ICANN | RrSG
Registrar Stakeholder Group

RrSG Public Comment: Preliminary Issue Report on a Policy Development Process on DNS Abuse Mitigation

18 October 2025

The Registrar Stakeholder Group welcomes the opportunity to comment on the GNSO Council's Preliminary Issue Report on a Policy Development Process on DNS Abuse Mitigation ("Report") and appreciates the time and work that went into drafting this Report.

Overall Input

Micro PDPs

The RrSG strongly believes that the selected topics should be approached separately, each with its own Charter and PDP. **The work should happen in sequence** rather than concurrently, to help ensure maximum participation from all groups, understanding that resources are tight.

Topics appropriate for Policy work

The RrSG notes per the Contracted Party House (CPH) DNS Abuse Working Group's public comment the three whitepapers recently published by the Contracted Party House on these topics and supports the information provided and conclusions reached within.

As discussed in the CPH whitepapers, these three topics are appropriate for policy development work:

- **API/Automated Registration Access:** With appropriate consideration of registrant rights and responsibilities, the RrSG supports policy development work towards establishing baseline obligations and controls that registrars should maintain over third parties who are authorised to access registrar platforms.
- **Associated Domain Checks**: While remaining in line with data access safeguards and privacy principles, the RrSG supports consideration of policy requiring accredited registrars to proactively investigate associated domain names, registrant accounts, and/or related orders when a domain under their management is conclusively found to

have been registered for malicious purposes (while not further victimizing customers found to have their domains compromised).
- **Domain Generation Algorithm (DGA)-based abuse:** The RrSG considers this appropriate for policy development, with work towards creation of a system available to the Community for the collection and distribution of DGA-based threat information, updates to the Security Response Waiver process, and consideration of how to dispose of the DGA domains.

Representation on the WG

The RrSG is concerned with ensuring that representation on these PDP Working Groups (as with all others) is appropriately balanced and that there is parity of representation from groups across the ICANN Community. The current draft Charter, however, provides for uneven representation across Stakeholder Groups, with most Stakeholder Groups allotted two seats on the Working Group but one Stakeholder Group allotted six seats.

While the representative model has its merits, it also causes problems of its own. ICANN policy development is meant to be multistakeholder and bottom up but limiting participation in PDPs erodes both of these principles and can mean that only the largest companies and most well-funded groups can engage in policy discussions.

For topics that impact the ICANN Community evenly, such as Latin Script Diacritics, it is acceptable to have the same number of representatives from each group. However, when a particular topic will have a greater impact on a particular group this model should be adjusted to ensure voices from the targeted group(s) are prioritized. For the recent Transfer Review PDP, additional registrars were allowed to participate to ensure diverse representation. When there will be a review of the UDRP, there should be additional seats for trademark owners to ensure their various viewpoints are considered.

In the context of these DNS Abuse PDPs it is crucial that registrars of different business models, geographies, and scales of operation are able to articulate their views and concerns, as the proposed PDPs will impact each business model (including wholesale, retail, and corporate registrars) in very different ways, and the additional dimension of a registrar's scale of operation and location can affect the types of DNS Abuse it faces; all of these factors also affect the types of mitigation strategies that are appropriate for that registrar.

Registrars have direct knowledge of and experience with DNS Abuse mitigation, including full understanding of the operational challenges involved in applying technical and organizational restrictions on a service. Registrars will ultimately implement the changes and requirements recommended by the Working Groups. Registrars will be responsible for ensuring that our namespaces remain free of DNS Abuse. Registrars will be held to account by ICANN Contractual Compliance for failing to comply with the implemented Recommendations.

If a representative model is chosen, the RrSG supports this only if that representation is even; if one Stakeholder Group has six seats then so should the other Stakeholder Groups. Alternatively, **if an open model is chosen, members of the RrSG stand ready to participate.** This will ensure that Registrar expertise and experience is included, that a broad range of Registrar business models is represented, and that the Stakeholder Group representation is even.

Discussion of Issues

Preventative Measures (Phase 0)

The RrSG supports the consideration in the Report of a balance between preventative measures towards security and the need for an open and accessible domain marketplace.

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

With appropriate consideration of registrant rights and responsibilities, the RrSG supports policy development work towards obligations and controls registrars must maintain over third parties that are authorised to access registrar platforms.

“API creates lower marginal cost for malicious actors…” and “malicious actors are highly price-sensitive” and “economic incentives, particularly when paired with automation, can increase vulnerability to abuse.” (p.5)

Comment: Gating of automated tools is reasonable to prevent abuse. Monetary barriers, however, are outside ICANN’s remit and must not be contemplated. That should be made explicit from the outset and not addressed later in the report as an afterthought.

“API access was linked to a 401 percent increase…” (p.13)

Comment: Gating measures will help but will not eliminate abuse. Criminals can and do replicate batch registrations through scripts or “human resources” (i.e., criminal 'crime-as-a-service' fulfillment networks, slavery). Expectations must be tempered: friction can reduce speed but it is not a silver bullet.

“The Netbeacon White Paper suggests that friction be implemented based on customer activity rather than customer identity. Friction based on activity (e.g., how old is the account and has it had reports of abuse) is suggested to be more robust, reliable, and easier to implement than attempts at customer verification” (p. 5)

Comment: The RrSG supports this approach and notes that each registrar is best suited to determine the type of friction that will ensure its customer base will maintain a high-quality namespace. It is only practical and possible to glean intent from actions actually taken.

P2 and P3: Lack of Proactive/Timely Contact Verification

"Some tested registrars did not fully perform syntactic checks…" (p. 14)

Comment: SSAC should be invited to provide or endorse tools for those basic syntactic checks (email and phone formats per RFC). Alternatively, the RrSG could share references to trusted open-source tools. Additionally, tested registrars found to be violating ICANN requirements should have been referred to ICANN Contractual Compliance.

P5. Minimal Deterrent Effect of Reactive Measures ("Uptime")

The RrSG agrees with the Report's conclusion that "this gap does not appear to warrant any specific solution".

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

The RrSG agrees with the Report that "combating short-lived DNS abuse requires a multi-layered approach" and should be approached holistically and outside of Policy.

P7. Underuse of Predictive Algorithms for Early Detection

The RrSG agrees with the Report that, "[g]iven the technical nature of this issue, it does not appear best suited for ICANN policy. A more feasible path might be inclusion in a non-binding best practices document."

P8. No Post-Registration Identity Checks for Suspicious Activity

"The Commercial Stakeholders Group (CSG) added this gap noting that after domains are registered, if they start showing patterns of abuse (e.g., multiple abuse reports or being added to blocklists), there is no policy requiring re-validation of the registrant's identity or information." (p. 17)

Comment: The RrSG notes that it is current practice to conduct some level of review when addressing Abuse reports, which can trigger further in-depth review of contact data as appropriate. The topic will also be addressed at least in part during the Associated Domains Check PDP.

That said, this identified gap blurs the line between contact detail verification and identity review. That distinction must remain clear: registrars can check contactability but are neither mandated nor equipped to provide identity verification.

Further, “multiple abuse reports” is a vague metric—”multiple substantiated abuse reports” could help prevent targeted attempted takedowns of non-abusive domains, competitive harassment upon legitimate registrants or other weaponization of such requirements.

Finally, the RAA already requires re-verification in specific circumstances; "start showing patterns" is not clearly defined and too subjective, and somewhat unnecessary as Registrars are already required to act on actionable abuse reports.

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

The RrSG agrees with the Report that “These ‘abuse side-effects’ based on the above description might be best addressed by building awareness and ultimately left with the contracted party to decide.”

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

The RrSG agrees with the Report that requiring use of commercial block lists is not appropriate for Policy.

Commercial blocklists often operate on a “better safe than sorry” principle, blocking domains suspected of malicious use without evidence, or blocking all newly-registered domains. They can be used to inform Registrar reviews but presence of a domain on such a list cannot be conclusive or determinative.

Further, most commercial block lists are designed to filter email or web traffic—not to combat Abuse, but to address symptoms of Abuse as they appear in a given medium. It is wholly inappropriate to use a commercial block list for a purpose for which it was not designed. For example, commercial block lists often include any domain or IP address used for sending bulk email, legitimate or otherwise.

Some block lists will include a domain name based upon a single user's report, without review or screening to ensure the reporter has correctly typed the domain, much less that there is any actual activity to merit listing it. The registrant experience when their domain name is misidentified by commercial blocklists is the disruption of legitimate service and a difficult appeal or removal process where they are even available.

Any suggested use of commercial block lists should be, at most, considered as a data point for use in review of abuse reports among other signals. It would be otherwise irresponsible and disruptive to treat blocklists as a takedown requirement without contracts that hold them to account on misidentification and standards of practice.

Abuse Reporting (Phases 1–2)

The RrSG agrees with the Report that “reporting-phase issues are largely about communication and ensuring the system to alert abuse is efficient” (p. 23) and is open to consideration of further Abuse reporting processes.

A1. Unactionable Complaints to ICANN

The RrSG appreciates ICANN Contractual Compliance’s efforts in filtering out unactionable or inappropriate complaints and supports educational initiatives on this topic.

A3. Malicious vs. Compromised - Clarifying Responsibility

The RrSG notes that this distinction between malicious and compromised domains is complex and sometimes impossible to determine. It may be more useful to refer to “fraudulent” registrations, as “malicious” implies a level of intent which we cannot determine while “fraudulent” relates to a demonstrated behavior and we can base processes and policies around it.

Taking Action on DNS Abuse (Phase 3: Contractual Obligations)

The RrSG reiterates our support for the 2024 DNS Abuse amendments to the RAA and base RA and reminds the community that we asked for and voluntarily negotiated these contractual commitments with ICANN directly in order to ensure that ICANN Contractual Compliance had the tools it asked for to shut down registrars refusing to combat DNS Abuse.

C1. Limited Transparency in Mitigation Actions taken

As a start, the Community should consider nonbinding guidance and best practices for abuse reporting. This would be a start down the path of broader transparency while permitting policy development work to focus on more high-impact areas.

C2. No Requirement to Check for Associated Domains

The RrSG acknowledges that the practice of performing associated domain name checks could indeed help address the gap identified by the GNSO Small Team. This topic is therefore a legitimate candidate for consideration within the Policy Development Process.

That said, initial discussions among stakeholders have brought to light the considerable complexity of codifying this practice into a policy that is both clear and enforceable. A range of variables are typically considered when identifying associated domains in the context of abuse reports, including: account holder details, use of resellers, IP addresses, payment methods, email addresses, phone numbers, however the circumstances dictate what is useful and each report can lead to different data being relevant for review. The feasibility and usefulness of implementing such checks also depends on factors such as the registrar's business model (retail, reseller-based, etc.) and the structure of the domain registration (direct or via multiple intermediaries).

Moreover, any resulting policy would need to strike a delicate balance: it must be specific enough to be enforceable by contract, flexible to accommodate for situations requiring different types of review, and sufficiently general so as not to inadvertently serve as a blueprint for malicious actors seeking to evade detection.

The RrSG believes the Community and the Working Group in particular should be empowered to assess whether a Policy is the most appropriate and effective mechanism to address the identified issue. While not opposing further exploration within a PDP framework, the RrSG wishes to underscore the above challenges at the outset.

Finally, the RrSG also notes that, should the WG determine that a Policy is not feasible or effective, the development of a best practices document or an ICANN advisory, particularly with respect to registrar obligations under section 3.18 of the RAA in the context of Abuse investigation, could represent a constructive and pragmatic alternative in the ongoing effort to combat DNS Abuse.

The Charter for this PDP must include consideration of data safeguards and privacy principles. This could be done by adding the question: "How are privacy rights and data security accommodated in this investigation?"

C3. Lack of Standard Dispute/Recourse Mechanism for Registrants

The RrSG agrees that this topic warrants further consideration to allow for appeals and also agrees that it should not be part of the initial set of PDPs undertaken on this topic (out of scope). The topics that will move forward for work at this time should include support for appropriate recourse where relevant.

C4. Unregulated Subdomain Abuse

The RrSG agrees that this topic warrants further consideration but is concerned about straying into the area of content moderation. The RrSG agrees that this need not be part of the initial set of PDPs undertaken on this topic.

C6 and C7. Due Diligence and Transparency in Mitigation

The RrSG agrees that this is not a gap in DNS Abuse mitigation itself and does not require policy development work at this time.

C8. Inconsistent Responses – Seeking Standardization

The RrSG notes that the flexibility allowed for in the amended ICANN contracts was deliberate, intentional, and necessary to ensure that Contracted Parties have the ability to take appropriate action depending on the circumstances. As such, this topic does not require further policy development; however, best practices could be useful.

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

The RrSG agrees with the Report that best practices towards a standardized approach may be useful.

Enforcement by ICANN Contractual Compliance (Phase 4)

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

The RrSG agrees that any adjustment in this area would require Policy development work and should not be prioritized over the other topics currently at hand.

E3. Delayed ICANN Enforcement Actions

Community Collaboration (Cross-Cutting)

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

The RrSG considers this appropriate for policy development, with work towards creation of a system available to the Community for the collection and distribution of DGA-based threat information, updates to the Security Response Waiver process, and consideration of how to dispose of the DGA domains.

The report suggests this could be addressed outside contractual requirements (p.33). The RrSG is concerned that this topic is being singled out for treatment as a non-binding best practice

while others are pushed to policy and does not agree that this is appropriate. We recommend a full PDP on this topic.

The RrSG further notes that DGAs and botnets should not be conflated. While Generative AI has enhanced the ability to algorithmically generate domain names, the use of domains for Botnets has dropped. Spamhaus now reports on IP addresses rather than domains, demonstrating this shift in usage trends. Coordination on DGA-based threats is valuable but should focus on malicious use as it occurs in the world rather than an expectation of Botnets.

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

The RrSG recognizes the diligence and commitment of the team working on the DNS Abuse Amendments to the RRA and Base RA. The RrSG is open to review where attributes of DNS Abuse clearly and objectively have changed and evolved away from the current definitions, while staying within ICANN's remit, and measuring emerging vectors against those attributes. For domain misuse not within ICANN's remit, the RrSG is not supportive of expansion of the Picket Fence. In any event, this should not be prioritized over the other topics discussed above.

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

The RrSG agrees that not everything requires policy work and that other approaches should be considered.

Data & Transparency (Cross-Cutting)

P4. Lack of Data on “Bulk Registrations”

The RrSG agrees with the Report that “the lack of data does not warrant a PDP topic on its own; note, the API/friction issue is intended to at least partially address “bulk-registration” abuse.” (p. 36)

DT2. Lack of Empirical Research on Abuse Factors

The RrSG stands ready to support ICANN if ICANN decides to gather more data on this topic.

Considerations for a PDP

The RrSG strongly believes that each topic should be approached separately, on its own merits, with its own Charter and PDP WG. The work should happen in sequence rather than concurrently, to help ensure maximum participation from all groups and allow for careful and thoughtful consideration and focus, with the understanding that resources of all stakeholders are tight.

Possible Impact on Human Rights

The RrSG strongly supports that the PDPs resulting from this Issue Report, and all future PDPs, include a Human Rights Impact Assessment (HRIA). As documented on the ICANN Wiki, "one of ICANN's core values is respecting internationally recognized human rights as required by applicable law" and conducting an HRIA as decisions are made will help ensure that fundamental human rights are considered and respected.

Specific questions to be considered in a possible PDP

For the API topic, the Charter must ensure the WG focuses on APIs that are used for registering domains rather than for other aspects of portfolio management or the EPP interactions between registry and registrar. The RrSG supports the questions noted in the CPH White Paper on the same topic.

For the Associated Domains topic, the Charter should be updated to include consideration of data safeguards and privacy principles. This could be done by adding a question: "*How are privacy rights and data security accommodated in this investigation?*" Further, as noted above the circumstances of each individual Abuse report investigation will dictate what is useful and each report can lead to different data being relevant for review. How will the requirements to check associated domains be enforced, and what kind of evidence will be expected?

Regarding DGAs, the RrSG believes that this issue is appropriate for a PDP. The CPH white paper on the topic offers the following questions for consideration which the RrSG supports:

- Should there be a centralized coordinating role within the ICANN community to perform the collection and distribution of DGA-based threat information to help protect the security and stability of the DNS? Can this be performed in a manner which respects regulatory constraints on data collection, distribution, retention and destruction?
- While the SRW is an established process and works for individual requests, are there ways to enhance the issuance process when an imminent threat to the security and stability of the DNS impacts several gTLDs?
- Should a registrar receive relief when a sponsored domain name is suspended or sinkholed by a gTLD registry pursuant to a DGA-based threat notice? If so, what type of remedies?
- Are there mechanisms for appeal where a registrant's legitimate domain is impacted by false identification?

ICANN | RrSG
Registrar Stakeholder Group

Draft Charter

The RrSG again strongly suggests that each of these three topics must be handled as a distinct "micro"-PDP, with its own Charter and schedule. This will allow the dedication of adequate policy resources to each topic in succession, making it easier for the Community to carefully consider each topic and participate. The proposed single PDP model is ill-suited to the three subject matters at issue while the "micro"-PDP approach will lead to agile solutions, improved focus, and efficiency. **The goal must be targeted PDPs producing straightforward outcomes with near-term operational effect** (see p.38). **The Charter must be divided into multiple Charters accordingly** (p. 48).

The RrSG is concerned that whatever PDP model is selected (representative or open) needs to be even and balanced among groups. The current draft Charter provides for uneven representation across Stakeholder Groups, with most Stakeholder Groups allotted two seats on the Working Group but the Commercial Stakeholder Group allotted six seats. This is inappropriate and should be adjusted to ensure even representation across Stakeholder Groups or open membership.

The RrSG stands ready to participate in these three PDP Working Groups and looks forward to reviewing the revised Charters.

Thank you,

Owen Smigelski
Registrar Stakeholder Group Chair