*

RySG Recommendation

Releasing sensitive network information such as lists of unicast IP addresses creates a security concern with members of the RySG. Not only is this information proprietary and confidential, revealing it to the public exposes registry service providers to considerable increase in risk. If an attacker gains access to a list of the unicast IPs, the whole network could be compromised. Instead the RySG recommends that the pre-delegation evaluator test the anycast system in the same way that the public uses the system. By testing from a large number (50) of locations instead of a small number as suggested in the RFP, results will be indistinguishable from what the public sees, and therefore much more indicative of the anycast network capability.

Issue 4 - "Self-certification" template and completed sample

The AGB states in Section 5.2.2 that:

"Self-certification documentation shall include data on load capacity, latency and external network reachability."

RySG Recommendation

We hereby seek the following clarification:

A. Can ICANN please provide a template and completed sample that covers exactly what ICANN is requesting as part of the applicant's testing reporting? A self-certification template and completed sample will help ensure uniform answers from all qualified applicants and should help to expedite the pre-delegation testing process.

Issue 5 - "Performing tests against existing infrastructure"

The AGB states in Section 5.2.2 that:

"The DNS infrastructure to which these tests apply comprises the complete set of servers and ***network infrastructure to be used by the chosen providers to deliver DNS service*** *for the new gTLD to the Internet."*

RySG Recommendation

We hereby seek the following clarification;

Performing tests against existing infrastructure, which are designed to cause packet loss, is not appropriate for infrastructure that is being used to service existing TLD zones and live customers, and therefore registry service providers will not be able to perform such tests as described. As such we offer the following suggestion:

A. We suggest that this test is included in the self-certification documentation with the option of the use of a dedicated Performance & Scalability (P&S) environment for use in load testing without causing harm to a shared system in Production.

Conclusion

As we now focus on the implementation of new gTLDs, we must all be wary of the finer technical implementation points that may create inefficiencies and unnecessarily increase costs for all parties involved.

Because many applicants and/or their backend registry service providers have already invested in a considerable amount of research/development work to ensure compliance with the guidebook requirements, it is critical that the recommendations discussed in this letter are considered as soon as possible so that reasonably sufficient advance time is made available for development and implementation of any such agreed-upon changes.

RySG Level of Support

1. **Level of Support of Active Members**: Supermajority
   1.1. # of Members in Favor: 11
   1.2. # of Members Opposed: 0
   1.3. # of Members that Abstained: 2
   1.4. # of Members that did not vote: 1

2. **Minority Position**(s): None

General RySG Information

- Total # of eligible RySG Members[1]: 14
- Total # of RySG Members: 14
- Total # of Active RySG Members[2]: 14
- Minimum requirement for supermajority of Active Members: 10
- Minimum requirement for majority of Active Members: 8
- # of Members that participated in this process: 14
- Names of Members that participated in this process:
  1. Afilias (.info, .mobi & .pro)
  2. DotAsia Organisation (.asia)
  3. DotCooperation (.coop)
  4. Employ Media (.jobs)
  5. Fundació puntCAT (.cat)

[1] All top-level domain sponsors or registry operators that have agreements with ICANN to provide Registry Services in support of one or more gTLDs are eligible for membership upon the "effective date" set forth in the operator's or sponsor's agreement (RySG Charter, Article II, RySG Membership, Sec. A). The RySG Charter can be found at http://www.gtldregistries.org/sites/gtldregistries.org/files/Charter_for_RySG_6_July_2011_FINAL.pdf

[2] Per the RySG Charter, Article II, RySG Membership, Sec.D: Members shall be classified as "Active" or "Inactive". An active member must meet eligibility requirements, must be current on dues, and must be a regular participant in RySG activities. A member shall be classified as Active unless it is classified as Inactive pursuant to the provisions of this paragraph. Members become Inactive by failing to participate in three consecutively scheduled RySG meetings or voting processes or both. An Inactive member shall continue to have membership rights and duties except being counted as present or absent in the determination of a quorum. An Inactive member immediately resumes Active status at any time by participating in a RySG meeting or by voting.

6. ICM, Inc. (.xxx)
7. Museum Domain Management Association – MuseDoma (.museum)
8. NeuStar (.biz)
9. Public Interest Registry - PIR (.org)
10. Societe Internationale de Telecommunication Aeronautiques – SITA (.aero)
11. Telnic (.tel)
12. Tralliance Registry Management Company (TRMC) (.travel)
13. Universal Postal Union (.post)
14. VeriSign (.com, .name, & .net)

- Names & email addresses for points of contact
  - Chair: Keith Drazek, kdrazek@verisign.com
  - Vice Chair: Paul Diaz, pdiaz@pir.org
  - Secretariat: Cherie Stubbs, Cherstubbs@aol.com
  - RySG representative for these comments: Keith Drazek kdrazek@verisign.com

Thanks you for your attention to these critical details. The RySG is available to respond to any questions you may have, and we look forward to working with you to resolve these remaining issues.

Sincerely,

Keith Drazek

Chair, Registries Stakeholder Group (RySG)

Cc: Akram Atallah, COO, ICANN