COALITION FOR ONLINE ACCOUNTABILITY
WWW.ONLINEACCOUNTABILITY.NET

C/O MITCHELL SILBERBERG & KNUPP LLP ● 1818 N STREET N.W., 8TH FLOOR ● WASHINGTON, D.C. 20036-2406
TEL: (202) 355-7906 ● FAX: (202) 355-7899 ● E-MAIL: INFO@ONLINEACCOUNTABILITY.NET

Comments of

Coalition for Online Accountability on

DAG version 4 and accompanying documents

July 21, 2010

The Coalition for Online Accountability (COA) provides the following comments on version 4 of the Draft Applicant Guidebook for new gTLDs (DAG v4), as well as on several other related documents posted by ICANN for comment by the same deadline.[1]

About COA

COA consists of eight leading copyright industry companies, trade associations and member organizations of copyright owners. These are the American Society of Composers, Authors and Publishers (ASCAP); Broadcast Music, Inc. (BMI); the Entertainment Software Association (ESA); the Motion Picture Association of America (MPAA); the Recording Industry Association of America (RIAA); the Software and Information Industry Association (SIIA); Time Warner Inc.; and the Walt Disney Company. COA has been an active participant in ICANN's work to develop the new gTLD program, both on its own account and as a member of the Intellectual Property Constituency (IPC). COA has filed more than a dozen submissions to ICANN on various topics related to new gTLDs, which can be reviewed at http://www.onlineaccountability.net/gTLD_submissions.htm.

About these Comments

Section I of these comments addresses a number of issues of concern to COA in the text of the DAG v4. Within Section I, the comments are organized by module of the DAG v4 text.[2]

[1] See http://www.icann.org/en/public-comment/#guidebook. These comments will also be cross-posted in the various separate public comment fora ICANN has established for the other documents.

[2] See http://www.icann.org/en/topics/new-gtlds/draft-rfp-redline-28may10-en.pdf.

The remaining sections of these comments address issues falling wholly or partially outside the text of DAG v4, issues that ICANN staff have designated, at one time or another, as "overarching" questions that must be resolved before the new gTLD launch occurs. Section II concerns the "Economic Framework" study released by ICANN in mid-June.[3] Section III addresses the "malicious conduct issues" covered in the Explanatory Memorandum on this subject and the High Security TLD Zone "snapshot" document.[4] Section IV concerns rights protection mechanisms (which have been integrated into DAG v4). Section V deals with the issue of restrictions on vertical integration of registries and registrars in the new gTLD environment.

Section I: DAG v.4 Issues

In general, the comments in this opening Section share two characteristics. First, as noted above, they do not directly involve so-called "overarching" issues, but instead focus on matters that were described by ICANN staff at the Nairobi meeting as "issues that have been addressed and closed." When asked why, if these issues were closed, they would be put out once again for public comment in DAG v4, staff replied, "We are still taking public comment on the draft applicant version 4. But the hope is that the issues are 99% complete as opposed to being completely open." See Nairobi session transcript at http://nbo.icann.org/node/8877 (statements of Kurt Pritz, and slides 4 and 5).

Second, most of this section concerns issues that COA – and often several other submitters as well – have raised repeatedly in the new gTLD process. We give them pride of place in this submission to underscore our strong view that in fact they are not "addressed and closed," nor even "99% complete." We urge ICANN staff to revisit these issues with an open mind and to propose needed changes before the Board meets in late September to consider "all of the outstanding issues relating to implementation of the new gTLD program." See http://www.icann.org/en/minutes/resolutions-25jun10-en.htm#11.

A. Module 2

COA commends ICANN for instituting background checks of new gTLD applicants, and for providing for disqualification of applicants on specified grounds set out in question 11 of the Evaluation Questions. We continue to find question 11(f) both ambiguously phrased and too narrow. This question reads: "Disclose whether the applicant has been involved in any administrative or other legal proceeding in which allegations of intellectual property infringement of a domain name have been made. Provide an explanation related to each such instance." This phrasing seems to assume that one has intellectual property rights in a domain name. The more relevant question is whether the applicant has been charged with activities that

[3] See http://www.icann.org/en/topics/new-gtlds/economic-analysis-of-new-gtlds-16jun10-en.pdf.

[4] See http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-memo-update-28may10-en.pdf and http://www.icann.org/en/topics/new-gtlds/hstld-program-snapshot-2-16jun10-en.pdf.

infringe intellectual property rights, in which a domain name has been used. The question should be rephrased to refer to "allegations of intellectual property infringement relating to registration or use of a domain name." To give one example, the operators of the websites whose domain names were recently seized by the U.S. government because of their use in carrying out massive criminal copyright infringement should have to disclose that fact if they applied for the right to operate a new gTLD registry. See http://www.justice.gov/usao/nys/pressreleases/June10/websitedomainnameseizurepr.pdf It should also be made clear in the adjoining "Notes" column that ICANN can reject an application in which the applicant cannot provide a satisfactory explanation.

ICANN should also require would-be new gTLD operators to disclose their policies for Whois data quality. Specifically, they should spell out how they will require registrars who sponsor registrations in the new gTLD to ensure the accuracy and currency of Whois data that they collect. As discussed in Section I-D below, the best approach would be to include requirements regarding Whois data quality in registry agreements with new gTLD operators, as is already the case with several existing gTLDs. But a worthwhile fallback would be to require disclosure in the application on this point.

The new gTLD application form already includes a number of open-ended questions in which applicants are required to spell out their planned policies, some of which are scored for purposes of application evaluation (see, e.g.., question 31 re security policies) and some of which are not scored (see, e.g., question 23 re registry services). No cogent justification has been offered for refusing to extend this treatment to the critical question of improving Whois data quality. Article 1.3(a)(i) of the current draft of the base registry agreement calls for registries to warrant the accuracy of "all material information provided and statements made in the registry TLD application," whether or not those statements are "scored," and thus would make it possible for ICANN to use contract compliance tools to pursue registries who misrepresent their plans on these important questions.[5]

Finally, in order to provide concrete, application-based incentives for applicants to protect the public by adopting the more rigorous protections spelled out in the High Security Zone TLD program, a specific evaluation question on this point should be included, and applicants should be awarded one or more optional points for a positive response. Alternatively, one or more points could be deducted from the evaluation score of an applicant who declines to take these additional steps to protect the public. See Section III below for further discussion of the HSZTLD program.

[5] For at least the fourth time, COA calls upon ICANN to revise the base registry agreement to give ICANN the authority to audit new gTLD registries regarding material misrepresentations made in the application and contract negotiation process, as well as material statements that are no longer true. The language now found in section 2.11 of the draft agreement remains deficient because it only authorizes audits for compliance with "covenants contained in Section 2 [sic: should be Article 2] of this Agreement," while the warranty of truthfulness of these statement appears in Article 1.

B. Module 3

1. Community Objections

While there have been some small steps taken in DAG v4 to facilitate the recognition of bona fide community objections to applications, much more should be done, for the reasons COA has spelled out in detail in its previous submissions.[6] Specifically:

- In section 3.1.2.4 of the DAG, dealing with standing to raise a community objection, insert the following at the end of the section:

"Where more than one entity joins together to file a community objection, or where more than one community objection is consolidated pursuant to 3.3.2, the qualifications of the objectors shall be cumulated for purposes of determining standing. Business and trade associations, and membership/affiliate organizations, are eligible to demonstrate standing to file a community objection under the above criteria."

- In section 3.4.4, setting forth the tests to be applied to a community objection, insert the following in lieu of the first paragraph under "Detriment":

"An objector that satisfies the preceding tests shall be presumed to have established a likelihood of detriment to the rights or legitimate interests of its associated community. However, this presumption may be rebutted by the applicant. Ultimately, for an objector to prevail, the panel must determine that such detriment is likely if the objected-to application were approved. Factors that could be used by a panel in making this determination include, but are not limited to:"

- In the same section, provision should be made for defining the circumstances under which "satisfaction of the standing requirements for filing a Community Objection …. by a community-based applicant is a complete defense to an objection filed on community grounds." An applicant asserting this defense should be required to affirmatively prove that the community it claims to represent is substantially identical to the community expressing opposition. While it should not be possible for a community-based applicant to assert the complete defense by claiming to represent a community that is not substantially identical to the one expressing the objection, proof of satisfaction of the standing requirements may also provide an element of a defense to the objection even if the complete defense is not available.

[6] See in particular http://www.onlineaccountability.net/pdf/COA%20comments%20on%20DAG%20v3%20excerpts%20and%20EMs%20072009.pdf and previous submissions cited therein.

2. *Morality and Public Order Objections*

COA has supported the previous comments of the Intellectual Property Constituency calling for a "quick look" procedure to reduce the detriment to free speech interests that could be inflicted by frivolous objections on this ground. ICANN's proposal on this score leaves much to be desired.[7] This procedure would require the applicant to respond fully to the frivolous objection, and to pay a response filing fee, before any "quick look" would occur. It would also postpone any "look" until a full complement of adjudicators had been empaneled. This process is unlikely to be "quick," and very likely to be inordinately costly.

COA understands that the entire morality and public order objection process is likely to be revisited in light of strong objections from the Governmental Advisory Committee. We urge that this review include developing a more expeditious and lightweight means of disposing of frivolous objections in this area.

3. *Malicious Behavior Vulnerability Objection Needed*

Some objection mechanism needs to be created to deal with the situation in which an application, while meeting the baseline standards for passing successfully through an evaluation, nonetheless would leave members of the public excessively vulnerable to the risks of malicious activities. Such a situation would arise on an application by application basis. The DAG recognizes that this might be the basis for a community objection, since it lists as one kind of "detriment" to the community "that the applicant has not proposed or does not intend to institute effective security protection for user interests."[8] But the problem could arise wholly outside the community context; and it should be possible to raise the concern without having to meet the standards for establishing standing to file a community-based objection.

Consider, for example, a proposed .kids gTLD. It could credibly be argued that all parties wishing to register in such a gTLD should be thoroughly vetted, or at least that their identities and contact information be fully verified before registration. Yet nothing in the evaluation process requires this; an applicant for .kids who proposed to dispense with such registrant vetting could achieve a perfect score as the evaluation process now stands. Nor should someone who wishes to raise this objection be required to prove its standing to speak on behalf of a "community" of children, even if such a community could be delineated. While it is true that this concern could be raised in public comments, which the evaluators are supposed to take into consideration, it is not even clear that the current proposal provides any path for an evaluator to act on these comments and insist on heightened security procedures for .kids. An evaluator cannot reject an application because the applicant refuses to do more than the evaluation standards now require.

---

[7] See http://www.icann.org/en/topics/new-gtlds/morality-public-order-quick-look-28may10-en.pdf and section 3.1.2.3 of DAG v.4.

[8] See section 3.4.4 of DAG v.4.

This significant gap in the objection process needs to be filled. One approach might be to assign this duty to the Independent Objector, who would be in a position to evaluate public comments that raise this concern, to consult with relevant experts, and then to launch an objection if needed. Other approaches should also be considered. But unless and until some mechanism is provided, the new gTLD system lacks a critical safeguard for the public interest.

C. Module 4

COA's concerns about the standards to be applied in a "community priority evaluation" process have also been expressed many times in its previous submissions. The staff's reversal of its decision to allow a community applicant to survive this process if it scores 13 of a possible 16 points, and its insistence on a 14-point threshold, which will be almost impossible for most community applications to achieve, has never been satisfactorily explained. The reversal has been attributed to "additional testing" of hypothetical scenarios, none of which have been publicly disclosed; and the staff seemed to concede at the Brussels meeting that this testing was not reproducible.[9] When it was pointed out that public comment had sided overwhelmingly with the 13-point threshold, the only response was that "often we have changed the guidebook based on a single comment."[10]

COA urges the staff to revisit this question, especially in light of the conclusion of the Economic Framework paper (discussed below in Section II of these comments) that "the development of gTLDs to serve communities of interest" is one of three categories on the list of the likely "largest sources of potential benefits from the creation of new gTLDs." In addition, to reduce at least slightly the likelihood that the community priority evaluation process will be nothing more than anteroom to an auction hall, COA proposes that the criteria for a top score on the following evaluation criteria, as set out in section 4.2.3 of DAG v.4, be modified to read as follows (adding the underlined text):

- Nexus: The string matches the name of the community, is a well known short-form or abbreviation of the community name, <u>or is otherwise strongly associated with the community.</u>

- Uniqueness: String has no other significant meaning beyond identifying the community <u>described in the application. (This criterion to be applied in the language associated with the described community, if applicable). A meaning unrelated to any community would not be considered significant</u>.

D. Module 5

COA offers the following comments on aspects of the draft Registry Agreement attached to this module.

---

[9] See http://brussels38.icann.org/node/12443, click on transcript-gtld-20jun10-en.pdf, at pp. 42-3.

[10] See id. at 47-48.

COA strongly supports the requirement that registries in the new gTLDs provide a fully searchable Whois service (see section 1.8 of Specification 4). However, the stated "point of reference" to .name is inapposite. Beyond the three existing gTLD registry agreements which already contain such a requirement[11], this provision hearkens back to the Whois service provided by the legacy gTLD registries at the time ICANN came into existence. Before the "thin Whois" system cut back on registry Whois and placed on registrars the primary responsibility for maintaining this critical tool for DNS accountability and transparency, the monopoly registration provider for .com/net/org provided a fully searchable Whois service. Proposed section 1.8 of Specification 4 is another small step that ICANN should take toward bringing the quality of Whois service back to the level that existed when ICANN took stewardship of it nearly a dozen years ago. In this context, the special arrangement approved by the Board on an explicitly non-precedential basis for the tiny .name registry is basically irrelevant. See http://www.icann.org/en/minutes/prelim-report-02dec02.htm.

Three of the gTLD registry agreements that ICANN has signed most recently – for .asia, .mobi and .post – go well beyond what is proposed in DAG v.4. First, they require fully searchable Whois services, not only at the registry level, but also for all registrars sponsoring registrations in those domains. Second, they call for registrars to adhere to a compliance review policy, under which they must –

- "designate a contact point to which evidence of false or fraudulent contact data may be reported";
- "institute procedures for investigating claims that registrations may contain false information";
- "for registrations found to contain false information, require their speedy and efficient correction, or otherwise cancellation"; and
- allow "interested third parties [to] invoke these procedures."[12]

These eminently reasonable and practical requirements represent the current best practice for gTLD registry agreements, and ICANN should bring them forward in the base registry agreement for new gTLDs. At a time when law enforcement, private sector security experts, consumer protection agencies, and many other groups all agree that more accurate Whois data is an essential tool in combating a growing tide of malicious, criminal, and otherwise illegal behavior online – including but by no means limited to copyright and trademark infringement – ICANN has provided no cogent reason why it should not take a more proactive role in setting the ground rules for the new gTLD space.

---

[11] See http://www.icann.org/en/tlds/agreements/asia/appendix-s-06dec06.htm#6; http://www.icann.org/en/tlds/agreements/mobi/mobi-appendixS-23nov05.htm; http://www.icann.org/en/tlds/agreements/post/post-appendix-S-11dec09-en.htm.

[12] See preceding footnote.

COA is also pleased to see that ICANN has provided an alternative version of section 4.5 of the base Registry Agreement under which a TLD cannot be redelegated over the reasonable objection of the original delegate. This could be an important safeguard for brand owners who may be interested in experimenting with a .brand registry. These new TLDs will not be applied for if there is any risk that the TLD might be redelegated to a third party, perhaps even a competitor, if the brand owner later decided that the experiment has failed and the TLD should be phased out.

Section II : Economic Framework

The most significant document contained in the latest release is the "Economic Framework for the Analysis of the Expansion of Generic Top-Level Domains." See http://www.icann.org/en/topics/new-gtlds/economic-analysis-of-new-gtlds-16jun10-en.pdf. The document concisely and persuasively challenges a number of the premises underlying the way ICANN proposes to roll out new gTLDs. COA strongly urges ICANN to heed these challenges by giving top priority to making the course corrections needed to maximize the positive potential, and to minimize the risks, of the new gTLD rollout.

The first challenge is found on the very first page of the document: "An open-entry process may not lead to the socially-optimal number of new gTLDs." An "open-entry" process precisely describes the ICANN new gTLD framework: every application that meets baseline technical and financial criteria, subject only to very limited objections and to a method of resolving incompatible proposals through auctions, will be approved, without regard to whether the application offers any chance of benefit to the public interest, or any near-certainty of harm to it. In essence, ICANN has spent three years building a machine that will spit out new gTLDs at the end. This is an abdication, not a vindication, of ICANN's public interest obligations.

Second, on page 3, the authors of the Economic Framework study identify the likely "largest sources of potential benefits from the creation of new gTLDs." There are three such sources: community applications; IDN TLDs that "offer new benefits to specific user communities"; and "innovative new business models that are very different from those of existing TLD's registry operators." In other words, ICANN can best carry out its responsibilities by giving preference to certain categories of applications. The third category listed above surely needs more definition; but the clear message of the Economic Framework paper is that ICANN's top priority right now should be to refine and sharpen the boundaries of this category, rather than to tinker with its new gTLD machine, so that it can churn out more smoothly or quickly a host of socially useless, or even detrimental, new gTLDs.

Third, the Economic Framework study calls for ICANN to exercise judgment. It can shape its "application and evaluation processes [so that they] are most likely to lead to the introduction of gTLDs that promote social welfare and economic efficiency" (page 2). To this end, the authors take the initial steps toward identifying studies that " would lead to recommendations on how ICANN could craft its application process and ongoing rules to lessen

the likelihood of delegating gTLDs that will have negative net social benefits and to enhance the net social benefits from gTLDs that are designated." (page 62)

Fourth, the paper provides insights on two key aspects of the studies that are needed to achieve these goals. It singles out "the potential for consumer confusion" as a crucial factor for "deciding how quickly to proceed with the introduction of new gTLDs." (page 61) Moreover, it calls for research that aimed at "enumerating and quantifying the external costs of a gTLD, i.e., the costs that are imposed on parties other than the gTLD owner." Prominent among these external costs is the burden imposed on rights owners with regard to "costs of increased registration, monitoring and enforcement of trademarks across multiple gTLDs." (page 55-56) Perhaps it is ICANN's failure to carry out any such studies on the "externalities" imposed by new gTLDs that helps to explain why (as discussed below, in Section IV) it has failed to develop a strong and comprehensive set of tools for protecting the rights of third parties that could be jeopardized in the "open-entry" new gTLD environment.

In short, the Economic Framework paper is a major step forward on the "overarching issue" on which ICANN has appeared, up to this point, to be most stymied. COA hopes that ICANN will take this perspective to heart and look to the "Economic Framework" as the main roadmap for the path ahead. That map calls for giving top priority to analyzing "the expected costs and benefits of various types of new gTLDs," (p. 61) and then focusing on those "types" that offer the greatest promise. This is, no doubt, a change in course from the path ICANN has chosen to follow over the past few years; but it could lead to a much better result from the standpoint of the public interest.

It will no doubt be pointed out that it would have been much better to have had an "economic framework" to navigate by at the beginning of the process. While true, that should not provide an excuse for failing to take up the roadmap now. Whether to do so is the most important choice the Board faces when it meets September 24 on the topic of new gTLDs.

Section III: Malicious Conduct

COA's comments on the "Update to Explanatory Memorandum" on this topic, and on the "Draft Program Development Snapshot #2" for the High Security Zone TLD Advisory Group, are brief, for two reasons.[13] First, there have been no fundamental changes in the approach ICANN is taking to this critical issue. Second, most of COA's main concerns with that approach have already been referred to in Section I of these comments.

[13] See http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-memo-update-28may10-en.pdf and http://www.icann.org/en/topics/new-gtlds/hstld-program-snapshot-2-16jun10-en.pdf. The cover page to the "Update" document announces that the new gTLD program "is expected to launch in calendar year 2010." COA doubts that the ICANN staff would have chosen this low-key a method of announcing – even before the community had considered DAG v. 4 – its conclusion that all outstanding issues – whether overarching or not – will be satisfactorily resolved within the next 5 months. But since the statement is made, it would be helpful to eliminate the passive voice and to specify who it is that "expects" this rosy scenario to occur.

The "update" paper reviews the status of "nine recommendations …. from which controls that would reduce the potential for malicious conduct within gTLDs could be created." In most cases, the status is about the same as it was six months or a year ago. No timetable is provided for next steps in most cases – for instance, on the report of the SSAC working group on removal of orphan glue records. While COA supports the first eight recommendations, particularly with regard to a thick and fully searchable registry Whois, the real question is whether, if they were all implemented, they would, taken as a whole, reduce the potential for malicious conduct to a satisfactory degree. It seems to be too soon to answer that question.

The ninth recommendation – on a "Draft framework for high security zones verification" – also seems far from implementation. Clearly progress has been made by a hard-working advisory group, which "plans to publish an actionable program for community consideration and review," though there is no timetable set for doing so. But COA remains greatly concerned that this framework, even when made "actionable," will contribute little or nothing to the goal of "reducing the potential for malicious conduct," because it is completely voluntary, and no gTLD applicant is given any incentive within the application process for adopting any part of it.

The possible methods for providing that incentive are fairly obvious. The first option, as COA called for in its comments eight months ago, would for the High Security Zones Verification Program to be made mandatory, either for all new TLDs, or at least for a defined set of new TLDs that require a "high-confidence infrastructure," or that are determined to be at an unusually high risk of being the venue for criminal, fraudulent or illegal conduct, including but not limited to copyright piracy. COA offered then to work with ICANN staff to help develop a workable definition for this subset of new gTLDs. ICANN never responded to this offer, and its summary and analysis of comments on whether the program should be made mandatory simply states: "Currently, the resulting standards created by the HSTLD program will be voluntary in nature….. The overall position on the voluntary nature of the program may be subject to change, as the ICANN policy development process, through a multi-stakeholder, consensus based process, will ultimately decide the overall course of the HSTLD program." See http://www.icann.org/en/topics/new-gtlds/hstld-program-snapshot-comments-28may10-en.pdf.[14]

The second option, also pointed out by COA last November, would be to provide incentives to adopt these enhanced protections against malicious conduct, by giving an applicant who did so extra points in the evaluation process, or taking away some points from applicants who failed to meet these standards. ICANN staff's response on this point was, if anything, even less illuminating: "At this point, the community has not yet discussed incentives for the HSTLD program. These comments will be taken into consideration as a component of HSTLD program development." Id.

[14] Incidentally, this response repeats almost verbatim one made by the ICANN staff three months earlier. http://www.icann.org/en/topics/new-gtlds/summary-analysis-agv3-15feb10-en.pdf, at 40.

A third option, as described above, would be to give someone the role of objecting to any application for which, by its nature, the failure to provide enhanced protections would inappropriately expose some segment of the public to an unacceptable risk of harm. See the example of .kids, discussed in Section I-B-3 above. This is clearly in some ways a less desirable option than either of the other two, since it would delay to a later point in the process the elimination of new gTLD applications that carry with them excessive risk. COA, which first put forward this option in comments filed on April 8, 2010, urges ICANN staff to make some meaningful response to all three options. Until it does so, it is impossible to consider the "malicious behavior" overarching issue satisfactorily resolved, or even to state a realistic timetable for doing so.

Section IV: Rights Protection Mechanisms

This was the first so-called overarching issue in the new gTLD process to which ICANN stepped up. Sixteen months ago, the ICANN Board asked the Intellectual Property Constituency to convene what became the Implementation Recommendation Team (IRT), an extraordinary team of volunteers with a wide range of perspectives. The IRT, in a matter of weeks, hammered out a detailed, compromise position on some safeguards to help reduce the risks that the new gTLDs, while enriching speculators, cybersquatters, registry operators and registrars, would require trademark owners to increase geometrically their expenditures on defensive registrations, monitoring and enforcing their trademarks.

Had the IRT compromise recommendations been incorporated into the Applicant Guidebook, we might be closer to a satisfactory resolution than we are today. Instead, the IRT proposals were subjected to another round of high-velocity negotiations. The results, as COA noted in comments filed January 26, 2010, included provisions that were necessary to protect the rights of brand owners and the public interest in preventing consumer confusion in the new gTLDs, but fell far short of establishing mechanisms that were sufficient to achieve that goal.[15] Those insufficient mechanisms have now been incorporated, without significant change, into DAG v.4.

It was clear from the comments of ICANN senior staff at the Brussels meeting that no further major changes to the DAG v.4 on these issues will be seriously entertained. This is truly unfortunate. ICANN staff has taken to portraying the whirlwind of volunteer, cross-community efforts on this topic as a triumph of the bottom-up policy development process. This is not the case. The almost complete lack of support for the final outcome among the members of the community with the most at risk on the issue demonstrates that, to a disheartening extent, the process has been a failure. The real losers will not be trademark owners, but the consuming public, on whose interests in avoiding marketplace confusion and fraud the entire trademark system is based.

[15] See http://www.onlineaccountability.net/pdf/2010_Jan26_STI_Recommendations.PDF.

COA's concerns on this issue have been well documented in previous submissions. We understand that submissions from other members of the IPC will address in more detail the shortcomings of the provisions of DAG v.4 regarding rights protection mechanisms. At this stage we will simply note the following:

- The trademark clearing house falls far short because registries are not required to incorporate into their pre-launch RPMs protections for all trademark registrations of national or multinational effect.

- The refusal to extend clearinghouse-based RPMs beyond exact matches, or to incorporate any form of a globally protected marks list, means that the impact on reducing the volume of defensive registrations is likely to be negligible.

- The decision to make the clearinghouse-based mechanisms such as trademark claims services wholly voluntary for registries in the post-launch environment simply kicks the bulk of the abusive registration problem into a later time frame. In many cases the rights protection mechanisms will be wholly inadequate without these post-launch protections.

- The uniform rapid suspension system, while an important step forward, is unlikely to achieve its full potential, because it will , in many cases at least, be hardly faster than the UDRP, with weaker remedies, and without adequate protections against abusive registrants, such as a loser-pays system for cases brought against high-volume registrants.

- Finally, it is ironic that ICANN prepares to announce "mission accomplished" on RPMs just at the moment when its 'Economic Framework" paper calls for an objective study of the full costs to trademark owners of new gTLDs, taking into account monitoring and enforcement costs as well as defensive registrations. This should have been the first step in devising a sound and efficient system of RPMs, not an epilogue to a tale on which ICANN is about to close the book.

Section V. Vertical Integration

As a general matter, COA sees little need to relax the strict prohibition on common ownership of new gTLD registries and registrars that the ICANN Board adopted in Nairobi. In its view, the main significance of the ensuing and sometimes feverish debate on vertical integration lies in the attempt to define a category of single-user or corporate TLD – sometimes referred to as .brand – for which different treatment is appropriate.

For those companies that believe that there may be some positive value in establishing their brand online via a new ".brand" TLD – a category that, while it surely exists, may be much smaller than some in the ICANN community have convinced themselves it is – the outcome of these debates is critical. There is no evident reason why TLD registries in this category should be barred from controlling their own accredited registrar; from entering into exclusive arrangements

with an independent accredited registrar; or from dispensing with accredited registrars altogether, and allocating second level domains as they see fit. Defining the contours of this category will be a significant challenge. Whether ICANN meets it successfully could have a major impact on the viability of the new gTLD launch. COA looks forward to participating in that definitional process.

Respectfully submitted,

Steven J. Metalitz, counsel to COA
Mitchell Silberberg & Knupp LLP
1818 N Street, NW, 8th Floor
Washington, DC 20036 USA
Tel: +1 (202) 355-7902
Fax: +1 (202) 355-7899
E-mail: met@msk.com