

Tucows public comment: Preliminary Issue Report on a Policy Development Process on DNS Abuse Mitigation

17 October 2025

Tucows welcomes the opportunity to comment on the Preliminary Issue Report on a PDP on DNS Abuse Mitigation ("Issue Report") and appreciates ICANN Org's work through the drafting process.

The Report covers a broad range of important topics and generally presents reasonable suggestions for next steps. Regrettably, this proposes one Charter for two topics which should remain separate, and assumes that a third topic should not go to PDP at all. Instead, **each of the three topics selected to be addressed at this time should be Chartered separately, and the work should be scheduled sequentially** rather than concurrently in order to ensure maximum availability across the ICANN Community and Org.

Tucows notes the hard work and dedication of the RRA Amendment Review Team, whose efforts resulted in the 2024 RAA and RA Amendments for DNS Abuse. **Tucows encourages ICANN Contractual Compliance to continue using the tools now available to them, and supports the definition of DNS Abuse formalized through those Amendments.**

Tucows supports the [RrSG's input on this Report](#), including that the topics should each be approached in a distinct and separate PDP, and that the representation model should be adjusted so that seats on the Working Group are equally distributed among Stakeholder Groups.

Tucows offers the following additional comments.

Discussion of the issue

Tucows notes with support the consideration in the Report of the importance of balancing prevention of DNS Abuse against the need to maintain an open and accessible domain name marketplace.

Tucows also notes that Personal Data must only be processed when there is a valid purpose and legal basis for the processing and, as such, any work to address DNS Abuse that includes

the processing of Personal Data must be clearly scoped and related to actual Abuse (not a preventative measure for Abuse that has not yet happened).

Unrestricted Application Programming Interface (API) access for domain name registration for new customers

Tucows agrees that this topic is appropriate to move forward as a PDP, while noting that each Contracted Party will be best suited to determine the specific types of friction for new users which would provide the greatest reduction in DNS Abuse while not unduly limiting access for good actors.

Associated Domain Checks

This practice is already common among Registrars and so Tucows supports it moving forward and being formalized. Tucows supports the RrSG's comments about the balance needed between specificity, flexibility, and generality so as to not give away too much info to bad actors. Any work on this topic must include consideration of privacy obligations and data protection standards, and **Tucows recommends that the Charter include a requirement that the WG perform a Data Protection Impact Assessment in addition to the planned Human Rights Impact Assessment.**

Limited coordination on Domain Generation Algorithm (DGA)-based abuse

Tucows supports work towards a clearinghouse of DGA domain lists as well as updates to the Security Response Waiver process and consideration of how to dispose of the DGA domains.

The Report determines that the DGA topic could move forward outside the ICANN policy development process; it is unclear why the same is not the case for the Associated Domain Checks topic. These two issues are equally well-suited for Community attention through the Policy Development Process.

Consideration of Gaps

Phase 0: Preventative Measures

P1: Unrestricted Access to Application Programming Interface (APIs) allowing for high-volume registrations

Tucows notes that the EPP is technically an API, so any work on this topic must be scoped appropriately.

Tucows supports the Report in saying that “This policy would need to differentiate between retail API access, and API access where a signed reseller agreement is in place” as an accepted reseller agreement is exactly the type of friction that would be needed.

Each Registrar will be best-suited to determine what type of friction or other measures are most appropriate to prevent inappropriate use of their own APIs. The suggestions from the NetBeacon report can be a starting point for discussion but should not be determinative on their own.

P2 and P3: Lack of Proactive/Timely Contact Verification

Tucows considers the current validation and verification processes to be effective and the current timeline to be appropriate in context of real-life user experiences.

If any consideration is to be made regarding adjustment of verification timing, there would first need to be a clear understanding of when the DNS Abuse occurs in relation to the verification process and whether verified or un-verified domains are more likely to be used in DNS Abuse.

The report mentions that some registrars did not perform full syntactic checks or complete operational validation; this should be addressed with ICANN Compliance as there are already relevant requirements in place.

P5. Minimal Deterrent Effect of Reactive Measures (“Uptime”)

Tucows supports the Report conclusion that this gap does not require further a specific solution.

P6. Challenges in Real-Time Detection of Short-Lived Abuse

Tucows supports the Report conclusion that this should be addressed outside policy work.

P7. Underuse of Predictive Algorithms for Early Detection

Tucows supports the Small Team’s note that “predictive algorithms may be useful but there is always the potential for false positives and the negative impact these may have on registrants” and agrees with the Report’s conclusion that this should be addressed through a non-binding best practices document.

P8. No Post-Registration Identity Checks for Suspicious Activity

Registrant identity and validation of the registrant’s information has not been shown to be a factor in identifying DNS Abuse. Tucows notes our recent publication “[Requiring registrants to show ID is a Bad Idea](#)” and does not consider any further policy to be needed in this context.

P9. and P10. Economic Incentives Prone to Abuse (P9 – Discounted Pricing and P10 – offering Free Services)

Tucows supports the Report’s conclusion that this be addressed by educational efforts. Tucows further supports the RrSG’s concerns about considering pricing within the ICANN Policy context.

P11. Limited Use of Abuse Feeds/Threat Data for Prevention

Tucows supports the RrSG’s input that requiring use of commercial block lists is not appropriate for Policy and should instead be considered as a best practice. Presence of a domain on a commercial blacklist is neither determinative nor conclusive but rather a single data point that may be considered when making a determination about the existence of DNS Abuse.

Phase 1 & 2: Abuse Reporting

A1. Unactionable Complaints to ICANN

Tucows appreciates the work of ICANN Contractual Compliance in filtering out unactionable complaints instead of forwarding them to us. Tucows supports the Report’s conclusion that this should be addressed through best practices and education rather than Policy.

A3. Malicious vs. Compromised – Clarifying Responsibility

Tucows supports the RrSG’s input on this topic.

Phase 3: Mitigation by Contracted Parties

C1. Limited Transparency in Mitigation Actions taken

Tucows supports the Report conclusion that although this could be addressed through policy development it is not a priority at this time and could be initially considered with non-binding best practices and community collaboration.

C2. No Requirement to Check for Associated Domains

Tucows supports this topic moving forward for Policy development in the context of maliciously-registered domains; this is already a common practice among registrars. Tucows notes that privacy and data protection principles must be considered and encourages the PDP WG to conduct a Data Protection Agreement as well as the planned Human Rights Impact Assessment.

C3. Lack of Standard Dispute/Recourse Mechanism for Registrants

Tucows suggests that all PDPs that have effects on registrants include consideration of recourse and dispute mechanisms available to registrants.

C4. Unregulated Subdomain Abuse

Tucows supports the RrSG input that this topic warrants further consideration but must not stray outside the Picket Fence.

C6 and C7. Due Diligence and Transparency in Mitigation

Tucows supports the Report's conclusion that further data is needed before the topic can be meaningfully addressed by the Community.

C8. Inconsistent Responses – Seeking Standardization

Tucows understands the Report's conclusion that pursuing non-binding best practices would be appropriate here but suggests instead that this should be addressed by offering education to those Abuse Reporters who are concerned about receiving different responses depending on the registrar or registry involved, which would cover the reasons why this is an expected and appropriate outcome.

Relation to other gaps in the DNS Abuse Small Team Matrix: E5 and E6. No Rapid Takedown Requirement (Desire for 24-hour response) and Lack of Feedback Loop

Tucows agrees that abuse reporting tools may offer further standardization but does not consider that this gap can be meaningfully addressed in policy work.

Phase 4: ICANN Compliance Enforcement

E2. No Clear Escalation of Sanctions for Recurring Non-Compliance

Tucows agrees with the Report's comment that it is unclear what additional intermediate penalties are envisioned and agrees that, while any further consideration of this topic would require policy work, it should not be prioritized at this time.

E3. Delayed ICANN Enforcement Actions

Tucows appreciates the work of ICANN Contractual Compliance and supports them in holding Contracted Parties accountable to our contractual agreements.

Community Collaboration

CC1. Lack of Coordination during Domain Generation Algorithm (DGA) Botnet Attacks

Tucows considers this topic appropriate for policy development work. As determined by the PDP WG, the outcome of the PDP could appropriately be further research and information, and should not be a revenue-generator for commercial blocklists.

CC2. No Mechanism to Update DNS Abuse Definitions (Periodic Review)

Tucows supports the current definition of DNS Abuse provided in the recently-amended RAA. No revisions are necessary at this time; if the DNS changes to the extent that a new form of Abuse emerges, it should be considered when relevant.

Relation to other gaps in the DNS Abuse Small Team Matrix: C5. Imposter Domain Names (Exact Matches to Trusted Names)

Tucows does not support further work on this topic in the context of DNS Abuse.

Data & Transparency

P4. Lack of Data on "Bulk Registrations"

Tucows notes that there are many reasons to register more than one domain at a time and agrees with the Report that "it may be difficult to identify objective factors that could flag when 'bulk registrations' may be intended for abusive purposes and there is a risk of impeding 'bulk registrations' for legitimate purposes." Tucows supports the Report's conclusion that this topic does not warrant a PDP on its own and will be addressed at least in part by the API PDP.

DT2. Lack of Empirical Research on Abuse Factors

Tucows supports the Report's note that a PDP working group on DNS Abuse may identify data that would be useful to collect for future consideration.

Conclusion

In order to successfully address concrete issues by creating Policy that will solve real problems, the Charter must be split up into three Charters for three separate, sequential "micro"-PDPs.

The representative model works only when it is truly representative; as such the Charter should be updated to ensure even numbers across Stakeholder Groups.

The Charter should be updated to include a requirement that the WG perform a Data Protection Impact Assessment in addition to the planned Human Rights Impact Assessment. Further, PDPs that have effects on registrants (all PDPs) should include consideration of recourse and dispute mechanisms available to registrants.

Tucows again thanks ICANN Org for their work drafting this Issue Report, and looks forward to reviewing the updated Charters.

Thank you,

Sarah Wyld
Head, Policy & Privacy, Tucows