The ICANN GNSO "Business Constituency"

Comments on New gTLD Board Committee Consideration of GAC Safeguard Advice

Status: FINAL
Version: 3
3-June-2013

Business Constituency Submission

GNSO//CSG//BC

Background

ICANN's new gTLD Board Committee has requested public comment on how it should address GAC advice to establish safeguards for categories of new gTLDs.

This document is the response of the ICANN Business Constituency (BC). While the BC includes a diverse range of businesses—including some who have applied for new gTLDs—these comments are solely from the perspective of business users and registrants, as defined in our Charter[1]:

> The mission of the Business Constituency is to ensure that ICANN policy positions are consistent with the development of an Internet that:
>
> 1. Promotes end-user confidence because it is a safe place to conduct business
> 2. Is competitive in the supply of registry and registrar and related services
> 3. Is technically stable, secure and reliable.

Introduction

The BC wishes to express its appreciation to the GAC and thank the government representatives for their significant contributions during the Beijing meetings. The BC recognizes the concentrated effort and long hours that the GAC invests in representing the public interest at ICANN.

The BC acknowledges earlier GAC contributions on new gTLDs, including: the 2007 GAC Principles; the April 2009 GAC letter to ICANN leadership; and GAC's Indicative Scorecard on new gTLD outstanding issues in the Cartagena Communiqué. The BC also notes that GAC advice has reflected many elements of the October 2012 Commercial Stakeholders Consensus Improvements to Rights Protection Mechanisms in new gTLDs.[2]

The BC especially appreciates the role played by GAC representatives from many of the world's fastest-growing Internet populations — including many businesses from developing economies. We applaud efforts to make these voices heard. Active participation by GAC members is crucial if ICANN is to maintain its central role in the global Internet community, and the BC looks forward to further close cooperation and collaboration with all members of the GAC.

The BC notes that since the GAC published its Beijing Communiqué, there has been extensive discussion within the community on this advice. The BC thanks the ICANN Board and its new gTLD Committee for allowing community input by opening a public comment period. This is a welcome initiative in keeping with ICANN's culture of multistakeholder interaction.

In the same spirit of ensuring all stakeholders are heard on key issues, the BC would encourage the GAC to hold some open meetings when working on documents such as GAC advice on policy issues. The BC thanks the GAC Chair for indicating this is possible to consider, in the Chair's recent video interview[3].

[1] Business Constituency Charter, at http://www.bizconst.org/charter.htm
[2] See http://www.bizconst.org/Positions-Statements/Consensus%20Improvements%20to%20RPMs%20for%20new%20gTLDs.pdf
[3] See http://youtu.be/I9hZCGnRh0I

Safeguard Advice for New gTLDs (Section IV.1.b. and Annex I of GAC Advice[4])

Safeguards Applicable to All New gTLDs

The GAC Advised that the following six safeguards should apply to all new gTLDs and be subject to contractual oversight.

1. ***WHOIS verification and checks*** *—Registry operators will conduct checks on a statistically significant basis to identify registrations in its gTLD with deliberately false, inaccurate or incomplete WHOIS data at least twice a year. Registry operators will weight the sample towards registrars with the highest percentages of deliberately false, inaccurate or incomplete records in the previous checks. Registry operators will notify the relevant registrar of any inaccurate or incomplete records identified during the checks, triggering the registrar's obligation to solicit accurate and complete information from the registrant.*
2. ***Mitigating abusive activity****—Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.*
3. ***Security checks****— While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.*
4. ***Documentation****—Registry operators will maintain statistical reports that provide the number of inaccurate WHOIS records or security threats identified and actions taken as a result of its periodic WHOIS and security checks. Registry operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request in connection with contractual obligations.*
5. ***Making and Handling Complaints*** *– Registry operators will ensure that there is a mechanism for making complaints to the registry operator that the WHOIS information is inaccurate or that the domain name registration is being used to facilitate or promote malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.*
6. ***Consequences*** *– Consistent with applicable law and any related procedures, registry operators shall ensure that there are real and immediate consequences for the demonstrated provision of false WHOIS information and violations of the requirement that the domain name should not be used in breach of applicable law; these consequences should include suspension of the domain name.*

BC Comments on Safeguards Applicable to All New gTLDs

The BC generally supports the six safeguards GAC has advised for all new gTLDs. Previous BC positions and statements have often called for Whois verification, prevention of registration abuse, stronger compliance enforcement, and rapid suspension of domains shown to be violating applicable law or terms of service.

Of the six safeguards above, the BC notes that many of the safeguards for Whois are already required of registrars under the final 2013 RAA (Registrar Accreditation Agreement). The BC recommends that ICANN staff evaluate the GAC safeguards and quickly identify all elements that are part of the 2013 RAA required of all registrars distributing domains in new gTLDs. Safeguards that are enforced as part of the RAA should not also be imposed on registries, except for circumstances where a registrar fails to comply with the RAA.

[4] http://www.icann.org/en/news/correspondence/gac-to-board-18apr13-en.pdf

Some BC members worry that implementing GAC safeguard advice would go beyond the requirements of the *Final Applicant Guidebook*. But the majority of BC members note that the registry agreement has designed a mechanism —in *Public Interest Commitments* – where applicants can add their commitments to implement safeguards such as the GAC has called for. Registries would therefore be bound contractually to adhere to those commitments and ICANN would be responsible for compliance enforcement.

The BC believes, however, that it would not be ideal for each new gTLD registry to have widely different implementation of safeguards that would be required across all new gTLDs. This diversity would be confusing for registrants and Internet users, and would make it difficult for ICANN to exercise its contractual compliance responsibilities.

Far better for ICANN to develop implementation specifications for common GAC safeguards, so that registries can voluntarily adopt them as part of their *Public Interest Commitments*. Standardized implementation of safeguards will benefit contract parties, registrants, users, and ICANN compliance. For example, the security checks safeguard (item 3 above) could be done effectively if ICANN designates approved security scanning software or vendors that registries could use to fulfill their safeguard commitment.

The BC notes that "applicable law" is a central concept in GAC Safeguards, but the scope of applicable law is not well understood by most registrants. To the extent possible, ICANN's Legal Department should provide guidance such that all stakeholders (users, registrants, contract parties, governments, law enforcement) can be informed about the scope of laws that would apply to a registrant's activity.

Finally, the BC recommends that ICANN develop standard procedures for suspension of domains as required in safeguard (3) Security Checks and safeguard (6) Consequences. The goal is to ensure that registries suspending a domain would not violate due process protections for registrants, under whatever is determined to be applicable law for such actions. The BC notes that suspension procedures might need to be expedited for TLDs and domains where there is immediate risk of fraud or abuse, such as in banking or critical infrastructure situations.

Safeguards for Category 1 gTLDs: consumer protection, sensitive strings, and regulated markets

The GAC Advises the ICANN Board: Strings that are linked to regulated or professional sectors should operate in a way that is consistent with applicable laws. These strings are likely to invoke a level of implied trust from consumers, and carry higher levels of risk associated with consumer harm. The following safeguards should apply to strings that are related to these sectors:

> *1. Registry operator will include in its acceptable use policy that registrants comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.*
>
> *2. Registry operators will require registrars at the time of registration to notify registrants of this requirement.*
>
> *3. Registry operators will require that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law and recognized industry standards.*
>
> *4. Establish a working relationship with the relevant regulatory, or industry self---regulatory, bodies, including developing a strategy to mitigate as much as possible the risks of fraudulent, and other illegal, activities.*

5. Registrants must be required by the registry operators to notify to them a single point of contact which must be kept up---to---date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self---regulatory, bodies in their main place of business.

BC Comments on Safeguards Applicable to Category 1 TLDs

The BC generally supports the five safeguards listed above for TLDs targeting areas of consumer protection, sensitive strings, and regulated markets.

In providing that support, the BC is assuming that Safeguard (3) requires notice to be provided in the registrant Terms of Service, describing the laws and industry standards applicable to the TLD. That interpretation treats Safeguards 1, 2, and 3 as applying to appropriate disclosure and notice of Terms of Service/acceptable use that apply to all registrants in the TLD.

The BC is not supportive of a requirement for registries to monitor security practices within each registrant's website and data operations, as required in safeguard (3). If a registry wanted to undertake that obligation—in satisfaction of GAC or government objections—it could add that obligation to the *Public Interest Commitments* of its registry agreement. In those cases, ICANN would be responsible for compliance enforcement.

However, the BC recognizes that certain strings pose a greater risk for exploitation, and supports GAC advice that a responsible approach to should be taken in response to GAC safeguard (3) and expects registry operators to implement responsible approaches which become part of the contractual terms and conditions.

Safeguards (1) and (3) above raise the same concern about "applicable laws" that was noted earlier regarding safeguards for *all* new gTLDs. The BC recommends that ICANN's Legal Department attempt to provide guidance such that all stakeholders (users, registrants, contract parties, governments, law enforcement) can be informed about the scope of laws that would apply to a registrant's activity.

With respect to Safeguard (4) above, the BC believes that working consultation with relevant regulatory and industry bodies, especially for the purpose of jointly developing harm mitigation strategies, will promote self-regulatory best practices that will improve consumer disclosure and protection.

Safeguards 6, 7 and 8, and on Related Advice Pertaining to Strings with Restricted Registration Policies

The GAC further advises the Board: In addition, some of the above strings may require further targeted safeguards, to address specific risks, and to bring registry policies in line with arrangements in place offline. In particular, a limited subset of the above strings are associated with market sectors which have clear and/or regulated entry requirements (such as: financial, gambling, professional services, environmental, health and fitness, corporate identifiers, and charity) in multiple jurisdictions, and the additional safeguards below should apply to some of the strings in those sectors:

> *6. At the time of registration, the registry operator must verify and validate the registrants' authorisations, charters, licenses and/or other related credentials for participation in that sector.*
>
> *7. In case of doubt with regard to the authenticity of licenses or credentials, Registry Operators should consult with relevant national supervisory authorities, or their equivalents.*
>
> *8. The registry operator must conduct periodic post-registration checks to ensure registrants' validity and compliance with the above requirements in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve.*

BC Comments on Safeguards 6,7, and 8 Applicable to Category 1 TLDs

The BC believes that safeguards 6, 7, and 8 are appropriate where the TLD creates a reasonable expectation in the mind of the average Internet user that registrants in that TLD are bona fide members of a regulated industry or profession.

For example, in the financial sector, .CASH and .MARKETS would not be likely to create such reasonable expectation, but .BANK and .CREDITUNION would. In the health and fitness sector, .DIET and .FITNESS have some governmental oversight, but other strings, such as .PHARMACY, .DENTIST, .DOCTOR and .HOSPITAL will clearly create such reasonable expectations. The responsibility of TLD operators to meet these GAC safeguards could be guided by Internet user expectations and governmental oversight.

The safeguards in this portion of GAC advice were designated for "*some of the above strings",* leaving the question of which of the many categories and strings would need to validate registrant credentials. The BC recommends that ICANN develop a list of TLDs in these categories where the string itself implies that it hosts domains mainly for regulated entities and/or licensed professionals. This list could be presented to the GAC, inviting GAC or governments to suggest additional strings for inclusion on the list.

Any registry needing to validate registrants—whether because their string is on this list or to satisfy government objections—could insert a validation process in the *Public Interest Commitments* of its registry agreement. At that point, ICANN would be responsible for compliance enforcement.

The aim of adopting the additional safeguards for strings connected to regulated industries is to assure that registrants are bona fide members of the regulated class and not entities that register domains to engage in fraudulent activities or that take unfair advantage of consumer expectations about registrants in such gTLDs. This would advance one of the most significant potential benefits for new gTLDs, which is to create trusted TLD spaces where consumers have greater protections against fraud and abuse by registrants.

The BC also believes that it would be highly beneficial for registry operators of such strings to establish Advisory Boards consisting of a balanced, international body made up of regulators, established trade

groups, consumer experts, and groups representing consumers from the affected market sector. Membership in the Advisory Board should be based on transparent and non-discriminatory criteria, and costs to create and maintain the Advisory Board should be borne by the gTLD registry.

A key responsibility of the Advisory Boards would be to establish registrant eligibility policies that conform to applicable laws and industry/professional standards. Another responsibility would be ensuring that the Registry Operator offers domains in a transparent way that does not give undue preference to any Registrars and Registrants, including itself, and does not subject Registrars or Registrants, or those they deliver services to as users, to an undue disadvantage.

The ability for a registrant to operate in a restricted access gTLD will likely be viewed by consumers as a demonstration of registrant validity – an 'approved member' of that industry/professional sector. So it is particularly important to have transparent and even-handed Registrant eligibility policies to minimize risks that a TLD operator could create competitive disparities among potential legitimate registrants.

Examples of such advisory groups exist in gTLDs today, such as IFFOR (International Foundation for Online Responsibility). Some country code TLD operators have also established similar approaches. The BC does not propose that ICANN itself dictate a model, but that registry applicants develop suitable approaches, based on the industry sector for their proposed registry application. The proposed approach should be subject to public comment.

The BC notes that these Category 1 safeguards reference "clear and/or regulated entry requirements" and "the registrants' authorizations, charters, licenses and/or other credentials" rather than the more general reference to "applicable law" of safeguards discussed above. Such credentials will generally be granted by the jurisdiction in which the registrant is domiciled. The BC also feels that appending "and common industry/professional standards" to the aforementioned phrase would provide for those situations where national law may not have kept pace with Internet growth and development, or where it is still evolving.

The BC notes that initial verification and validation of domain Registrant authorization, charter, license or other relevant credentials may be performed by Registrars and not by the Registry Operator. Typically, the Registry of record would establish such requirements for Registrars who serve their Registry and require a specific clause in a Registry/Registrar agreement.

In certain industry sectors, the expertise to provide this validation will be found among experts from within the sector, so the registry would be responsible to enlist experts to preform validation services for potential registrants. As an example, it is impossible for a general-purpose registrar to validate providers of content appropriate for children, should a child-oriented gTLD choose to allow only registrants displaying 'child friendly content'.

In those processes, as well as when a Registry Operator has reasonable doubt about the Registrant's credentials, initial verification and any additional consultation should take place with the supervisory authority for the jurisdiction in which the Registrant is domiciled.

Restricted Registration Policies: Exclusive Access

The GAC advises the ICANN Board: For strings representing generic terms, exclusive registry access should serve a public interest goal.

BC Comment on Exclusive Access

The BC supports this advice and puts forth several possible ways for ICANN to address the GAC's concerns.

First, ICANN could implement the remediation steps proposed by Australia in the GAC Early Warning submission from November 2012. Australia specifically urged that closed/exclusive gTLD applicants

> "should specify transparent criteria for third party access to the TLD…[that] should be appropriate for the types of risks associated with the TLD, and should not set anticompetitive or discriminatory conditions related to access by third parties."

Australia went on to urge that "these criteria should form part of any binding contract with ICANN," and "be subject to clear compliance oversight by ICANN".[5]

Second, ICANN should explore whether concerns about certain exclusive generics can be addressed by additional safeguards that essentially convert a "closed" gTLD to a "managed" gTLD. ICANN would need to create criteria to ensure that access to second level domain registrations are open to all qualified third party registrants who are not partners, affiliates or customers of the gTLD registry applicant. For example, in certain regulated areas, third parties holding a license or contract to provide services from a governmental regulatory body (and their customers and partners) should be provided with equal access to second level domain names in the new gTLD.

For all closed/exclusive gTLDs, ICANN should create policies that:

> (1) address antitrust and other anti-competition concerns;
>
> (2) minimize the risk of potential consumer confusion for users, who may not realize that the information, products or services promoted is provided via a closed or restricted registry;
>
> (3) appropriately and fairly define the class of potential second level domain name registrants;
>
> (4) prevent onerous and potentially anticompetitive registration fees; and
>
> (5) explore any necessary security and operational safeguards to minimize fraud, abuse and consumer complaints.

The BC further supports Australia's advice that all criteria and policies become part of a registry's binding contract with ICANN and that ICANN undertake compliance oversight over such activities.

An additional way that ICANN can respond to this element of GAC Advice is to clarify the process and criteria for obtaining exemptions consistent with the public interest, as permitted in the proposed *Registry Operator Code of Conduct*.

In public comments on "Closed Generic TLDs" in March-2013, the BC re-iterated prior positions supporting sponsored and community TLDs and flexibility for single-registrant TLDs to control domain names and bypass

[5] See https://gacweb.icann.org/download/attachments/27131927/Phone-AU-80942.pdf?version=1&modificationDate=1353431757000&api=v2

use of all registrars. In those comments the BC took no position on whether single-registrant TLDs should seek exemptions to the *Registry Operator Code of Conduct* in order to register its own domain names. At the time, the *Code of Conduct* included an exception allowing registration of names "*that are reasonably necessary for the management, operations, and purpose of the TLD.*"

In the April-2013 proposed final Registry Agreement, ICANN changed the base Registry Agreement to strike the exception above and replace with this new text:

> 1. In connection with the operation of the registry for the TLD, Registry Operator will not, and will not allow any parent, subsidiary, Affiliate, subcontractor or other related entity, to the extent such party is engaged in the provision of Registry Services with respect to the TLD (each, a "Registry Related Party"), to:
>
> > a. directly or indirectly show any preference or provide any special consideration to any registrar with respect to operational access to registry systems and related registry services, unless comparable opportunities to qualify for such preferences or considerations are made available to all registrars on substantially similar terms and subject to substantially similar conditions;
> >
> > b. register domain names in its own right, except for names registered through an ICANN accredited registrar that are reasonably necessary for the management, operations and purpose of the TLD; provided, however, that Registry Operator may (a) reserve names from registration pursuant to Section 2.6 of the Registry Agreement and (b) may withhold from registration or allocate to Registry Operator up to one hundred (100) names pursuant to Section 3.2 of Specification 5;

This new *Code of Conduct* limits a closed (or "exclusive") generic TLD to register up to 100 domain names for its own purposes. Any exclusive generic TLDs that wants to own more than 100 domains and/or avoid use of all registrars will therefore have to pursue an exemption to the *Code of Conduct*:

> 6. Registry Operator may request an exemption to this Code of Conduct, and such exemption may be granted by ICANN in ICANN's reasonable discretion, if Registry Operator demonstrates to ICANN's reasonable satisfaction that (i) all domain name registrations in the TLD are registered to, and maintained by, Registry Operator for its own exclusive use, (ii) Registry Operator does not sell, distribute or transfer control or use of any registrations in the TLD to any third party that is not an Affiliate of Registry Operator, and (iii) application of this Code of Conduct to the TLD is not necessary to protect the public interest.

The above exemption was part of the Final Applicant Guidebook, and the BC has often asked ICANN to clarify the process and criteria for obtaining this exemption. ICANN should develop criteria for determining whether giving an applicant this exemption would fail to "protect the public interest" as required by section 6 of the *Code of Conduct*. These criteria should be subject to pubic comment, including input from the GAC.

The BC has previously stated that "public interest" in the ICANN context should be narrowly defined to fit the limited scope of ICANN's mission. To that end, The BC has said that public interest should be measured in terms of the integrity and availability of registrations and resolutions.

In the process of defining the criteria for protecting the public interest, the ICANN community may conclude that public interest might *not* be protected if a TLD operator is allowed to retain up to 100 names for its own exclusive use. For instance, if the operator of a generic gTLD like .DRUGS were a drug producer or distributor, it could control most relevant categories if allowed to retain 100 second level domains for its own exclusive use. (allergy.drugs, sleep.drugs, pain.drugs, headache.drugs, etc.) In this example, competition authorities might object to allowing a single competitor to control 100 domains for its own exclusive use.

After the criteria for public interest test is defined, ICANN should then develop a process for TLD operators to seek the *Code of Conduct* exemption, including public comment and GAC participation.

These comments were prepared in accordance with the BC Charter.
The BC held extensive member discussions on this issue on May 1, May 8, May 10, and May 22.
Steve DelBianco acted as rapporteur and several BC members contributed content and edits.
Member review and approval began on 15-May-2013 and the present text was deemed approved on 3-Jun-2013.