ICANN | GAC

Governmental Advisory Committee

Comments to "New gTLD Program Safeguards Against DNS Abuse[1]" Report

Note: This document was initially produced by the Governmental Advisory Committee (GAC)'s Public Safety Working Group. It was reviewed and endorsed by the GAC by written procedure on 19 May 2016 and constitutes GAC input.

The GAC recognises the critical importance of rigorous evaluation of the effectiveness of safeguards put in place to mitigate abuse in connection with the expansion of the top-level domain space. Confidence in the Domain Name System and its future expansion through further gTLD auctions is predicated on effective analysis and safeguards to mitigate current DNS abuse practices and ensure increased resiliency against future threats.

Vital to consumer trust is responsible oversight of domain operators and resellers through stringent vetting procedures, transparency around domain delegation through Thick WHOIS across the top-level domain space, open and comprehensive compliance processes, and handling of abuse complaints.

The GAC appreciates both the organized approach and significant research reflected in the "New gTLD Program Safeguards Against DNS Abuse" report ("Report"). The GAC suggests that the Report would be improved, however, if it included certain other safeguards that have been generated via the Governmental Advisory Committee, and ICANN contracts, policies, and multi-stakeholder group efforts. Accordingly, the Report should include:

1. Relevant provisions of the 2013 Registrar Accreditation Agreement (RAA)[2]:

   The 2013 RAA includes many DNS abuse mitigation tools, with improvements derived from the 2009 GAC Law Enforcement Due Diligence Recommendations, which can and should be used more effectively. The following RAA provisions provide useful ways to mitigate DNS abuse and should be stringently enforced through ICANN Contract Compliance:

   - Registrar's Abuse Contact and Duty to Investigate Reports of Abuse, Section 3.18;
   - Data Retention Specification;
   - WHOIS Accuracy Program Specification: To include implementation of Cross Field Address Validation. Per 2013 RAA, WHOIS Specification, Section 1 (e): Registrars are contractually obligated to "Validate that all postal address fields are consistent across fields (for example: street exists in city, city exists in state/province, city matches

[1] https://www.icann.org/public-comments/new-gtld-safeguards-dns-abuse-2016-03-15-en
[2] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa

postal code) where such information is technically and commercially feasible for the applicable country or territory."[3]

2. Registry Vetting and Comprehensive Audits:

   We recommend that the Report include data related to this requirement. Examples include the number of complaints that a registry received, how many resulted in a domain suspension, registries or registrars that had a high number of complaints – in relation to the total number of domains they control – or who showed a statistically significant variation from the norm, etc.[4]

3. Other Safeguards and Policies:

- Trademark Claims Service in the Trademark Clearinghouse
- Uniform Rapid Suspension System and UDRP (involving new gTLD abuse-related activities)
- Relevant policies and activities of registrars selling new gTLDs
- Data from industry collaboration and information sharing used to identify new gTLD domain names registered or used for abusive purposes
- New gTLD Applicant Guidebook
- WHOIS Policy Review Team Final Report and Staff implementation plan
- New gTLD Program Explanatory Memorandum, "Mitigating Malicious Conduct," 3 October 2009
- Registration Abuse Policies Working Group Final Report, May 2010
- ICANN Operations and Policy Research, "Reviewing New gTLD Program Safeguards Against DNS Abuse," teleconference proceedings, 28 January 2016

[3] Populated address fields are not the same as address fields that are validated. For US-based domains, the free USPS Web Tools® API provides a mechanism to validate US-based addresses. There are other paid services that provide address verification (e.g., SmartyStreets). There should be a feedback mechanism in place where public safety organizations can provide registrars examples of domains that had "validated" address fields but were still involved in domain abuse. Registrars would review and incorporate these findings into their validation process.

[4] https://www.icann.org/resources/pages/application-2012-02-25-en Per the ICANN Registrar accreditation process and consistent with the Report's Recommendation 1 – "Vet Registry Operators", ICANN should implement the same vetting requirements for all registries, consistent with the ICANN registrar process. In conjunction with this requirement, ICANN should conduct comprehensive audits on ALL accredited registries and registrars. ICANN should use all associated and derived revenues generated from the new gTLD program, to fund the extensive audit program. Moreover, ICANN should gather and publish results of the vetting process and audits to include the number of complaints that a registry received, how many resulted in a domain suspension, etc. Registries or registrars that had a high number of complaints – in relation to the total number of domains they control – who showed a statistically significant variation from the norm would receive a secondary review and/or face administrative penalties. There should be objective criteria to measure compliance.

4. Specific Studies to Assess Impact of Safeguards:

   The GAC further considers that the CCT-RT should not be constrained in scope to the nine safeguards, should it feel that new measures outside of those identified to be relevant to the mitigation of DNS abuse going forward and thus worthy of exploration, or that current safeguards require adjusting in light of contemporary practices.

   The GAC also notes that a significant portion of abuse is associated to issues of copyright-infringement. This is an issue which the report has not specifically addressed and which the CCT-RT will need to consider when examining the impact of new gTLDs on competition and consumer trust. It will be important therefore to include within the scope of the proposed review of safeguards an analysis of the available means to mitigate these forms of abuse.

5. Collaboration and awareness-building

   Relative to the question on "How do we ensure more focussed efforts on combating identified abuse?", the report should mention possible collaboration with renowned international security organizations like SANS, ISC2, ICANN Security, Stability and Resiliency Team, Interpol Cyber Security cell etc., in order to create awareness with regards to the new gTLD programme and possibilities of abuse.

6. Measuring the effectiveness of safeguards for TLDs

   In relation to the question on "How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?", the report should mention that "the analysis to measure the effectiveness of safeguards against DNS abuse should keep in mind the particular risk, threat and business profile of the gTLD in question". For example the risk profile for .bank and .pharma is likely to be more vulnerable as compared to .music or .amazon.

7. Other comments:
   It would be helpful to include references in the Report to additional existing and related studies / reports, for example:
   - DNSSEC related Reports from ICANN's SSAC (SAC 26, 29, 30, 35, 63) https://www.icann.org/groups/ssac/documents
   - Non-PDP Joint DNS Security and Stability Analysis Working Group Final Report https://ccnso.icann.org/workinggroups/dssa-final-08nov13-en.pdf