

Affirmation of Commitments Excerpt

9.3 Promoting competition, consumer trust, and consumer choice:

ICANN will ensure that as it contemplates expanding the top-level domain space, the various issues that are involved (including competition, consumer protection, security, stability and resiliency, malicious abuse issues, sovereignty concerns, and rights protection) will be adequately addressed prior to implementation. If and when new gTLDs (whether in ASCII or other language character sets) have been in operation for one year, ICANN will organize a review that will examine the extent to which the introduction or expansion of gTLDs has promoted competition, consumer trust and consumer choice, as well as effectiveness of (a) the application and evaluation process, and (b) safeguards put in place to mitigate issues involved in the introduction or expansion. ICANN will organize a further review of its execution of the above commitments two years after the first review, and then no less frequently than every four years. The reviews will be performed by volunteer community members and the review team will be constituted and published for public comment, and will include the following (or their designated nominees): the Chair of the GAC, the CEO of ICANN, representatives of the relevant Advisory Committees and Supporting Organizations, and independent experts. Composition of the review team will be agreed jointly by the Chair of the GAC (in consultation with GAC members) and the CEO of ICANN. Resulting recommendations of the reviews will be provided to the Board and posted for public comment. The Board will take action within six months of receipt of the recommendations.

CCT RT Terms of Reference Excerpts

1. The Affirmation of Commitments.

. . . . The goal of the CCTRT is to assess the impact of the expansion of the DNS marketplace on competition, consumer trust and consumer choice. In addition, this review shall examine the effectiveness of the application and evaluation process used for the 2012 round of gTLD applications, and the effectiveness of the safeguards enacted to mitigate issues involved in the introduction of new gTLDs. *The Program Implementation Review, a series of self-assessments examining the effectiveness and efficiency of ICANN's implementation of the New gTLD Program.* [note: this is a fragment that we should revise] The review defines effectiveness as, "to what degree the process (of

implementing the New gTLD Program) was successful in producing desired results/achieving objectives.” The CCTRT will analyze both quantitative and qualitative data to produce recommendations for the ICANN Board to consider and adopt.

3. Framework

a. Scope.

This review shall assess the New gTLD Program’s impact on competition, consumer trust and consumer choice. This includes reviewing the implementation of policy recommendations from the launch of the program through delegation and on to general availability. To conduct the evaluation, review team members may be asked to review data derived from processes related to the program, as well as broader inputs on marketplace indicators and consumer trends and feedback from the community.

*** Finally, the review will also consider the effectiveness of safeguards enacted to mitigate abuse. This is understood to include a review of the rights protection mechanisms that were implemented in the program, as well as other efforts to mitigate DNS abuse (such as the various Public Interest Commitments incorporated into Registry Agreements).

d. Definitions

Consumer: Generally refers to a natural person, acting primarily for personal, family or household purposes and may, depending on the context, include businesses and government agencies as well. For the purposes of this review, consumers generally fall into two categories: (i) Internet Users and other market participants who make use of domains through DNS resolution, such as by navigating to a URL or sending an e-mail; and (ii) Registrants (and potential registrants).

Consumer trust: The confidence Consumers have in the function, reliability, safety, security, and authenticity of the domain name system. This includes (i) trust in the consistency of name resolution; (ii) confidence by Internet users that they can safely navigate to a

domain name to find and safely use the site they intend to reach; (iii) confidence that a TLD registry operator is fulfilling the Registry's stated purpose; and (iv) confidence by a Registrant in a domain's registration process and life cycle.

Consumer choice: The range of meaningful options arising from new entrants and innovations over incumbent offerings available to Consumers for domain names (including in their preferred languages and scripts.)

Goals of New gTLD Program

In June 2011, ICANN's Board of Directors approved the Guidebook and authorized the launch of the New gTLD Program. The program's goals include enhancing competition and consumer choice, and enabling the benefits of innovation via the introduction of new gTLDs, including both new ASCII and internationalized domain name (IDN) top-level domains.

<https://newgtlds.icann.org/en/about/program>

Discussion Paper Topics [these are reordered]

Mandate issues:

Has the new gTLD Program promoted Consumer Trust in the Domain Name System?

Effectiveness of Safeguards enacted to mitigate issues involved in expanding gTLDs ***

- 1) Has the new gTLD program put mechanisms in place to improve trustworthiness in the DNS?
 - a) Mechanisms include: safeguards and Rights Protection Mechanisms
 - i) Safeguards include: safeguards based on GAC Advice incorporated into the 2013 Registry Agreement (specification 11: mandatory and voluntary Public Interest Commitments), Registrar Agreement and Registrant Agreement.
 - ii) Rights Protection Mechanisms include: **TBC**
- 2) Has the new gTLD program put sufficient mechanisms in place to mitigate risks to the trustworthiness of the DNS? **
 - a) Have the safeguards and Rights Protection Mechanisms been fully implemented [PROCESS] (to include GAC safeguards and technical safeguards)? (Laureen, Carlos, Calvin)
 - b) Have the new gTLD operators complied with the safeguards and Rights Protection Mechanisms? [PROCESS] (to include enforcement mechanisms as written and as enforced) (Fabro, Carlton, David)
 - i) What about non-compliance?
 - c) What was the impact of the new safeguards on DNS abuse? [IMPACT] [to include safeguards implemented via Spec 11 and voluntary PICs] (Drew, Fabro, Calvin, Carlos, Gao)
 - d) Did the new Rights Protection Mechanisms mitigate the risks involved with the expansion of the gTLD program? [IMPACT] [to include whether dispute resolution processes reduced TM infringement] (David, Jamie, Fabro, Carlos)
- 3) Have these efforts had an impact on public perception of the DNS?
 - a) What is the level of consumer (users and registrants) awareness of new gTLDs (Carlton, Gao, Calvin)

- b) Have consumers (users and registrants) expressed trust in the new gTLD program efforts? (Laureen, Gao, Carlos)
 - i) Do Consumers perceive value in the new innovations (e.g. validation)?
 - ii) Do Consumers perceive value in the risk mitigation initiatives (e.g. Safeguards, PICs, etc.)?
 - iii) Do Consumers have confidence in the implementation of the innovations and initiatives?
- c) Has consumer trust in the DNS improved overall since the introduction of new gTLDs?

Possible Consolidated Discussion Paper Topics w/subquestions

Mandate issue: Have new gTLDs promoted Consumer Trust?

- 1) To what extent, are consumers aware of the New gTLD Program? (Carlton, Gao, Calvin)
 - a. What are the levels of awareness of new gTLDs vs. legacy gTLDs?
 - b. What factors might have contributed to the levels of awareness?
 - c. Did ICANN have a role in promoting increased awareness by consumers of the New gTLD Program?
 - i. If so, what role
 - d. What steps might be necessary to expand/increase awareness?
 - i. What role should ICANN play?

- 2) Do consumers trust new gTLDs? (Laureen, Gao, Carlos)
 1. Why do consumers visit gTLDs?
 - a. Do consumers visit new gTLDs as much as legacy gTLDs?
 2. Do consumers trust new gTLDs as much as legacy gTLDs?
 - a. Do consumers trust certain specified gTLDs?
 - b. Why do consumers trust certain specified gTLDs?
 - i. What is the consumer expectation between the name of a gTLD and the content?
 3. Do consumers provide sensitive information (e.g., personally identifiable; financial or health information) to new gTLDs?
 - a. Compared to legacy gTLDs?
 4. Do consumers trust new gTLDs that offer domain names to:
 - a. Take precautions regarding who gets a domain name
 - b. Give consumers what they think they're getting
 - c. Screen individuals/companies who register for certain special domain names
 5. Do restrictions on who can purchase domain names contribute to consumer trust?
 - a. Do consumers expect restrictions on who can purchase new gTLDs?
 - b. Do consumers expect restrictions on who can purchase legacy gTLDs?
 6. Do consumers expect certain restrictions to be enforced?

7. What makes a gTLD trustworthy [text box]?
 - a. What factors contributed to trust?
 - i. How does navigation method impact trust?
 - b. What factors contributed to distrust?
8. Why do consumers avoid unfamiliar gTLDs [text box]?

Mandate issue: Effectiveness of safeguards enacted to mitigate issues involved in expanding gTLDs

4) Have the safeguards been fully implemented (to include GAC safeguards and technical safeguards)? (Laureen, Carlos, Calvin)

LK

1. [IDENTIFY RISK INTENDED TO BE MITIGATED] Have the GAC safeguards applicable to all new gTLDs been fully implemented?
 - a. WHOIS verification and checks and of same (directed to Registry operators)
 - b. Mitigating abusive activity (directed to Registry Operators)
 - c. Security checks
 - d. Documentation (inaccurate WHOIS and security threats)
 - e. Making and Handling Complaints
 - f. Consequences
2. Have the safeguards applicable to gTLDs that raise consumer protection concerns, contain sensitive strings, or contain strings in regulated markets been fully implemented? **Note: GAC directed responsibility for these safeguards to Registry Operators.**
 - a. Compliance with applicable laws (Registry Operators include in acceptable use policy that Registrants comply w/all applicable laws; Registry Operators require Registrars to notify Registrants of this requirement at time of registration)
 - b. Implement reasonable/appropriate security measures for collection of sensitive financial/health information
 - c. Establish relationship with relevant regulatory/industry bodies to mitigate risks of illegal activity
 - d. Require Registrants to have a single point of contact for complaint reporting and contact info for relevant regulatory bodies
3. Have the safeguards applicable to highly regulated gTLDs been fully implemented?
 - a. Verify/validate credentials
 - i. In case of doubt, consult with relevant authorities
 - ii. conduct periodic post--registration checks to ensure registrants' validity
4. Safeguards for gTLDs with inherent gov't functions (.army .navy; .airforce)?
5. Safeguards for gTLDs that may have increased risk of cyber bullying/harassment?
 - a. Develop clear policies to minimize risks of cyber bullying/harassment
6. Have the safeguards applicable to restricted registration policies been fully implemented? [perhaps also a Competition issue?]
 - a. Ensure registration restrictions appropriate for risks associated with particular gTLDs
 - b. Ensure registration restrictions are transparent

- c. Ensure registration restrictions do not result in either an undue preference or an undue disadvantage to registrars and registrants

CRG

Specification 11 has delimited some relevant “categories” of TLDs, in terms of their public interest impact.

Is this grouping appropriate?

Has this been an adequate process to implement safeguards and PICs? Should those considerations be officially added to the applicant's process so as to add predictability in subsequent rounds? Will they impact new applications?

CB

1. [IDENTIFY RISK INTENDED TO BE MITIGATED] Have the Technical safeguards applicable to all new gTLDs been fully implemented?
 - a. Have registry operators been technically vetted.
 - b. Has DNSSEC been deployed (and monitored).
 - c. Has Wild-carding been prevented.
 - d. Has orphan glue been appropriately managed.
 - e. Has Thick WHOIS been implemented.
 - f. Has centralised access to zone file data been implemented.
 - g. Expedited Registry Security Request (ERSR) Process.
 - h. Voluntary framework for high-security zones/High security top level domain-draft program development.

5) Have the new gTLD operators complied with the safeguards? [to include enforcement mechanisms as written and as applied] (Fabro, Carlton, David)

Fabro

What is ICANN's contract compliance role in enforcing safeguards involving gTLD registry operators in general?

Carlton (re: procedures to enforce safeguards)

[TIE ENFORCEMENT OF SPECIFICATION 11 TO RISK SPECIFICATION 11 SAFEGUARDS WERE INTENDED TO MITIGATE]

6) Did the new safeguards mitigate DNS abuse? [to include safeguards implemented via Spec 11 and voluntary PICs] (Drew, Fabro, Calvin, Carlos, Gao)

Safeguards and Abuse

Rate of Abuse

1. What is the rate of abuse in legacy gTLDs?

2. What is the rate of abuse in new gTLDs?

a. What factors appear to contribute to abusive registrations in new gTLDs?

i. Price?

ii. Common Registrar/Reseller?

iii. Overall popularity of the TLD?

iv. Restrictive terms of use?

3. What was the rate of abuse in legacy gTLDs upon the introduction of new gTLDs?

4. What has happened to the rate of abuse in legacy gTLDs since the introduction of the new gTLDs?

a. Has the overall rate of abuse dropped?

b. Has the overall number of abusive registrations dropped?

PICs

[CATEGORIZE THE PUBLIC INTEREST COMMITMENTS BY TYPE E.G. ALL GTLDS & SENSITIVE AND HIGHLY REGULATED GTLDS THAT INCLUDE VOLUNTARY PICs]

1. Which types of PICs were incorporated into the new gTLD program?

2. What restrictions were imposed by the PICs?

a. registrant restrictions

b. use restrictions

7) Did the new Rights Protection Mechanisms mitigate the risks involved with the expansion of the gTLD program? [to include whether dispute resolution processes reduced TM infringement] (David, Jamie, Fabro, Carlos)

(a) Were they used? How were they used?

(b) Did their existence deter infringers?

(c) Did they provide an effective solution to the overarching issue of trademark protection in the new gTLDs?

(d) Were other new gTLD RPMs introduced by Registry Operators (i.e. over the baseline of obligatory RPMs) effective?

(e) Did the availability of new RPMs cause an increase in the total number of complaints (URS/UDRP) being brought overall?

(f) If there was an increase in number of complaints (URS/UDRP) how did this compare to the total number of new domain name registrations across all gTLDs?

(g) Did the availability of these RPMs reduce TM infringement (by discouraging abuse)?

(h) What other enforcement measures were taken in addition to complaints (cease and desist, watching, lawsuits, increase registrations?)

(i) Did the launch of new gTLDs create an increase in enforcement costs for brand owners compared to pre-new gTLD status quo?

(j) What type of abuse is prevalent in new gTLDs?

1.Bad Faith Registration and Use

2.Malware

3.Phishing

4.Security breaches

(k) Has the rate of transfer or cancellation changed in the UDRP since the existence of new gTLDs?

(l) Has the TMCH functioned satisfactorily? Has there been abuse of it? What if anything should be changed?

(m) Has the URS functioned satisfactorily? Has there been abuse of it? What if anything should be changed?

(n) Has the PDDRP functioned satisfactorily? Has there been abuse of it? What if anything should be changed?

(o) Has the TM Claims Service functioned satisfactorily? Has there been abuse of it? What if anything should be changed?

(p) Has the Sunrise Period system functioned satisfactorily? Has there been abuse of it? What if anything should be changed?

(q) Has the Legal Rights Objection Mechanism functioned satisfactorily? Has there been abuse of it? What if anything should be changed?

(r) Has the String Confusion Objection Mechanism functioned satisfactorily? Has there been abuse of it? What if anything should be changed?

(s) Has the Community Objection Mechanism functioned satisfactorily? Has there been abuse of it? What if anything should be changed?