

At-Large Draft Report: New gTLD Program Safeguards to Mitigate DNS Abuse Workspace

Comment Close Date	Statement Name	Status	Assignee (s)	Call for Comments Open	Call for Comments Close	Vote Open	Vote Close	Date of Submission	Staff Contact and Email	Statement Number
2016/04/25	Draft Report: New gTLD Program Safeguards to Mitigate DNS Abuse	No Statement	n/a	n/a	n/a	n/a	n/a	n/a	Brian Aitchison brian.aitchison@icann.org	n/a

For information about this Public Comment, please click [here](#) >>

- [Comments Forum](#)

Brief Overview

Purpose: This draft report explores methods for measuring the effectiveness of safeguards against Domain Name System (DNS) abuse that were implemented as part of the New gTLD Program.

Current Status: The draft report is open for public comment.

Next Steps: Staff will collect, collate, analyze, and incorporate public comments into the next draft report upon close of public comment proceeding.

Section I: Description, Explanation, and Purpose

In accordance with section 9.3 of ICANN's [Affirmation of Commitments](#) (AoC) to promote competition, consumer choice, and consumer trust in the Domain Name System (DNS), this report is intended to aid the work of the review team on Competition, Consumer Choice, and Consumer Trust (CCT-RT). It will do so by:

- Providing an overview of the state of DNS abuse following the roll-out of the New Generic Top-Level Domain (gTLD) Program in January 2012
- Discussing options for measuring the effectiveness of nine safeguards put in place to mitigate DNS abuse in new gTLDs
- Proposing a research model to help assess the effectiveness of the nine safeguards in mitigating DNS abuse in new gTLDs

Section II: Background

In preparation for the potential expansion of the DNS, ICANN solicited advice from its expert constituencies to examine the potential for increases in abusive, malicious, and criminal activity in an expanded DNS and to make recommendations to pre-emptively mitigate those activities through a number of safeguards. The effort to identify steps for mitigating potential abuse began with posing four questions to experts in a diverse array of groups including the Anti-Phishing Working Group (APWG), the Registry Internet Safety Group (RISG), the Security and Stability Advisory Committee (SSAC), Computer Emergency Response Teams (CERTs) and members from the banking, financial, and Internet security communities. Those questions were:

1. How do we ensure that bad actors do not run registries?
2. How do we ensure integrity and utility of registry information?
3. How do we ensure more focused efforts on combating identified abuse?
4. How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?

After extensive consultations, the expert groups arrived at the following recommendations to address each issue area:

Question	Recommendation(s)
1. How do we ensure that bad actors do not run registries?	1. Vet registry operators through background checks to reduce the risk that a potential registry operator has been party to criminal, malicious, and/or bad faith behavior.
1. How do we ensure integrity and utility of registry information?	<ol style="list-style-type: none"> 1. Require Domain Name System Security Extension (DNSSEC) deployment on the part of all new registries to minimize the potential for spoofed DNS records. 2. Prohibit "wild carding" to prevent DNS redirection and synthesized DNS responses that may result in arrival at malicious sites. 3. Encourage removal of "orphan glue" records to minimize use of these remnants of domains previously removed from registry records as "safe haven" name server entries in the TLD's zone file that malicious actors can exploit.
1. How do we ensure more focused efforts on combating identified abuse?	<ol style="list-style-type: none"> 1. Require "Thick" WHOIS records to encourage availability and completeness of WHOIS data. 2. Centralize Zone File access to create a more efficient means of obtaining updates on new domains as they are created within each TLD zone. 3. Document registry- and registrar-level abuse contacts and policies to provide a single point of contact to address abuse complaints. 4. Provide an expedited registry security request process to address security threats that require immediate action by the registry and an expedited response from ICANN.
1. How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?	1. Create draft framework for a high security zone verification program to establish a set of criteria to assure trust in TLDs with higher risk of targeting by malicious actors—e.g. banking and pharmaceutical TLDs—through enhanced operational and security controls.

Measuring the effectiveness of these safeguards is a central aim of the work of the CCT-RT. To aid that work, this report presents an in-depth examination of each of these safeguards, proposes potential means to measure their effectiveness where possible, and puts forward a research model to analyze their effectiveness in a scientifically rigorous and comprehensive manner. Note that this report is meant as an *aid* to the CCT-RT. It is meant to offer *possible* methods and to provoke discussion within the team about how best to approach their study of DNS abuse and the safeguards put in place to mitigate it in the context of the New gTLD Program.

Section III: Relevant Resources

- [New gTLD Program Safeguards Against DNS Abuse Draft Report \[PDF, 1.17 MB\]](#)
- [New gTLD Program Explanatory Memorandum, "Mitigating Malicious Conduct," 3 October 2009](#)
- [Registration Abuse Policies Working Group Final Report, May 2010 \[PDF, 1.73 MB\]](#)
- [ICANN Operations and Policy Research, "Reviewing New gTLD Program Safeguards Against DNS Abuse," teleconference proceedings, 28 January 2016](#)

Section IV: Additional Information

Section V: Reports

Staff Contact

Brian Aitchison
brian.aitchison@icann.org

The final version to be submitted, if the draft is ratified, will be placed here by upon completion of the vote.

FINAL DRAFT VERSION TO BE VOTED UPON BY THE ALAC

The final draft version to be voted upon by the ALAC will be placed here before the vote is to begin.

FIRST DRAFT SUBMITTED

The first draft submitted will be placed here before the call for comments begins.