

For Council consideration: DNS Abuse Small Team Preliminary Findings on input received on bulk registrations

Background

On October 7, 2022, the “DNS Abuse Small Team Report to GNSO Council” [was published](#), taking into account input gathered from great part of the ICANN community, and raising a series of questions and recommendations for consideration, which fell into three categories:

- Issues that may benefit from GNSO policy development;
- Issues that may benefit from education/communication/outreach;
- Issues that may benefit from contractual negotiations between ICANN org and Contracted Parties.

The small team is pleased to note that some of the recommendations are already being considered and advanced by relevant parties, such as is the case of targeted contractual negotiations to mitigate DNS Abuse.

The issue of bulk registrations was one that was considered to need better context in order to be advanced, therefore, on January 6, 2023, the GNSO Council [sent a letter](#) on the subject to the RrSG, RySG, DNS Abuse Institute, and ICANN Contractual Compliance.

The following questions were asked:

- What information, evidence or complaint statistics can you share that can shed further light on the potential role of bulk registrations in DNS Abuse?
- Are you of the view that further work may be beneficial to address potential issues with bulk registrations in the context of DNS Abuse? If yes, please provide further details.
- What measures, if any, do registrars and/or registries have in place in relation to bulk registrations (examples might include, but are not limited to, additional checks adopted where registrations go above a certain threshold, and restrictions on bulk registrations from new accounts)? Are these found to be effective in constraining malicious actors? Would there be value in promoting the adoption of such measures on a voluntary basis, or should adoption through policy development be considered? Is there potential harm in the adoption of such measures?

Summary of feedback received on contractual negotiations

The CPH as a house (via Ashley Heineman and Beth Bacon) [responded](#) to concerns regarding potential gaps in the Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) DNS Abuse provisions. Regarding the RAA Section 3.18.1, the RrSG is currently attempting to address those issues within the existing text of the RAA through ongoing contractual negotiations with ICANN. As for the RA, the CPH noted that they do not believe there are any interpretation or enforceability gaps in relation to Specification 11(3)(a) and reiterated that the obligation was audited by ICANN Contractual Compliance in the most recent round of Registry audits. The CPH

stated that the pass-through provisions of Specification 11(3)(a) extend beyond DNS Abuse and include areas of website content abuse and fall outside the current efforts undertaken by the CPH to better address DNS Abuse. The CPH thanked the GNSO for their proactive steps in addressing DNS Abuse and noted that redline draft versions of the RA and RAA will be subject to a public comment period.

A relevant correspondence exchange [took place](#) in parallel to these between ICANN Board of Directors and the BC, IPC, and ALAC. The Board has stated that “Based on discussions with various constituencies at the recent ICANN76 meeting, the Board is considering coordinating a listening session once the proposed amendments are available for public comment. The listening session could include an overview of the proposed amendments. With that background, the community could begin a constructive discussion about what aspects may remain that could further benefit from Policy work, to help facilitate tangible next steps.”

Summary of feedback received on bulk registrations

ICANN Contractual Compliance (via Jamie Hedlund) [stated](#) that their agreements and policies do not have requirements or limitations related to bulk registrations. ICANN does not collect or track information on bulk registrations or any measures related to them. Complaints involving large numbers of domain names are addressed through the same process as those involving single domain names. ICANN Contractual Compliance enforces accuracy requirements for all relevant domain names within each complaint. Examples of complaints includes issues with renewal or transfer requests of entire portfolios, registration data inaccuracies for numerous domain names, and lists of domain names allegedly used to perpetrate abuse. However, statistics related to these complaints are not always available or provided to ICANN.

The RySG (via Alan Woods) has [responded](#) stating that it is difficult to comment on the potential role of bulk registrations without more specific information from the GNSO Small Team. The RySG notes that DNS Abuse management is a resource-heavy endeavor and that evidence-based escalation of DNS Abuse remains the preferred avenue for management and escalation processes at the registry level. The RySG remains committed to addressing any established vector for DNS Abuse and suggests that mitigation efforts based on an evidence-based approach are the most effective means of DNS Abuse management, regardless of the presence of bulk registrations. The RySG also notes that effective responses to domain generation algorithms (DGAs) have been based on existing and established anti-abuse escalation paths and that the success of such actions have hinged on highly responsive and effective involvement of targeted victim registries as part of international coordinated law enforcement actions.

The RrSG (via Ashley Heineman) [stated](#) that "bulk registrations" cannot be defined, tracked or used to measure DNS Abuse. The RrSG's DNS Abuse Sub Group suggested that other means should be used to address DNS Abuse, such as payment verification, IP address tracking, and personal relationships with customers. The RrSG also noted that restricting domain purchases or adopting policies for bulk registration might not be effective and may harm the diversity of business models.

The DNS Abuse Institute (via Graeme Bunton) also [notes](#) that “not only is there is no consistent definition of bulk registrations, there is no particular effort to define the concept clearly”. It furthermore notes that prior to any policy work, further research would need to be conducted to determine the scale of any potential issues as well as the role of bulk registrations as “it is difficult to determine definitively that works need to be conducted with regards to the role BDR plays in DNS Abuse”. The DNSAI concludes that “there are sensible and practical options available to registrars that will reduce DNS Abuse regardless of transaction volume right now. We should encourage their adoption, and endeavour to understand the landscape of bulk domain registration before committing to any particular solutions”. We would like to inquire about potential definitions to “bulk registration abuse” so that this can be put into better context.

Answer from the Small Team to Bulk registration letters

The Small Team would like to thank the timely responses received from the community and ICANN org. We have restarted deliberation on these matters and have come up with thoughts on the subject that we socialize on this letter.

- The general responses received were:
 - Complaints from single or multiple registrations are handled uniformly, without clarity on what might constitute bulk registrations warranting targeted reactions.
 - The lack of a clear definition did not elicit a clear response.
 - Other Know Your Customer tools are deemed more efficient in detecting potential abuse, and should warrant more attention.

ICANN’s recently started Inferential Analysis of Maliciously Registered Domains (INFERMAL) [project](#) seems to indicate a willingness from the org. to look into this matter and provide us with better statistics and intelligence. We have also heard from the colleagues at the DNS Abuse Institute that this could be on their radar.

Our preliminary conclusion has been that this does not fall within the realm of Consensus Policy at the moment. With the understanding that the above does not directly relate to policy, we appreciate the importance of other bodies taking these matters into consideration.