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

NCSG Comments

October 18,2025

About NCSG

NCSG represents the interests of non-commercial domain name registrants and end-users in formulating the Domain Name System policy within the Generic Names Supporting Organisation (GNSO). We are proud to have individual and organizational members in over 160 countries, and as a network of academics, Internet end-users, and civil society actors, etc, we represent a broad cross-section of the global Internet community. Since our predecessor's inception in 1999, we have facilitated global academic and civil society engagement in support of ICANN's mission, stimulating an informed citizenry and building their understanding of relevant DNS policy issues.

About this Public Comment

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

Our Comment

The issue of DNS abuse mitigation is not a new one; however, with the contractual amendments to Registrar Accreditation Agreements (RAAs) to mitigate DNS abuse having come into force, registries and registrars must now "promptly take the

appropriate mitigation action(s) reasonably necessary" to disrupt the abuse.[1] Yet the question remains: how to address the DNS abuse without overreaching and running the risk of censorship?

Registrars and registries are often limited in what they can do: if they wish to block a particular activity, often their only recourse is to take down the entire domain name. This blunt force action should only be taken as a last resort. Finding alignment between ensuring the safety and security of the DNS, and safeguarding registrants' rights to freedom of expression and privacy online is paramount and they are not always contradictory.

With this in mind, the NCSG offers its contribution to the preliminary issue report on a PDP on DNS abuse mitigation. Our position is grounded in two key principles:

I. Requirement of specific policies in the concern of DNS Abuse as it has a direct impact on registrants, end-users, and the operations of registries and registrars.
II. Collaboration with technical experts & DNS abuse small team to identify sources of DNS abuse and its impact on human rights.

We have organized our comments in order of proposed mitigation method:

I. Unrestricted API Access for Domain Name Registration for New Customers
II. Associated Domain Checks
III. Post-registration Identity Checks (p.17)
IV. Lack of Standard Dispute/Recours Mechanism for Registrants (C3)
V. Due Diligence and Transparency in Mitigation (C6 & C7)
VI. Discounted Pricing (P9) & Free Services (P10)
VII. No Mechanism to Update DNS Abuse Definition (CC2)

Overarching Feedback

We applaud the clear effort made by the authors to ensure that all recommendations put forward integrate human rights considerations. We especially want to reiterate the author's prescient statement that "preventative measures [must be] balanced against the need for an open and accessible domain name marketplace" and that "overly onerous checks could hinder legitimate registrations" (p.12).

We also appreciate the authors' efforts to cite outside research to back up their positions. However, of the sources cited from outside ICANN, only a handful of reports are referenced, primarily NetBeacon and ICANN's own commissioned study. Whereas

---

[1] https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en

the cross-community working party on human rights (CCWP-HR) and members of the NCSG have developed several tools regarding how to conduct human rights impact assessments specifically focused on DNS abuse,[2] we have also undertaken a collective human rights impact assessment session for DNS Abuse mitigation during ICANN. These resources and analyses were not cited. These resources could have provided additional and much-needed information to ground this report. For example, the CCWP-HR in its Human Rights Gap Analysis of ICANN's amendments to the base gTLD RA and RAA has similarly cautioned registries/registrars to ensure that enforcement or mitigation mechanisms remain within the scope of ICANN's remit and that procedural safeguards are integrated to protect registrants' rights. We therefore urge the authors to review and reference a broader set of stakeholder resources and research outputs when developing future reports.

There are also recommendations that request for 'proactive monitoring' for DNS abuse (see "P6. Challenges in Real-time Detection of Short-Lived Abuse). 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, but may also become co-opted by governments interested in limiting the dissemination of information or stifling oppositional or unpopular speech — especially given the considerable control that governments already have over country-code top-level domains like .uk, .us, or .tv. We urge the authors to emphasize that such proactive techniques are not only outside of ICANN's scope (p.16), but should only be undertaken with clear safeguards as they could pose very real censorship and surveillance threats to registrants.

Additionally, regarding "P7. Underuse of Predictive Algorithms for Early Detection" we agree with the authors' conclusion that this issue is not suited for ICANN policy development. In addition to the issues noted by the authors, we also suggest noting that the burden of the potentially high costs of compliance would be particularly an issue for small businesses and non-commercial entities such as not-for-profits.

Additionally, algorithms are poor evaluators and lack the nuanced decision making skills. Robust human review is needed to ensure that algorithmic decision making does not infringe upon legally protected speech online. Any such proactive measure must be subject to rigorous human rights risk assessment, implemented with narrowly tailored scope, transparency, and meaningful recourse options to ensure proportionality and accountability. We therefore urge the authors to strengthen their rejection of this proposal by noting the human rights risks associated if ICANN were to contractually require specific security mechanisms based on an algorithm.

[2] http://digitalmedusa.org/wp-content/uploads/2024/11/DNS-IHRL-Cheat-Sheet.pdf + any other sources?

Feedback on Identified Policy 'Gaps'

I. Unrestricted API Access for Domain Name Registration for New Customers

We appreciate the authors' logic that by taking action at this stage of the domain lifecycle, we could prevent DNS abuse further down the line.A requirement of information sharing in the concern of any update regarding attempts and examples of DNS abuse. However, 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?*"

II. Associated Domain Checks

When investigating actionable DNS abuse, registrars may need to examine other domains associated with the same registrant data to disrupt broader abuse networks. However, as the NCSG highlighted in its contribution to the GNSO Small Team on DNS Abuse's Gap Analysis document, such inspections must be conducted with strict safeguards to avoid undue surveillance of legitimate registrants. Investigations must be grounded in clear, specific evidence of abuse linked to the registrant—never on speculative or broad profiling. The focus must remain on the abusive activity, not on surveilling the registrant's broader online presence.

We also concur with authors that "the potential solutions and their feasibility must be considered during the PDP deliberations"; however, an HRIA must also be conducted for any solutions to ensure that the risk to privacy and anonymity of registrants is not compromised and that this does not pose an undue burden on smaller registrants (p.25).

III. Post-registration Identity Checks (p.17)

Here the NCSG reiterates its position that the requirement for "data accuracy" when it comes to registrant data only encompasses contactability, not identity verification. This is because for many human rights activists who may register a domain, there is a need to maintain their anonymity online, and a post-registration identity check both violates their right to privacy and could lead to real-world harms (such as surveillance, arrest, or even threats to life).

IV. C3. Lack of Standard Dispute/Recourse Mechanism for Registrants

The NCSG is very concerned that this gap was not listed as a priority item for a policy development process. Such a PDP would go far in terms of operationalizing/respecting ICANN's human rights commitment per section 1.2(b)(viii) of ICANN's bylaws by protecting registrants' rights to freedom of expression online through procedural safeguards and remain in compliance of section 1.1(c) by ensuring that enforcement mechanisms do not lead to overblocking of legitimate online content.

Regardless of the specific issue to be prioritized for a PDP, the outcome of any PDP must include clear due process elements. Examples include: accessible and transparent mechanisms for registrants to seek remedy or challenge decisions and timely notifications to users when enacting domain suspensions or takedowns. As the ALAC noted in their contribution to the GNSO small team on DNS abuse policy gaps documents, "introducing a clear, fair, and timely appeals process would be essential for trust and balance in domain abuse mitigation."

V. C6. & C7. Due Diligence and Transparency in Mitigation

The NCSG is similarly disappointed that this gap was not listed as a priority item for a policy development process. Registries should commit to full transparency through transparency reporting on actions taken in response to DNS abuse, and a clear and consistent redress framework.

The authors argued that it is "currently unclear" whether there is a gap in DNS abuse mitigation "due to lack of data," and therefore it is "difficult to assess the best mechanism to mitigate the potential harms (p.28)." However, we would like to highlight the numerous 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.[3] NCSG members have limited resources to conduct the kind of specific research that NetBeacon (among others) have been able to supply to ICANN; however, our contributions are no less significant and point to a clear need for due diligence and transparency mechanisms to be incorporated and accounted for as part of any PDP process on DNS abuse mitigation.

Regarding the "Limited Transparency in Mitigation Actions taken," we agree with the authors that minimum reporting requirements can be addressed by policy development or best practices, and we urge the ICANN community to place greater priority on actioning these transparency requirements. The NCSG has already proposed recommendations for best practices, including:

[3] Examples include: ARTICLE 19's "Human Rights Due Diligence and Internet Infrastructure" report; [others please feel free to add here!]; Digital Medusa's blog post "DNS Abuse Mitigation and Human Rights Impact Assessment"

- Notice: When action is taken against a domain, the registrant must be promptly notified. This notice should include: the reason for the action; the type of action taken; the initiator of the action (e.g., registrar, third-party request); and a clear explanation in accessible language.
- Restoration Process: A pathway for legitimate registrants to demonstrate that abuse has been resolved—or that the action was mistaken—and regain control of their domain in a timely manner.
- Complaints & Appeals: A clear and fair process through which registrants can file complaints or appeal mitigation actions, reinforcing procedural fairness, access to remedy, and accountability.

VI. Discounted Pricing (P9) & Free Services (P10)

We agree with the authors' conclusion that this issue is ultimately best addressed by building awareness, and should be left with the contracted party to decide (p.19). We would also be concerned with contracted parties setting higher prices as this could risk pricing out registrants operating under tight margins and smaller budgets. Any such decision regarding economic incentives to prevent DNS abuse should be taken with this consideration in mind.

Affordable or free domain names are essential for digital inclusion. They allow individuals, small businesses, and civil society groups to establish a presence online. Pricing should not be used as a blunt tool for abuse mitigation. Doing so risks disproportionately harming legitimate users and undermining efforts to expand equitable access to the Internet. Abuse mitigation by registrars offering low-cost domains should instead rely on rights-respecting measures: clear abuse reporting channels, prompt investigation, proportionate response, and strong due process—not financial barriers.

VII. No Mechanism to Update DNS Abuse Definition (CC2)

We agree with and especially appreciate the authors' conclusions regarding the proposed expansion of the definition of DNS abuse. The authors helpfully note that the additional examples of 'abuse' that have been brought up in the community "while malicious, are deemed outside of ICANN's remit as they pertain to content and therefore would violate ICANN's bylaws." As the report also hopefully noted, there are other more appropriate avenues to resolve disputes related to IP and trademark issues–two examples that have been raised as potential examples to be added to the ICANN definition.

We therefore strongly urge the authors to reiterate its stance against expanding the definition of DNS abuse beyond those currently outlined in the ICANN definition. Any changes to the definition risks placing DNS operators in the position of content

moderators, which would both contradict ICANN's mission[4] and heighten the risk that legitimate speech online is censored.

As content moderators, registries have very few options: if they decide to censor content, their only course of action is to completely take down the domain name of the website hosting the content, effectively removing the website from the internet. Efforts to remain in compliance risks leading to the takedown of websites hosting content that is actually lawful under international freedom of expression standards. For example, if even one sentence on the ARTICLE 19 website was perceived to constitute some definition of DNS abuse, Public Interest Registry (PIR) would be obligated to take down article19.org entirely.

Additionally, any revision process should also involve the ICANN multistakeholder community in order to update DNS access policies, which should come to consensus on a clear definition of the term to be consistently applied, including a clear and exhaustive scope and an indication of remedies and actions that registries may take. Should such a revision process take place, it must involve the ICANN multistakeholder community, which should come to consensus on a clear definition of the term, to be consistently applied, including a clear and exhaustive scope and an indication of remedies and actions that registries may take.

Resources

- DNS & IHRL Cheat Sheet
- [DRAFT] NCSG DNS Abuse Position Paper
- ListofGapsDNSAbuse.xlsx

[4] As outlined in Section 1.1(c) of ICANN's mission, "ICANN shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide…."