Reviewing New gTLD Program Safeguards Against DNS Abuse

ICANN Operations and Policy Research | 28 January 2016

Discussion Details

- **This discussion is being recorded.** Recordings and supporting materials will be published at http://newgtlds.icann.org/reviews.
- **Methods of participation:**
  - Adobe Connect + audio (Recommended)
  - Adobe Connect listen only + "Comments for Discussion" pod
  - Phone only + moderator polling
- **Providing input:**
  - Moderator will invite you to speak or read your comment from the "Comments for Discussion" pod.
  - Mute / unmute = *6 (dial star six on your phone)
  - Mute your line when not speaking. Don't use speakerphone.
  - State your name and affiliation prior to giving your input.
- **Chat:** Comments will not be read aloud. Use the "Comments for Discussion" pod to contribute to the dialogue.

Agenda

1	Introduction	(10 minutes)
2	Defining DNS Abuse	(15 minutes)
3	Measuring DNS Abuse	(15 minutes)
4	Measuring New gTLD Program Safeguards	(20 minutes)
5	Participant Experience with New gTLD Program Safeguards	(25 minutes)
6	Wrap Up: Next Steps and Methods of Additional Input	(5 minutes)

Topic 1: Defining DNS Abuse

Which activities do you consider to be DNS abuse?

If you could put forth a globally accepted definition of DNS abuse, what would it be?

This definition should be broad enough to cover various malicious uses of the DNS.

[15 minutes]

Topic 2: Measuring DNS Abuse – General

What are the most effective methods to measure the prevalence of abusive activities in the DNS?

[15 minutes]

Topic 3: Measuring New gTLD Program Safeguards

How do we measure the effectiveness of these safeguards? [20 minutes]

Safeguard	Rationale
Vet registry operators	To prevent “bad actors” from running registries
Require DNSSEC deployment	To minimize potential for spoofed DNS records
Require Thick WHOIS records	To ensure accuracy and completeness of WHOIS data
Prohibit “wild carding”	To prevent DNS redirection and synthesized DNS responses
Remove orphan glue records	To minimize use of remnant registry records as “safe havens” for DNS abuse
Centralize Zone file access	To allow more efficient access to updates on new domains as they are created within a zone
Document registry- and registrar-level abuse contacts and policies	To provide a single point of contact to address abuse complaints and to have a publicly-available description of their anti-abuse measures
Establish Expedited Registry Security Request Process (ESRP)	To address security threats that require immediate action by the registry and an expedited response from ICANN
Create a high-security zone verification program [NB: Not implemented as new gTLD safeguard; voluntary for registries]	To establish a set of criteria to assure trust in TLDs with higher risk of targeting by malicious actors through enhanced operational and security controls

Topic 4: Experience with Safeguards in New gTLDs

What has been your experience, personally or on behalf of an organization, with these safeguards?

- Which were effective? Ineffective?
  - How so?
  - Why do you believe they were or were not effective?

- Are there safeguards that you would suggest for consideration?

[25 minutes]

Wrap Up: Additional Input

Think of something else? Unable to fully express your ideas?

Use our questionnaire to provide additional input.
Responses must be submitted by Wednesday, 3 February at 18:00 UTC.

http://survey.clicktools.com/app/survey/go.jsp?iv=1fkefwusw9hjo

Want to know when the report has been published?

Send an email to brian.aitchison@icann.org with subject line "DNS Abuse Notification"

Engage with ICANN

Thank You and Questions

Reach us at:
Email: brian.aitchison@icann.org
Website: icann.org

twitter.com/icann

gplus.to/icann

facebook.com/icannorg

weibo.com/ICANNorg

linkedin.com/company/icann

flickr.com/photos/icann

youtube.com/user/icannnews

slideshare.net/icannpresentations