Comments of the Registries Stakeholder Group

New gTLDs DAG3 Modules 1-4

20 November 2009

The comments below, including a minority position, are submitted on behalf of the gTLD Registry Stakeholder Group (RySG) regarding Modules 1-4 of the New gTLD Draft Applicant Guidebook Version 3 (DAG3) posted in October 2009. They begin with a general comment followed by comments organized by section numbers for each of the four modules.
Note: Comments regarding the base registry agreement in Module 5 and the application terms and conditions in Module 6 will be submitted separately.

General Comment

Timing of IDN TLDs

At this point in time it seems clear that the IDN ccTLD Fast Track Process will begin significantly before the new gTLD process. In fact, the gap between the two processes could be a year and possibly longer. The RySG continues to be concerned about the pending divergence of these two processes and strongly recommends that steps be taken to reduce that gap. The demand for IDN TLDs includes both the ccTLD and gTLD marketplaces. There is a reasonable expectation from Internet end-users that when IDN ccTLDs work, IDN gTLDs will also work. In cases where gTLD registrants do business in multiple countries an IDN under an IDN gTLD may better serve their customers (i.e. Internet end-users).

Module 1 – Introduction to New gTLDs Application Process

1.1.2.4 Objection Filing

In response to DAG v.2 (DAG2), the RyC (now the RySG) recommended that the amount of time between the posting of the results of Initial Evaluation and the close of the objection filing period be specified in the next version and that it be a minimum of two weeks. We appreciate the fact that that period has now been defined to be two weeks.

1.1.2.6 Dispute Resolution

> In DAG2 the RyC recommended that "DRSPs should be strongly encouraged if not required to allow for consolidation of objections where possible and to thereby minimize expenses for applicants and objectors". In DAG3 some minor improvements were made but the decision is still at the discretion of the DRSP. We recommend that DRSPs be required to consolidate objections where feasible.

1.1.2.7 String Contention

Thank you for fixing this language: "String contention cases are resolved either through a community priority (comparative) evaluation (if a community-based applicant elects it) or through an auction."

1.2.3.1 Definitions

For DAG2 the RyC stated that the "definition of Community-based TLDs should be clear, measurable and concise and should not be subjected to "considerable subjective evaluation" as stated in the 'ICANN CALL FOR EXPRESSIONS OF INTEREST (EOIs) for a New gTLD Comparative Evaluation Panel' (http://www.icann.org/en/topics/new-gtlds/eoi-comparative-evaluation-25feb09-en.pdf)" In DAG3 it was changed to the following: "For purposes of this Applicant Guidebook, a **community-based gTLD** is a gTLD that is operated for the benefit of a clearly delineated community. . . . Designation or nondesignation of an application as community-based is entirely at the discretion of the applicant. Any applicant may designate its application as community-based; however, each applicant making this designation is asked to substantiate its status as representative of the community it names in the application. Additional information may be requested in the event of a community priority (comparative) evaluation (refer to Section 4.2 of Module 4). An applicant for a communitybased gTLD is expected to: 1. Demonstrate an ongoing relationship with a clearly delineated community. 2. Have applied for a gTLD string strongly and specifically related to the community named in the application. 3. Have proposed dedicated registration and use policies for registrants in its proposed gTLD, commensurate with the community-based purpose it has named. 4. Have its application endorsed in writing by one or more established institutions representing the community it has named.".

We appreciate the improved clarity but still recommend that the criteria should ensure 1) a mere customer or subscriber base is not deemed to be a community and 2) to qualify as a community-based gTLD, an applicant must demonstrate that community members would likely self-identify themselves as a member of the community. This clarification would add more objective criteria while at the same time making it clear that an organization or company couldn't take advantage of the community-based advantage just by claiming its customer base as a community. For example, the definition should preclude an applicant from claiming to be a community with an IDN version of an existing gTLD. In particular, we recommend the following be added to the definition of a Community-based TLD: "The following shall not be deemed to be a community: (i) a subscriber or customer base; (ii) a business and its affiliated entities; (iii) a country or other region that is represented by a ccTLD; or (iv) a language except in cases where the TLD is a recognized identifier for a UNESCO recognized language."

1.2.7 Voluntary Verification for High Security Zones

The RySG fully recognizes the value of "high security zones" for particular gTLDs, but we do not believe that is an appropriate role for ICANN for the following reasons: 1) it is not within ICANN's limited technical coordination mission related to Internet identifiers; 2) it would expand ICANN's authority to address malicious uses of domain names; 3) it

would put ICANN into direct competition with organizations that already are capable of performing such a function; and 4) the demand for such zones could be met more effectively by registries in cooperation with existing security organizations.

The RySG first offers the following general comments concerning the model for a High Security Zone Verification Program (HSZVP) and then provides some detailed comments.

General Comments

- The HSZVP proposes that ICANN participate in the development of a standards-based "trust seal" program. The extent of ICANN's participation in the development of this program is unclear and without foundation. The development of the standards should be left to other organizations that have the appropriate expertise in this area.
- The HSZVP contemplates registries taking responsibility for registrar functions, and for the accuracy and completeness of registrant data. Recent registrar failures have demonstrated the extreme challenges involved in factually providing such assurances.
- The HSZVP proposes to alter the fundamental contractual registry/registrar relationship and thrust registries into a de facto enforcement role vis-à-vis registrar functions. Not only does this run counter to the fact that ICANN, not registries, should enforce against contractual breaches by registrars, it fails to identify the suitable repercussions for registrar non compliance. This proposal also raises policy questions that are distinct from the issues raised by proposed contractual revisions.
- The HSZVP is contemplated for the newTLD program. The proposal raises fundamental issues concerning potential disparity of treatment between newTLD registries and existing TLD registries.

We note that the HSZVP is a new addition to the DAG, and that the details of this program are to be determined. The draft Explanatory Memorandum is a strawman proposal, and offers a surprising amount of detail given the newness of the concept. The Explanatory Memorandum notes that "a multi-stakeholder working group will be initiated that will be tasked with establishing a proposed implementation plan, with the intent to build a fully functional program." It is unknown under what auspices the working group will be established. ICANN staff members have told the RySG that with the input of the WG, the program could become mandatory for certain high security zones, or could become mandatory even perhaps at a much broader level. It is therefore difficult to comment fully at this time. The RySG reserves the right to comment further as plans unfold, and our comments here are not meant to be a full response to the proposal.

Detailed Comments

1. A central premise of the program is that the registries will be able to ensure the registrars' compliance with requirements. We question whether this is even possible for ICANN-related requirements.

The Exploratory Memorandum says that the program "builds upon the assumption that Registrars will be required to perform procedures to authenticate the accuracy of Registrant information at the time of domain registration." And that "The registry maintains effective controls to provide reasonable assurance that the processing of core registrar functions by its registrars is authorized, accurate, complete, and performed in a timely manner in accordance with established policies and standards…. The processes required to achieve this high-security status include verification of both registry operations and supporting registrar operations."

These assumptions raise several issues:

a. It is unclear how a registry would be able to guarantee a registrar's internal processes and choices. The reseller level of the distribution chain adds even more complexity and challenges.
b. Authentication of registrant information at time of registration may not be reasonable or reliable -- socially or technically. For example, there are no worldwide databases that provide reliable registrant verification. Registrars that are located in or do business with registrants in certain parts of the world may be at a disadvantage.
c. Auditing makes the registry operator responsible for the actions of the registrars, and for the results of the program as a whole. Given the facts outlined in (a) and (b) above, what registry operator and independent assessor would take on liability to develop and/or attest to the controls in place?

2. It has not been demonstrated if or how this new program can deliver better security and reduced malicious activity in the participating TLDs.
   a. Criminals already circumvent registrar-side controls designed to catch fraudulent credit card and contact data.
   b. Further to the authentication issue: checking to see if an individual or business is in a database does not constitute verification that that entity is purchasing the domain name. Every day criminals register domain names by appropriating the identities and contact data of other people and often obtain that information from databases.
   c. To our knowledge there have not been empirical studies of how domain eligibility policies and related procedures affect the amount of e-crime in a TLD. For example, abuse occurs regularly in some ccTLDs that have nexus requirements.
   d. Registries and registrars cannot control how registrants use the domains, or how registrant servers become infected by malware or hacked for phishing. So the proposed "SLA based on percent of malicious domains per 'unit measure' of registrations" is problematic.

3. The program is designed to provide a "competitive advantage" and a "business advantage" to new TLDs, and excludes many existing TLDs from participating. We wonder why ICANN is getting involved in the market, and why the program should not be open to all registries who wish to participate.

A central assumption of the program is that participating registries will be able to bind their registrars to certain requirements and that the registries will be able to choose which registrars they will do business with. This runs contrary to existing equal access and non discrimination obligations under current ICANN policy and is reflected in current registry contracts. If ICANN is proposing to eliminate the equal access and non discrimination obligations through the HSZVP proposal, it has failed to take into account the disparity of treatment between newTLD registries, who would operate without these obligations and existing TLDs who would continue to operate under these obligation. Moreover, it appears that the HSZVP grants the privilege of writing a registry-registrar contract uniquely to new TLD registry operators.

4. As noted above, the Explanatory Memorandum details how registry operators will "undergo an audit per the requirements of the Program." The proposed controls and audits will impose undefined financial and resource costs on newTLD registry operators. Given the unknown volume of registrations in certain newTLD registries, these costs could be prohibitive.

5. The Explanatory Memorandum says that "Other considerations, such as controls to address intellectual property concerns, could be added as components for future consideration in the lifecycle of the program." (page 4) We note that intellectual property concerns are NOT security issues. The two topics are very different and should not be conflated. This program should not be used as a test or template for a rights-protection mechanism.

6. ICANN should not circumvent consensus policy-making by offering game-changing inducements. The draft says that "Potential incentives (beyond market value) should be considered as a component of the program" (page 15) If the inducements are large enough, such opt-in programs can also become de-facto "requirements" in the registry space.

1.5.1 gTLD Evaluation Fee

We repeat our recommendation from DAG2: "In cases where a specific portion of the Initial Evaluation (e.g., Technical & Operational Capability, Financial Capability) is identical for multiple applications, applicant evaluation fees should be credited with the projected costs of that portion of the Initial Evaluation less any minor amount needed for evaluating such portion for multiple gTLDs. The costs of evaluation should reflect the actual cost of doing such evaluation and should not be based on a hypothetical average of projected total evaluation costs across all applicants."

Given that the IDN ccTLD fast track is on-going, and that applied for strings that are in the process are not disclosed until later in the process, it would be appropriate to provide

special full refunds for applicants submitting an application for a gTLD string that may later be found to have been in conflict with an IDN ccTLD.

1.5.2 Fees Required in Some Cases

The estimate of USD 50,000 for registry services evaluation seems excessive. It would be helpful to see a cost build-up of this estimate.

All new TLDs are required to provide DNSSEC support at launch as per Module 5 paragraphs 5.2.2 and 5.2.3, and DNSSEC is mentioned in Module 3 paragraph 2.1.3.1 as a "customary" registry service. We therefore assume that DNSSEC services will not trigger additional reviews or fees. ICANN should examine each applicant's proposed DNSSEC implementation for stability or security issues as part of the core evaluation process, as would be the case for all required registry services.

Module 2 - Evaluation Procedures

2.1.1.1 String Similarity Review

In DAG2 we recommended: "When performing the string confusion review against existing TLDs, an appropriate exception should be allowed in cases where the applicant is applying for an IDN version of its existing gTLD name." We are disappointed to note that our recommendation, which seemed simple and noncontroversial, was ignored. We again make this request.

2.1.1.3.2 String Requirements

We understand that work is continuing regarding the allowability of one and two character gTLD IDN strings. In that regard, we continue to support our previous position: "The following requirement as applied to IDN gTLDs should allow for exceptions in Chinese, Japanese and Korean scripts: "Policy Requirements for Generic Top-Level Domains – Applied-for strings must be composed of three or more visually distinct letters or characters in the script, as appropriate."

2.1.1.4.1 Strings Considered Geographical Names

The definition of geographical names is quite broad as copied below, including some possible gTLDs like .mac, .geo, etc.

> "The following types of applications are considered geographical names and must be accompanied by documentation of support or non-objection from the relevant governments or public authorities:
>
> 1. An application for any string that is a *country or territory name.* A string shall be considered to be a country or territory name if:
>   i. it is an alpha-3 code listed in the ISO 3166-1 standard.

ii. it is a long-form name listed in the ISO 3166-1 standard, or a translation of the long-form name in any language.
iii. it is a short-form name listed in the ISO 3166-1 standard, or a translation of the short-form name in any language.
iv. it is the short- or long-form name association with a code that has been designated as "exceptionally reserved" by the ISO 3166 Maintenance Agency.
v. it is a separable component of a country name designated on the "Separable Country Names List," or is a translation of a name appearing on the list, in any language. See the Annex at the end of this module.
vi. It is a permutation or transposition of any of the names included in items (i) through (v). Permutations include removal of spaces, insertion of punctuation, and addition or removal of grammatical articles like "the." A transposition is considered a change in the sequence of the long or short–form name, for example, "RepublicCzech" or "IslandsCayman."

2. An application for any string that is an exact match of a *sub-national place name*, such as a county, province, or state, listed in the ISO 3166-2 standard.
3. An application for any string that is a representation, in any language, of the *capital city name* of any country or territory listed in the ISO 3166-1 standard.
4. An application for a *city name*, where the applicant declares that it intends to use the gTLD for purposes associated with the city name.
5. An application for a string which represents a *continent or UN region* appearing on the "Composition of macro geographical (continental) regions, geographical sub-regions, and selected economic and other groupings" list.[5] In the case of an application for a string which represents a continent or UN region, documentation of support will be required from at least 69% of the relevant governments in the region, and there may be no more than one written objection to the application from relevant governments in the region and/or public authorities associated with the continent or the UN region.

"An applied-for gTLD string that falls into any the above categories is considered to represent a geographical name. In the event of any doubt, it is in the applicant's interest to consult with relevant governments and public authorities and enlist their support or non-objection prior to submission of the application, in order to preclude possible objections and pre-address any ambiguities concerning the string and applicable requirements."

Regarding point 5 of section 2.1.1.4.1 Strings Considered Geographical Names, specifically for strings representing "a continent or UN region", we observe that there are a very small and finite number of macro geographical regions and sub-regions. Furthermore, it is understandable that the cultural and geopolitical conditions for each region could vary substantially. We therefore find it inappropriate to assign any specific (and largely arbitrary) percentile to the requirements. Rather, they should be examined on a case-by-case basis in consultation with the GAC. Unlike general generic strings for which there is a large number of possible names and scalability is an issue, this is, by definition in the DAG v.3, a special consideration for a very specific sub-set of names, for which case-by-case consideration should be appropriate.

Consideration should be given to the following: if in looking at the string there is clearly no association with the geographic location, the new TLD applicant should be able to override the presumption in favor of the geographic entity. For example, if one applies for .geo and in looking at the application, it is clear that the TLD is not geared towards the nation of "Georgia", it should be allowed to proceed.

2.1.2.3 Evaluation Methodology

We were disappointed that the following sentence was not changed in DAG v.2: "Evaluators are entitled, but not obliged, to request further information or evidence from an applicant." DAG3 says, "The evaluators may request clarification or additional information during the Initial Evaluation period. The applicant will have one additional opportunity to clarify or supplement its application in areas requested by the evaluators." So we are disappointed again. The DAG position assumes that the Evaluation Questions and Criteria in Module 2 are perfectly clear and complete; if they are not, applicants are at the mercy of the evaluators, thereby making the process more subjective. It is one thing if information required is specifically stated in the Evaluation Questions and Criteria but, in cases where it is not explicit, evaluators should be easily able to identify that and should be required to request further information via an explicit request.

2.1.3.1 Definitions

The definitions of "Security" and "Stability" raise a number of policy and scope issues and subject registry operators to unilateral contract changes and unpredictable obligations. They therefore require revision.

These definitions are also found in other places in the modules and their attachments, notably in the Draft Registry Agreement paragraph 8.3.

The definitions read:

> "***Security*** – an effect on security by the proposed registry service means (1) the unauthorized disclosure, alteration, insertion or destruction of registry data, or (2) the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards.
> ***Stability*** – an effect on stability means that the proposed registry service (1) does not comply with applicable relevant standards that are authoritative and published by a well-established, recognized, and authoritative standards body, such as relevant standards-track or best current practice RFCs sponsored by the IETF, or (2) creates a condition that adversely affects the throughput, response time, consistency, or coherence of responses to Internet servers or end systems, operating in accordance with applicable relevant standards that are authoritative and published by a well-established, recognized and authoritative standards body, such as relevant standardstrack or best current practice RFCs and relying on registry operator's delegation information or provisioning services."

These definitions need revision for the following reasons:

A. "Unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards" is too broad. That language potentially takes in a wide variety of small and large security incidents on the Internet, such as unauthorized access or data breaches on third-party networks, malware

that has infected individual user systems, phishing on compromised web sites, etc. The mere fact that services are operating on a domain name does not imply or require registry involvement. Registries do not have any technical ability to mitigate many of those kinds of problems. And most do not threaten the systematic security, stability and resiliency of a TLD or the DNS itself, and are therefore out of ICANN's mission scope.

We suggest the language be changed to read: "Unauthorized disclosure, alteration, insertion or destruction of registry data, or the unauthorized access to or disclosure of registry information or resources on the Internet by registry systems operating in accordance with all applicable standards."

The DAG3 language seems to come from the Registry Services Evaluation Policy (RSEP) definition of an "effect on security" that is found in all Registry Agreements. The RSEP discusses how new registry services should not negatively impact security, and that new registry services should be compliant with applicable relevant standards. That context is missing in DAG3. Without that context, the language has become more expansive and open to interpretation. Both ICANN and the RySG desire that registries function within applicable standards, and that current or future registry services not be the genesis of security problems.

B. This language is unacceptable: "authoritative and published by a well-established, recognized, and authoritative standards body." ICANN should not leave the language open-ended and make contracted parties subject to any and all standards bodies. ICANN needs to more explicitly enumerate the standards and name the authoritative body, which we believe is the IETF. Application of additional standards should be considered via the consensus policy process instead.

The definitions also conflict with and exceed the draft gTLD Agreement, which names the IETF and enumerates RFCs:

> "Specification 6:1. **Standards Compliance**
> Registry Operator shall implement and comply with relevant existing RFCs and those published in the future by the Internet Engineering Task Force (IETF) including all successor standards, modifications or additions thereto relating to (i) the DNS and name server operations including without limitation RFCs 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 3901, 4343, and 4472; and (ii) provisioning and management of domain names using the Extensible Provisioning Protocol (EPP) in conformance with RFCs 3735, 3915, 5730, 5731, 5732, 5733 and 5734" etc.

C. The DAG3 definitions misunderstand IETF practices and definitions. The contract language must be revised to adhere to proper terminology.

The inclusion of "Standardstrack" [sic] is inappropriate, since only some documents on the "standards track" are authoritative. IETF Internet specifications go through stages of development, testing, and acceptance. Within the Internet Standards process, these stages are called "maturity levels." These maturity levels include "Proposed Standard", "Draft

Standard", and "Standard" Specifications.[1] Documents at lower maturity levels are not Internet Standards, do not enjoy enough development or vetting, and registries should not be required to follow them.

Contracted parties should not be required to adhere to IETF Best Practices or "best current practice RFCs". By definition, best practices are not mandatory, and the IETF chose to make them Best Practices for a reason. Nor are IETF BCPs considered technical standards. They tend to deal with processes and procedures rather than protocols -- they represent a consensus of a way to do something because it is recognized that a user experience can be enhanced when there is an agreed-upon way to complete a task. However, interoperability is not usually applicable. As long as the user experiences standards-compliant behavior, ICANN does not need to say more about how that behavior is achieved.

Attachment to Module 2: Evaluation Questions and Criteria

Question 31

Answering parts of Question 31 could disclose details about operational security at a registry -- publicly revealing sensitive security procedures and vulnerabilities. This question is scored on a 0 to 2 scale, and applicants will feel it necessary to provide detail in their attempts to achieve a "1 meets requirements" or "2 exceeds requirements" score.

We therefore suggest that these sub-questions be protected by confidentiality:

- "provisioning and other measures that mitigate risks posed by denial of service attacks;"
- "a threat analysis for the proposed registry and the defenses that will be deployed against those threats;" and
- "independent assessment report to demonstrate security capabilities, if any"

Question 35

Answering parts of Question 35 could disclose details about operational security at a registry, publicly revealing sensitive security procedures and vulnerabilities. We therefore suggest that ICANN offer more guidance to applicants, and allow them to designate sensitive portions of their replies as confidential.

Question 35 also requires that applicants describe their "proposed measures for management and removal of orphan glue records for names removed from the zone." The issue of orphan record management may not be adequately or commonly understood, and we wonder what criteria evaluators will use to evaluate it. We also see that ICANN has cited an APWG study on this issue[2], but this report has not yet been published. The

[1] http://www.ietf.org/about/standards-process.html and http://tools.ietf.org/html/rfc2026#section-4

[2] "New gTLD Program Explanatory Memorandum: Mitigating Malicious Conduct," page 9: http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf .

issue requires more discussion in general, and ICANN should not rely on unpublished or non-public material.

Module 3 - Dispute Resolution Procedures

3.1.5 Independent Objector

As stated it its Explanatory Memorandum, ICANN claims that the "need for an "Independent Objector" would arise when no objection is filed to a TLD that would be considered objectionable across many jurisdictions." ICANN Staff state that they are attempting to simply provide an answer to the question of "What will be done if there is an application for a highly objectionable name but there are no objections within the process?" The simplest response is that if no one is willing to file an objection then clearly the proposed TLD is not objectionable.

Two situations are identified for which there may be a need for an "Independent Objector". The first is where "no objection is filed to a TLD that would be considered objectionable across many jurisdictions" and the second is where a government might have an objection but chooses not to utilize the independent dispute process and instead (because of political and perhaps sovereignty concerns) would use courts or an outside agency to attempt to block the application outside of the new gTLD process.

The real reason why no one might file an objection to what may be an objectionable TLD is that ICANN's proposed objection process may be flawed for one or both of these reasons: (i) requiring Objectors to be able to pay the dispute resolution fees (which in the instance of objections based on community or morality are likely to be on the high end because of the inherent contentious nature of the subject matter); (ii) expecting sovereign entities to be willing to submit to the Independent Dispute Resolution process with regard to matters that a country might view as relating to their religious, social or ethnic identity or otherwise relate to fundamental public policies.

Even the use of an Independent Objector to raise these concerns will not prevent a country or other governmental entity from resorting to courts or outside agencies to block an application it deems objectionable if the Independent Objector does not prevail in the Independent Dispute Resolution Process, thereby making the applicant in this instance having to argue their case in at least two forums.

However, the role of the Independent Objector may have some value where its role is limited to providing a means for those who are not financially able to file an objection to be able to be heard. However, the use of an Independent Objector in this manner must be tightly limited:

- First, a process would be needed for individuals and/or groups to submit a request that the Independent Objector file an objection on their behalf. Objectors would need to provide a statement of interest and be able to demonstrate that they are not

financially able to file an objection themselves. An applicant should be able to object to an objector's standing. Under no circumstance should the Independent Objector be able to file an objection without a request from an outside group or individual -- no "sua sponte" "unidentified objectors" or "on its own behalf" objections may be filed by the Independent Objector.

- Secondly, ICANN's Board should establish the criteria that the Independent Objector must follow in choosing which objections, and at the time of filing the objection with a Dispute Resolution Provider, the Independent Objector would be required to provide the applicant with a written statement of how the objection met the established criteria. A failure to follow the established criteria should be a basis for dismissal of the Objection by the Dispute Resolution provider.
- Third, the Independent Objector should not be allowed to file an objection if a third party has already filed an objection against an applicant for the same or substantially similar reasons.
- Fourth, Because ICANN would be essentially funding the objection, in all fairness, ICANN should also advance the applicant's share of the dispute resolution fees, requiring payment only in the event that the dispute resolution provider decides in favor of the Independent Objector

Most of the suggestions above were ignored

3.3.2 Consolidation of Objections

In response to DAG2, the RyC stated, "It is not clear that DRSPs should be given full discretion on this issue, but at a minimum, it would seem highly desirable for each DRSP to publish the criteria it will use to make such a decision and DRSPs should be encouraged to consolidate similar objections into one proceeding if requested by either the Applicant or any Objector.' DAG3 says, "ICANN continues to strongly encourage all of the DRSPs to consolidate matters whenever practicable." We repeat our recommendation from DAG2.

3.3.3 Negotiation and Mediation

Note the following from DAG2: "There are no automatic extensions of time associated with the conduct of negotiations or mediation. The parties may submit joint requests for extensions of time to the DRSP according to its procedures, and the DRSP or the panel, if appointed, will decide whether to grant the requests, although extensions will be discouraged. Absent exceptional circumstances, the parties must limit their requests for extension to 30 calendar days." The RyC commented: "Except in cases where a time extension might negatively impact applicants who are not involved in a negotiation or mediation, granting a small time extension (e.g., not more than 30 days) would seem like a very reasonable step to take if all involved parties concur and that would likely encourage negotiation and mediation. Why shouldn't automatic extensions be granted for 30 days or less if all impacted parties agree and request them? Moreover, when disputes are settled by negotiation without DRSP intervention, all or a portion of DSRP

fees should be refunded." Not only were no changes made in DAG3 but the questions have not been answered so we hereby repeat our comments and questions.

For DAG2 we asked: "Why was the following text deleted: "~~ICANN will strongly encourage DRSPs to use reasonable efforts to issue all final decisions within 45 days of the panel appointment date unless, after both parties have completed their initial submissions, the parties jointly request a short postponement of their adjudication date to accommodate negotiation or mediation or to accommodate other aspects of the proceedings, and the panel agrees.~~"? Timely action by DRSPs is an important part of the process. The deleted text did not set any firm requirements but at least gave DRSPs a target." No changes were made in DAG3 and the question was not answered so we hereby repeat our DAG 2 comments and question.

Attachment to Module 3 ***New gTLD Dispute Resolution Procedure***

Article 4. Applicable Rules

For DAG2 we stated, "The applicable rules and procedures that the different DSRP's will follow should be published and made subject to comment." We state this again because there were no changes made in DAG3 in this regard.

Article 13. The Panel

For DAG2 we commented: "The following should be changed to provide the option for a 3-person panel: "(b) Number and specific qualifications of Panelist: (i) there shall be one Panelist in proceedings involving a String Confusion Objection." It is contrary to normal commercial dealings to allow a single arbitrator to determine important disputes. Indeed, the philosophy of the ICC rules, and the rules of most other arbitral authorities, is clearly to the contrary. Among other things, use of a single arbitrator in all disputes would inject large uncertainty into the process of dispute resolution, for ICANN as well as the applicants and objectors." Why was there no response to this? We submit this comment again for DAG3.

Module 4 - String Contention Procedures

4.1.3 Self-Resolution of String Contention

As stated in response to DAG2: "The continued rejection of the formation of joint ventures seems unreasonable, especially in cases where there are no material changes in applications or need for re-evaluation."

4.2.3 Community Priority (Comparative) Evaluation Criteria

The only purpose of Comparative Evaluation criteria is to resolve string contention. Why has Nexus criteria (e.g. "uniqueness") been implemented to only qualify applicants not facing string contention (thus not the need for Comparative Evaluation)?

GNSO gTLD Registry Stakeholder Group Statement of Support with regard to These Comments

A majority of 9 RySG members supported this statement:

- Total # of eligible RySG Members[3]: 14
- Total # of RySG Members: 14
- Total # of Active RySG Members[4]: 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)
2. DotAsia Organisation (.asia)
3. Dot Cooperation LLC (.coop)
4. Employ Media (.jobs)
5. Fundació puntCAT (.cat)
6. mTLD Top Level Domain (.mobi)
7. Museum Domain Management Association – MuseDoma (.museum)
8. NeuStar (.biz)
9. Public Interest Registry - PIR (.org)
10. RegistryPro (.pro)
11. Société Internationale de Télécommunication Aéronautiques – SITA (.aero)
12. Telnic, Limited (.tel)
13. Tralliance Corporation (.travel)
14. VeriSign (.com, .net & .name)

- Names & email addresses for points of contact:
  - Chair: David Maher, dmaher@pir.org

[3] 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 (Article III, Membership, ¶ 1). The RySG Articles of Operations can be found at http://www.gtldregistries.org/about_us/articles .

[4] Per the RySG Articles of Operations, Article III, Membership, ¶ 4: Members shall be classified as "Active" or "Inactive". 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 a Constituency meeting or voting process for a total of three consecutive meetings or voting processes or both, or by failing to participate in meetings or voting processes, or both, for six weeks, whichever is shorter. An Inactive member shall have all rights and duties of membership other than being counted as present or absent in the determination of a quorum. An Inactive member may resume Active status at any time by participating in a Constituency meeting or by voting.

- Alternate Chair: Jeff Neuman, Jeff.Neuman@Neustar.us
- Secretariat: Cherie Stubbs, Cherstubbs@aol.com

Regarding the issue noted above, the level of support in the RySG for the Constituency statement is summarized below.

1. **Level of Support of Active Members**:
   1.1. # of Members in Favor: 11
   1.2. # of Members Opposed: 1
   1.3. # of Members that Abstained: 0
   1.4. # of Members that did not vote: 2
2. **Minority Position**(s): Telnic submits the following minority position:

There is more to a sponsored TLD community than the string. Similarly there is more to a community-based application than the string.

In this draft, the objection process focuses on string conflicts.

A gTLD could conflict with an existing sTLD (or a community based TLD) not through the string, but through the concept it claimed to support.

We believe that there should be a *new* requirement for the gTLD concept to be described in all applications - both standard and community-based ones. This would highlight confusingly similar concepts, which is a concern for sponsored TLDs (and community-based TLDs) and could be a justification for an objection.

Also, the definition of institution that is capable of launching a community-based objection is much narrower than was the case in the previous sTLD round; there seems to be no justification for this change.

The DAG process has missed this concept confusion issue; it is not mentioned in the draft at all. Given that this is a substantive gap, we believe this should be discussed with the stakeholders before the DAG is complete.