

Public Comment Summary Report

Preliminary Issue Report on a Policy Development Process on DNS Abuse Mitigation

Open for Submissions Date:
Monday, 08 September 2025

Closed for Submissions Date:
Saturday, 18 October

Summary Report Due Date:
Monday, 17 November 2025

Category: Policy

Requester: Generic Names Supporting Organization (GNSO)

ICANN organization contact(s): policy-staff@icann.org

Open Proceeding Link:
<https://www.icann.org/en/public-comment/proceeding/preliminary-issue-report-on-a-policy-development-process-on-dns-abuse-mitigation-08-09-2025>

Outcome:

On 14 August 2025 the GNSO Council requested an Issue Report on DNS Abuse Mitigation based upon the DNS Abuse Small Team [Report](#) from July 2025. ICANN org delivered the Preliminary Issue Report on 8 September, and the community was invited to comment on the identified issues and draft charter.

The Preliminary Issue Report received 27 comments from across the ICANN community. ICANN Org will consider all comments submitted and update the Preliminary Issue Report where necessary. Once the Final Issue Report is ready, it will be shared with the GNSO Council for their consideration.

Section 1: What We Received Input On

This summary report presents an overview of the Public Comments received on the Preliminary Issue Report on DNS Abuse and provides a record of community input across all issue areas identified in the report.

There is overall support for pursuing focused policy development on two priority topics: unrestricted API access for high-volume registrations and Associated Domain Check. Both were viewed as having the most immediate potential to reduce systemic DNS abuse. Most commenters also supported continued exploration of Domain Generation Algorithm (DGA)

coordination, though with varying opinions about whether it should proceed as consensus policy or as a best-practice initiative. In parallel, many commented on the Policy Development Process (PDP) structure and preferred individual PDPs for each topic instead of one PDP for both topics.

Commenters also raised other issues identified in the report, mentioning topics they think should be considered for subsequent PDPs or not prioritized at all. “Verification of Contact Data” and a “Recourse Mechanism” have been noted as other priority topics for subsequent PDPs.

Section 2: Submissions

Organizations and Groups:		
Name	Submitted by	Initials
Messaging, Malware and Mobile Anti-Abuse Working Group	Amy Cadagin	M3AAWG
Fraudkillers.org	Steven Tenny	Fraudkillers
CleanDNS	Chris Lewis-Evans	CleanDNS
Non-Commercial Stakeholder Group	Mesumbe Tomslin Samme-Nlar	NCSG
Contracted Party House	Sue Schuler	CPH
Ministry of Electronics and IT, Government of India	Pradeep Verma	Government of India
Registries Stakeholder Group		RySG
Identity Digital Inc.	Catherine Paletta	ID
Registrar Stakeholder Group	Zoe Bonython	RrSG
At-Large Advisory Committee		ALAC
Tucows	Sarah Wyld	Tucows
Namecheap, Inc.	Owen Smigelski	Namecheap
Intellectual Property Constituency	Margaret Milam	IPC
Ethereum Name Service (ENS) Labs	Alexander Urbelis	ENS Labs
Public Interest Registry	Elizabeth Bacon	PIR
NetBeacon Institute	Graeme Bunton	Netbeacon
INTA	Lori Schulman	INTA
Business Constituency	Business Constituency	BC
Meta Platforms, Inc.	Mia Brickhouse	Meta
DNS AXE	Mark William Datysgeld	DNA Axe
Governmental Advisory Committee	Fabien Betremieux	GAC
.au Domain Administration Limited	Jordan Carter	auDA

Individuals:		
Name	Affiliation (if provided)	Initials
Sourena MAROOFI		SM
Isaac OMAR		IO
Nick WENBAN-SMITH	Nominet UK	NWS
Maciek PIASECKI	ICANN Fellowship	MP
Raffaele SOMMESE	University of Twente	RS

Section 3: Summary of Submissions

The Preliminary Issue Report on a PDP on DNS Abuse Mitigation received twenty-seven (27) comments during the Public Comment period. ICANN received input addressing three principal aspects of the DNS Abuse Issue Report:

- a. The scoping of the identified issues, including views on which issues warrant policy development and how they should be framed;
- b. Suggested additional charter questions and considerations to guide the work of a potential PDP; and
- c. Proposed solutions and implementation approaches as proposed by the commenters or Public Comment input.

This Public Comment Summary Report organizes and discusses the community feedback according to these three broad areas of input where relevant.

Issue 1: Unrestricted Advanced Programming Interface (API) for high-volume registrations

Scoping: Most commenters support moving forward on “unrestricted API access” as a policy topic, with 15 submissions recorded as supporting the recommendation as written. One commenter, SM, asks to clarify what “large volumes” means and “to consider the potential for bad actors to operate across many registrar accounts, which would complicate detection thresholds that reinforce the call for careful scoping and measurable objectives.”

Meta and M3AAWG note similarly that “access to API” is just part of the problem and not the root cause. Meta suggests further that “bulk registration must be defined as being in-scope for the PDP, and calling this policy initiative an “API issue” is in some ways confusing. The GNSO should clarify that bulk registrations made for abusive purposes are the main problem that needs to be solved.

Charter questions: The ALAC supports prioritization and highlights additional Charter questions when considering this topic. The Government of India also supports controls for high-volume registrations APIs and references analysis indicating materially higher abuse when APIs are un gated.

However, the RrSG noted: “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 [Extensible Provisioning Protocol] interactions between registry and registrar.” auDA notes that API use is common in reseller models and proposes straightforward vetting and verified payment before opening programmatic access and notes examples from their business practices that demonstrate how “access to APIs” can be managed.

The NCSG suggested that “the charter question for this PDP neglects to account for undue burden that such barriers to accessing APIs could pose to new registrants. The charter should therefore also include a question about how to find this balance, such as: ‘How can such safeguards be implemented in ways that ensure new registrants, particularly smaller entities

and/or those from the global majority, can still demonstrate basic trustworthiness? How can we ensure that any such safeguards are not overly burdensome for these registrants?”

Proposed Solutions by Commenter(s): CleanDNS, DNS AXE, M3AAWG, and NWS argue for activity-based friction, trust thresholds for new or untested accounts, and risk-based gating as proportionate, targeted mitigations that preserve legitimate high-volume use. CleanDNS notes its support for “the introduction of proportionate, risk-based friction for new or untrusted accounts before granting access to high-volume registration tools. This friction should be based on customer activity (e.g., account age, abuse history), not just identity, to avoid unnecessary barriers for legitimate users.”

Multiple commenters, including the IPC, Meta, Namecheap, RrSG, RySG and Tucows, concur that gating and measured friction for APIs access can be required, with registrar discretion in how friction is applied, to achieve evidence-based reductions in abuse. Meta adds that “this includes encouraging waiting periods for new accounts, verifying and validating account activity and history to ensure no prior abuse reports, and implementing tiered access based on risk signals. This approach will reduce the speed and scale at which attackers can launch phishing and impersonation campaigns.” NC further adds “we additionally caution that by providing specific details, limits, or exact requirements into a public ICANN policy will allow bad actors to easily circumvent the policies and continue their campaigns unimpeded and without recourse.”

Issue 2: Associated Domain Check

Scoping: Most commenters support taking up “Associated Domain Checks” as priority topics for a PDP. Supporters including CleanDNS, the CPH, IPC, and the Government of India endorse a policy track to enable or require checks that help link domains associated with an actor or incident. CleanDNS noted that “this *pivot* approach is already best practice among many of their clients and should be standardized as an effective anti-abuse model.” Tucows also notes that this is a practice in their organisation and they support this being formalized. SM questions whether the solution proposed for associated domain checks meaningfully differs from the API-gating work, and suggests that “if a compromised domain is mistakenly flagged as malicious, checking associated domains could result in the take-down of several legitimate domains registered by the same account.”

Charter questions: Commenters such as the ALAC, CPH, and CleanDNS stress that the policy should clearly set the objective, scope, and evidentiary threshold so registrars know what to look for and how to act, while ensuring due regard for registrant rights. IPC suggests that “any obligations should be scoped to ensure it is practical for both retail and wholesale registrars, with clear criteria for what constitutes “association” (e.g., account ID, email, payment method, account access).”

The ALAC, CPH, DNS Axe, and Meta provide additional draft charter questions that should be considered.

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.”

M3AAWG, NCSG, and the RrSG also ask for concrete answers during PDP scoping: which data are necessary and proportionate to request when investigating complaints; how data minimization, burden on smaller or low-resource registrants, and privacy will be handled; what enforcement mechanisms and proof standards will apply; and how to assure interoperability and fairness across contracted parties. The RrSG further notes that “initial discussions among stakeholders have brought to light the considerable complexity of codifying this practice into a policy that is both clear and enforceable.” They suggest that “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.”

Proposed Solutions by commenter(s): Commenters such as CleanDNS and Netbeacon suggest that “for overall impact to the reduction of DNS Abuse and online harms, we believe that Associated Domain Checks should be the priority effort as it will have the more significant impact across the industry while continuing to counteract the malicious actor’s ability to adapt.”

Issue 3: Limited coordination on Domain Generation Algorithm-based abuse

Scoping: The majority of commenters such as the BC, CleanDNS, DNS AXE, Identity Digital, Meta, and the RrSG agree that there should be a clearing house or coordination hub to quickly disseminate Domain Generation Algorithm (DGA) domain lists to all relevant operators. However, the approach on how to create that coordination hub varies significantly amongst commenters and stakeholder groups.

The BC, CleanDNS, DNS Axe, Meta, ID, and RySG support best-practices to establish a coordination role for ICANN in this area. However, commenters such as the CPH, the Government of India, IPC, Namecheap, RrSG, and Tucows suggest a PDP on this topic. Tucows noted concerns “that this topic is being singled out for treatment as a non-binding best practice while others are pushed to policy and do not agree that this is appropriate.”

CPH and IPC suggest policy requirements to formally recognize ICANN’s role as “clearing house” or “coordination hub” for DGA-based abuse. The CPH noted that policy should consider, amongst others, the following question: “Should there be a centralized coordinating role within the ICANN community to perform the collection and distribution of systemic DGA-based threat information to help protect the security and stability of the DNS?”

The RrSG noted that policy is needed for the “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.”

Significant concerns were expressed by M3AAWG, which notes that ICANN itself may not be the right place or may not have the “ability to create an effective solution” here.

PDP Structure

Scoping: The Preliminary Issue Report proposed covering the two priority topics in one PDP and dividing the PDP into phases. Some commenters, such as the Government of India, favor launching a single, narrowly scoped PDP that tackles the two top-priority gaps (unrestricted API access and associated domain checks) first, emphasizing that these enable bulk or fast-moving abuse and merit immediate treatment.

However, seventeen (17) commenters such as CleanDNS, CPH, ID, Namecheap, PIR, Tucows, and RrSG, prefer individual PDPs for each topic rather than multi-layered or phased constructs, arguing that bundling issues increases complexity and delays measurable outcomes. Commenters note that the topics are not similar (enough) to be covered in one PDP. CleanDNS for instance “believe[s] that a phased PDP approach would lead to unnecessary delay, in further bolstering anti-DNS abuse actions.” The Preliminary Issue Report also added that having these two topics covered in one PDP would “fail the aspiration of a *narrowly scoped PDP*.”

On aspects of the WG model, Tucows, Namecheap, and RrSG ask for balanced, parity-minded participation across the community in any working group, noting that “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.” Adding that “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.” The ALAC and INTA also note that the Representative Model could “lock out experts who are not part of current ICANN AC/SOs/C/SG groups” and therefore ALAC and INTA recommend a “Representative + Open Working Group Model.”

Proposed Solution by Commenter(s): The IPC pointed out that “additional gaps highlighted in the Preliminary Issue Report should be addressed concurrently or in parallel, rather than postponed for years. Rather than endure years of policy-making, ICANN should consider contract negotiations as an alternative approach to a PDP.” The GAC asks in its comments that the Issue Report provides potential solutions to other issues identified in the report, while the IPC further added that a PDP with the other priority topics named by the DNS Abuse Small Team report should begin in parallel, suggesting issues such as “Proactive contact verification” be included in the PDP. The BC similarly notes that policy work on DNS Abuse that takes all gaps into consideration might take many years and therefore, ICANN org should: “Enter into contract negotiations with registries and registrars to amend the Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) to implement new obligations for mitigating DNS abuse.” BC and Meta suggest that ICANN should deliver the PDP on DNS Abuse within 12 months.

Other Issues discussed in the report

This section covers the comments made related to other Issues identified in the Preliminary Issue Report, but not named as priority topics for a PDP.

- **Sources:** The NCSG asked that ICANN and the GNSO draw on a broader and more diverse set of research sources when preparing future Issue Reports. They recommended incorporating other studies and regional perspectives to improve objectivity and global representation when drafting Issue Reports. Furthermore, Namecheap noted that publishing too much detail about detection methods or mitigation strategies can inadvertently aid bad actors. They advised maintaining discretion in future reports and avoiding disclosure of specific technical indicators or operational processes.

Phase 0: Preventative Measures

- **P2 and P3 Lack of Proactive or Timely Contact Verification:**

Scoping: Commenters such as the Government of India would like to see a PDP on this issue. The BC sees policy development on this issue as “top priority” and adds that “as of April 2024, GoDaddy has required domain name auction participants to complete a reasonably stringent verification procedure that includes submission of government-issued identification, a photograph of the user, and a copy of proof of address (e.g., a utility bill or credit card statement).”

Other commenters, such as Namecheap and Tucows, however, consider “the current validation and verification processes to be effective and the current timeline to be appropriate in context of real-life user experiences.” Tucows further added that “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.”

Proposed Solution by Commenter(s): The Government of India would prefer immediate contract amendments instead of a PDP by “amending the RAA’s Section 3.7 and the RDDS Accuracy Program Specification to mandate instant (simultaneous) email and phone verification via OTP at the time of registration, thus eliminating the current 15-day window.” The RySG notes that this issue should be covered within a DNS Abuse PDP, but “could be part of other GNSO-led efforts.”

Regarding the lack of full syntactic checks, Tucows noted that the issue should be raised to ICANN Compliance. Namecheap and the RrSG suggest that “SSAC should be invited to provide or endorse tools for those basic syntactic checks (email and phone formats per RFC).”

- **P5 Minimal Deterrent Effect of Reactive Measures (“Uptime”):**

Commenters such as the Government of India, the RrSG, and Tucows agree that no specific solution is needed for this issue. The Government of India notes, however, that increasing education on preventative measures should be considered.

- **P6 Real-Time Detection of Short-Lived Abuse:**

Scoping: Most commenters, such as Namecheap, Tucows, and the RrSG, agree that “combating short-lived DNS abuse requires a multi-layered approach” and should be approached holistically and outside of policy. The NCSG suggests that this issue is outside of ICANN’s remit. It argues that “even where technically possible, the constant monitoring of all registrants’ domain-related activities amounts to a staggering system of surveillance that may not only produce a chilling effect among registrants and should only be undertaken should with clear safeguards.”

Proposed Solution by Commenter(s): The Government of India suggests that “the root cause of the problem can be addressed through instant/ simultaneous verification (meaning gap P2 and 3) along with other approaches.” The BC and IPC both suggest that this Issue could be solved addressing P2 and P3 as well as P7 and suggests that ICANN “facilitate data sharing and technology tools to help registrars identify high-velocity abuse (e.g., feed of domains generated by DGAs or reported in near-real-time).”

- **P7 Underuse of Predictive Algorithms for Early Detection:**

Scoping: Most commenters supported the Preliminary Issue Report’s conclusion that predictive algorithms for early detection of DNS Abuse are not for inclusion in ICANN contractual obligations and potentially best addressed in non-binding best practices. The Government of India, NCSG, and Namecheap caution that automated detection tools risk high false-positive rates, potentially leading to unjustified mitigation actions against legitimate domains.

Proposed Solution: The IPC, on the other hand, would like to see a policy recommendation on this issue. Even so, they recognize “that one cannot mandate specific algorithms, but policy can require registrars to have a fraud detection mechanism in place and act on its output.”

- **P8 No Post-Registration Identity Checks for Suspicious Activity:**

Scoping: Commenters such as the BC, the Government of India, and IPC supported additional post-registration identity verification for suspected abuse, while other commenters, such as the RrSG, Tucows, and Namecheap, note that no further policy work is needed here.

Proposed Solution by Commenter(s): The Government of India proposes “amending RAA Section 3.7 or adding a new section requiring triggered KnowYourCustomer-style checks after specific thresholds of abuse (e.g., multiple abuse reports within 30 days).” The IPC suggests that “when a domain is reported for serious abuse (with evidence), the registrar should be obligated to

re-confirm the registrant’s identity and details. For example, require the registrant to provide a valid government-issued ID or additional verification promptly once their domain is the subject of a credible abuse complaint.”

The RrSG added 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.” The RrSG cautions that “this identified gap blurs the line between contact detail verification and identity review. That distinction must remain clear[.]”

Namecheap and RrSG both point out that the “RAA already requires re-verification in specific circumstances.” Tucows added that “Registrant identity and validation of the registrant’s information has not been shown to be a factor in identifying DNS Abuse.” The NCSG further emphasizes its position on “registration data accuracy” to focus on “contactability, not identity verification.”

- **P9 and P10 Discounted Pricing and Free Services:**

All commenters, such as the Government of India, NCSG, and RrSG, agree that while free or heavily discounted domain pricing can correlate with DNS Abuse, pricing policies fall outside ICANN’s remit. Furthermore, commenters support the report’s recommendation to address this issue through education and awareness. Some commenters, such as the BC and IPC, encourage ICANN to publish educational material and best practices or “future contract incentives.”

- **P11 Limited Use of Abuse Feeds and Threat Data:**

Scoping: Commenters such as the Government of India and the RrSG agree with the report that requiring use of commercial block lists is not appropriate for policy.

Proposed Solution by Commenter(s): Tucows suggested that this can be addressed by best practices but also points out that the “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.” Namecheap adds that “it should be for individual contracted party to determine which of these commercial (e.g. paid) services they should utilize, based upon the registrar or registry’s unique business needs” and emphasized “that some popular abuse feeds contain high levels of false positives and little (if any) transparency regarding data collection and analysis.”

Phase 1 and 2: Abuse Reporting

- **A1 Unactionable Complaints to ICANN:**

Scoping: Many commenters, such as the RrSG, appreciate the current approach, where ICANN org filters “unactionable complaints” and supports “educational initiatives” to improve DNS Abuse reporting. Commenters reported

that complainants often receive limited feedback or unclear referral paths. The BC and IPC note that “part of the issue at play is standards and procedures that differ by registrar or registry” and don’t seem to be “user-friendly.”

Proposed Solution by Commenter(s): The BC and IPC “support efforts to standardize the DNS abuse reporting intake process, and the community should define what constitutes an ‘actionable’ abuse report (fields, evidence required and other elements of actionable report) and ensure complainants are guided to provide.”

The Government of India “proposes a narrowly scoped PDP amending RAA Section 3.18.4 to require registrars to publish a clear abuse reporting user-friendly web form with mandatory fields (e.g., domain name, evidence of abuse) and step-by-step guidance with FAQs to assist the complainants, combined with best-practice educational materials, will reduce unactionable reports and improve responsiveness.”

INTA noted in its comment “that there is no mention of whether ICANN Compliance provides feedback to complainants on why their report was unactionable when closing a report,” explaining that “INTA members and a minority of registrars agree that ‘fake web shops’ constitute phishing, whereas most registrars will not action DNS abuse reports related to ‘fake web shops.’” INTA, therefore, recommends “ICANN to add language to A1 (issue) that addresses our concern regarding the subjectivity of responses and require ICANN compliance to report the reasons why a report is unactionable when closing the file.”

SM suggests clearer publication of abuse-contact details by registries and registrars. He urged that each contracted party maintain an easily discoverable, functional email address for reporting abuse and that ICANN ensure these contacts remain accurate. SM objected to the growing trend of replacing abuse-reporting email addresses with online forms. He argued that forms can fail or restrict urgent reports, especially for automated submissions from security researchers. He asked that ICANN reaffirm the requirement for a working abuse email address as a baseline standard, allowing web forms only as supplementary channels.

- **A3 Malicious vs. Compromised Domains:**

Scoping: The IPC expresses a view that policy efforts should focus on malicious registrations (within ICANN’s remit) but encourages cooperative action on compromised domains. In contrast, the BC does not agree that compromised domains are expressly outside ICANN’s remit, stating: “we acknowledge that it may be prudent to focus initially on mitigation of maliciously registered names”

and emphasizes that this could be addressed by focusing policy on preventative measures.

Proposed Solution by Commenter(s): Commenters such as Namecheap, the RrSG, and Tucowas note 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, whereas “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.

The Government of India “insists registrars be required to publish clear FAQs and guidance for registrants whose domains have been compromised, explaining how they may contact agencies (e.g. national CERTs, cybercrime units), what documents must be submitted (identity proof, domain ownership evidence, security logs), and what procedural steps are available to restore suspended or blocked sites.”

Some commenters provided the following comment regarding the use of the Centralized Zone Data Service (CZDS): The BC noted “this is not directly tied to this request for comment; however, the BC offers in good faith its ideas for improving CZDS as an abuse mitigation tool.” The BC further proposed “Voluntary Daily Zone File Publication by Commercially Used ccTLDs - Increasing Transparency & DNS Security via CZDS,” referencing research “that at least 1% of domain names exist in a ‘window of invisibility’ registered and used maliciously within the 24-hour gap between daily zone file publications (Sommese et. al.,2024).”

RS proposed a similar approach, noting “DarkDNS: Revisiting the Value of Rapid Zone Updates (IMC 2024), we measured a persistent visibility gap in the ICANN Centralized Zone Data Service (CZDS), where at least one percent of newly registered domains never appear in the daily zone snapshots.” SM also suggests “a log would allow security experts and organizations to instantly access changes in zone files, enabling real-time monitoring of newly registered domains. This, in turn, would make it possible to detect malicious activities more quickly and effectively.”

Phase 3: Mitigation by Contracted Parties

- **C1 Limited Transparency on Mitigation Actions Taken:**

Scoping: Some commenters, such as the IPC, would like to see policy development on this issue. The NCSG “urge[s] the ICANN community to place greater priority on actioning these transparency requirements” and to consider policy development. RrSG and Tucows note that this could be addressed via policy development but is not a priority topic at this time.

Proposed Solution by Commenter(s): The IPC would like to see a requirement “(via policy or procedure) that registrars send a response to the abuse reporter when a case is resolved.” The Government of India, for instance, proposes “a contract amendment complemented by best practices to establish transparency in reporting mitigation actions by registrars/registries. In this context, amending RAA Section 3.18.4 (handling and tracking abuse reports) by setting up obligations upon the registrars to publish periodic statistics.”

The RrSG, however, suggests that “as a start, the Community should consider nonbinding guidance and best practices for abuse reporting.” INTA noted that “the Issues Report should consider the overlap between C1 (Limited Transparency in Mitigation Actions Taken) and A1 (Unactionable Complaints to ICANN) and identify that there is a common theme of needing to close the feedback loop to reporters.”

- **C3 Lack of Standard Recourse or Appeal Mechanisms for Registrants:**

Scoping: Many commenters such as Namecheap and the RySG agree with the conclusion of the Preliminary Issue Report and support this topic being considered in subsequent PDPs. The NCSG added “concern that this gap was not listed as a priority item for a policy development process.” The M3AAWG, however, noted “this idea is not designed to prevent or mitigate abuse. The need for a policy has not been justified, and a policy could be abused if not written properly.”

Proposed Solution by Commenter(s): The IPC suggests that this could be addressed by “simply requiring registrars to offer a point of contact for suspension disputes, and to promptly review any evidence provided by the registrant.” Tucows suggests that “all PDPs that have effects on registrants include consideration of recourse and dispute mechanisms available to registrants.”

- **C6 and C7 Due Diligence and Transparency in Mitigation:**

Commenters such as the RySG and Tucows agree with the report’s conclusion that “this is not a gap in DNS Abuse mitigation itself and does not require policy development work at this time.”

The Government of India and IPC support best practices. India also recommends to “develop policy once more data is available.” The NCSG, however, disagrees significantly with the report noting that this should be a priority policy topic and that there is sufficient data available on the topic.

The NCSG points to “civil society organisations who have conducted research on the importance of human rights impact assessments (HRIAs) for infrastructure companies and for technology companies more broadly.”

- **C8 Inconsistent Responses - Seeking Standardization:**

The RrSG noted that the contract amendments kept the timeline to respond intentionally flexible “to ensure that Contracted Parties have the ability to take appropriate action depending on the circumstances.” 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.”.

The IPC, however, notes that “promptly” is “too elastic” and proposes “the community could agree that an abuse complaint with sufficient evidence should be processed within 24 hours in normal circumstances”. “SM asked in his comment: “It is important to clearly define what ‘promptly’ means in practice. Does it refer to 24 hours, 48 hours, one week, or another timeframe?” He references the RA that “registry operators must promptly take the appropriate action...” Furthermore, SM comments noted a lack of transparency in sink holing practices. He explained that he “observed cases where some registrars’ ‘sinkhole’ a domain by changing its nameservers to ones under their control” and according to him “this practice is fundamentally problematic.”

Phase 4: ICANN Compliance Enforcement

- **E2 No Clear Escalation of Sanctions for Recurring Non-Compliance:**

Scoping: Most commenters agree that addressing this would require policy work. However, commenters such as the RrSG argue that this is not a priority topic and the community should address other issues first. Tucows notes, “it is unclear what additional intermediate penalties would be envisioned.”

Proposed Solution by Commenter(s): The Government of India “favours exploring a PDP to establish graduated sanctions, balanced with due process.” The IPC suggests “if a few registrars are responsible for an outsized share of abuse, ICANN should be able to initiate audits or impose conditions on accreditation renewal.” INTA “suggests that an intermediate sanction could be introduced by creating two tiers of registrar fees: lower fees for registrars who receive less than a given number of compliance inquiries and non-compliance notices in a billing period, and, likewise, higher fees for registrars who exceed this number.”

- **CC.2 No Mechanism to Update DNS Abuse Definition:**

Scoping: There is broad agreement amongst commenters such as Government of India, NCSG, and Tucows for not expanding the current definition of DNS Abuse currently; commenters endorse using the existing RAA-anchored definition. The Government of India and NCSG agree that other definitions such as the current ICANN definition “while malicious, are deemed outside of ICANN’s remit as they pertain to content and therefore would violate ICANN’s bylaws.”

Proposed Solution by Commenter(s): 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.”

The BC, Fraudkillers, INTA, and IPC in contrast ask for a continuous update to the DNS Abuse definition based on emerging and evolving threats. The BC and INTA reference “that SAC115 recommends periodic review of abuse definitions, as did the recommendations from the SSR2 team.” Fraudkillers want to see “scams and fraud” included in the definition.

Section 4: Analysis of Submissions

In addition to the Public Comment, ICANN organized a [DNS Abuse Working Session at ICANN84](#). The session was convened to move from issue-framing to possible solutions on the two topics highlighted in the Preliminary Issue Report. The goal was to gather community perspectives to inform a draft charter and updates to the Issue Report.

The Public Comment and ICANN84 session showed areas of convergence and divergence.

Areas of Convergence:

- With respect to Issue 1 (API Access) and Issue 2 (Associated Domain Checks), ICANN notes that nearly all commenters agreed these topics should be prioritized for policy development through a GNSO PDP. The comments confirm that both issues are well-supported by data and provide a clear foundation for meaningful consensus policy work.
- Many commenters argued for outcome-oriented requirements that specify what must be achieved rather than dictating how each registrar must perform checks. This flexibility was seen as essential to account for varying business models, technical systems, and local legal contexts. Registrars noted that different technical infrastructures already support abuse checks; mandating specific tools or data points could be counterproductive.
- Support for proportionate, risk-based safeguards on API/high-volume access. There was broad recognition that not every reseller or registrar needs the same level of gating. Participants converged on a risk-tiered approach.
- There was general acknowledgment that registrant rights, data privacy, and non-discrimination must be built into any new policy requirements, and recognition that a Human Rights Impact Assessment is now a standard procedure for every PDP.
- Participants and commenters noted Associated Domain Checks as a potentially “high-impact” first-step PDP. There was relatively broad alignment that requiring checks for associated domains using existing registrar tools could produce tangible results relatively quickly.
- Participants urged designing solutions resilient to evolving attacker behaviour and emerging technologies.

Areas of Divergence:

- Commenters expressed differing preferences for a single comprehensive PDP or two smaller, narrowly focused PDPs. The majority seems to favor two separate charters for the topics.
- Regarding the third issue from the Preliminary Issue Report: Limited Coordination of DGA-based abuse. The community had varying opinions on whether this should be addressed as a best practice or via PDP. The CPH proposed policy development on this issue.
- Participants and commenters emphasized that publicly detailing association signals could allow bad actors to reverse-engineer systems.
- Some noted that requirements to document every Associated Domain Check or maintain detailed investigation logs could impose significant administrative load, particularly on smaller registrars, without necessarily improving detection outcomes.

Incorporation Into Issue Report

ICANN org will integrate additional clarifications and proposed charter questions suggested by commenters concerning evidentiary thresholds, implementation feasibility, and metrics for measuring effectiveness for both priority topics. For the third priority topic, ICANN org will update the section with the differing views and suggestions on whether to address this topic via policy development or best practices.

On PDP structure, ICANN org acknowledges the thoughtful feedback received from multiple stakeholder groups regarding scope, sequencing, and representation. ICANN recognizes these concerns and will update the Preliminary Issue Report incorporating two (2) draft charters for Council consideration.

Regarding the other issues analyzed in the Preliminary Issue Report, ICANN appreciates the detailed input provided by commenters. Where appropriate, ICANN will update the “Proposed Solutions” section of the report to reflect community feedback and incorporate additional examples or refinements suggested during the comment period.

Section 5: Next Steps

ICANN org appreciates the valuable and substantive input received from all commenters on the Preliminary Issue Report. Based on the comments received, ICANN will update the report and deliver the Final Issue Report to the GNSO Council for consideration.