

Comments on

New gTLD Board Committee Consideration of GAC Safeguard Advice

Status: DRAFT

Version: 1

15-May-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]](#footnote-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. iI technically stable, secure and reliable.

**Introduction** [Intro contributed by Ron Andruff and Andrew Mack]

The BC wishes to express its appreciation to the GAC and thank the governmental representatives for their significant contributions during the Beijing meetings.  The BC recognizes and acknowledges the hard work and long hours that the GAC invests in the ICANN process and the effort put into representing the public interest.  The strong set of recommendations put forward by the GAC in Beijing in the form of Public Interest Commitments Specifications (PICS) and safeguards help clarify –  and are major contributions to improving – the process as ICANN implements the new gTLD expansion.

Without wishing to single out any specific governments, the BC is especially appreciative of the role played by GAC representatives from the global south. These governments represent many of the world's fastest-growing Internet populations — including many businesses from developing nations — and 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 the GAC.

**Safeguard Advice for New gTLDs (Section IV.1.b. and Annex I of GAC Advice[[2]](#footnote-2))**

**Safeguards Applicable to all new gTLDs**

*The GAC Advises 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 frequently 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. Any safeguards that are enforced as part of the RAA should not be duplicated by also imposing them on registries.

Some BC members worry that safeguard advice goes beyond the requirements of the *Final Applicant Guidebook*, and should therefore be referred to a Policy Development Process. 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. The consequence of failing to add safeguard commitments could be objections from governments or the GAC, which provides an incentive for applicants to be responsive to GAC advice.

The BC believes, however, that it would not be ideal for each new gTLD registry to have widely different implementation of common safeguards. 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 noted that “applicable law” is an undefined term that should be explicitly defined. ICANN’s Legal Department should research and recommend a definition for “applicable law” such that all stakeholders (users, registrants, contract parties, governments, law enforcement) can be informed about what laws apply to a registrant’s activity. For instance, would the national laws of any Internet user be regarded as “applicable law” when that user visits a domain registered by someone in a different legal regime? If that’s the case, the Terms of Service shown to registrants should certainly highlight that risk and provide a link to an online resource describing all applicable national laws.

Finally, the BC recommends that ICANN develop standard procedures for suspension of domains called for 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.

**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 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 would not support a requirement for registries to monitor security practices within each registrant’s website and data operations. 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. ICANN would therefore be responsible for compliance enforcement.

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 provide a definition for “applicable law” such that all stakeholders (users, registrants, contract parties, governments, law enforcement) can be informed about what laws apply to a registrant’s activity. For instance, would the national laws of any Internet user be regarded as “applicable law” when that user visits a domain registered and based in a separate country? If that’s the case, the Terms of Service shown to registrants should certainly highlight that fact and provide a link to an online resource describing all applicable national laws.

[Ron Andruff] 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 further consumer disclosure and protection in the most effective and least burdensome manner.

**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**

[this section proposed by Ron Andruff] The BC supports safeguard measures 6,7, and 8 in order to allow new TLDs in these areas to proceed by showing that they meet the public interest responsibility and will implement GAC advice in a reasonable, responsible, and accountable manner.

The BC believes that such additional safeguards are appropriate where the string creates a reasonable expectation in the mind of the average Internet user that registrants in such string 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 responses of applicants could be guided by the level of Internet expectation and governmental oversight, in how they would satisfy GAC advice.

[proposed insert by Steve DelBianco]

The safeguards in this portion of GAC advice were for “*some of the above strings”,* leaving open the question of which of the many categories and strings would need to validate registrant credentials or licensing. 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.

[end of Steve’s insert]

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 may seek domain registrations to engage in nefarious activities or that take unfair advantage of consumer expectations about registrants in such gTLDs. This would fulfill one of the most significant potential benefits for new gTLDs, which is to create trusted top level name domain spaces in which consumers have greater protections against fraud and abuse by registrants.

The BC also believes that it would be highly beneficial for the 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 who represent consumers from the affected industry or profession, with membership based on transparent and non-discriminatory criteria.

A key responsibility of the Advisory Boards would be to establish registrant eligibility policies that adhere to applicable laws and common industry/professional practices to ensure that the Registry Operator administers access 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. As the ability for a Registrant to operate in such a restricted access gTLD will likely be viewed by consumers as a demonstration of registrant validity – an ‘approved member’ of that industry/professional sector – it is particularly important to have transparent and even-handed Registrant eligibility policies to remove any possibility that managers of regulated strings may seek to 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.

While the BC has reservations about the broad inferences that the phrase “adherence to applicable law” connotes, the BC feels that appending “and common industry/professional practices” 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 will in most cases 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 those processes, as well as in those instances where a Registry Operator has reasonable doubt about the Registrant’s credentials, both initial verification and validation and any additional consultation should take place with the supervisory authority for the jurisdiction in which the Registrant is domiciled in order to assure that the responsibilities imposed on Registrars and Registry operators are reasonable.

The BC recommends that the aforementioned verifications and validations be encoded in Registrant eligibility policies by the recommended Advisory Boards. Applicants should develop their own for their particular application to operate a string that is identified by the GAC as being in a regulated industry sector or a sector of concern.

**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** [proposed by Steve DelBianco]

The BC supports this advice and believes that one possible means for ICANN to address such concerns would be to build on the idea of remediation steps proposed by Australia in the GAC Early Warning submission from November, 2012. Australia specifically urged that various closed 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 to urge that “these criteria should form part of any binding contract with ICANN,” and “be subject to clear compliance oversight by ICANN.” See, e.g., <https://gacweb.icann.org/download/attachments/27131927/Phone-AU-80942.pdf?version=1&modificationDate=1353431757000&api=v2>

ICANN should explore whether concerns about certain closed 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 gTLDs, ICANN will need to 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 created criteria form part of a registry’s binding contract with ICANN and that ICANN take on compliance oversight over such activities.

1. Business Constituency Charter, at <http://www.bizconst.org/charter.htm> [↑](#footnote-ref-1)
2. <http://www.icann.org/en/news/correspondence/gac-to-board-18apr13-en.pdf>   [↑](#footnote-ref-2)