ICANN | GNSO

Generic Names Supporting Organization

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

## Status of This Document

This Preliminary Issue Report has been drafted by ICANN Policy Support Staff and shall be published for Public Comment. Staff will review all comments and based on the feedback, make any necessary amendments to forward the Final Issue Report to the GNSO Council for its consideration.

## Preamble

On 14 August 2025, the GNSO Council passed a motion, requesting ICANN's Policy Support Staff to draft a Preliminary Issue Report on DNS Abuse. The objective of this Preliminary Issue Report is for Staff to assess all relevant issues related to the GNSO Council request and, following Community Input during the Public Comment phase, to recommend a course of action to the GNSO Council. It remains the GNSO Council's prerogative to either follow Staff recommendations or to pursue alternative action.

# Table of Contents

# 1 Executive Summary

## 1.1 Discussion of the issue

The impetus for this Issue Report stems from the recognition by the GNSO Council that Domain Name System (DNS) Abuse as defined in the Registrar Accreditation Agreement (RAA) and the Base Generic Top-Level Domain (gTLD) Registry Agreement (RA) remains a significant challenge to the security, stability, and trust in the DNS. For the purpose of the RAA and the RA, DNS Abuse means malware, botnets, phishing, pharming, and spam (when spam is used as a delivery mechanism for any of the other four types of DNS Abuse). Recent contractual amendments, while impactful and a big milestone for the ICANN Community in addressing DNS Abuse, could not address all mitigation gaps. The GNSO Council's request for an Issue Report is grounded in the DNS Abuse Small Team's findings[1] that certain DNS Abuse mitigation gaps may be best remedied through GNSO consensus policies.

In early 2025, the GNSO Council reconvened its DNS Abuse Small Team with a revised assignment form to re-examine DNS Abuse mitigation considering new developments, research, and data. The previous Small Team (2021–2022) had identified obligation gaps and issued recommendations,[2] some of which were addressed through contractual amendments to the RA and RAA. Those amendments (effective since April 2024) strengthened abuse mitigation obligations, and ICANN Contractual Compliance has since reported initial data on their impact. With these measures in place and new research available, the Small Team was tasked to consider new insights and discuss potential next steps on DNS Abuse. Drawing from community input, compliance data, and external studies, the team was tasked with identifying remaining gaps and assessing whether further policy development is warranted.

The DNS Abuse Small Team conducted a review of data and source documents noted in their assignment form, focusing on identifying potential gaps in DNS Abuse mitigation efforts across multiple phases of the DNS Abuse lifecycle (as proposed by the Small Team in 2022[3]). The Small Team compiled a matrix of DNS Abuse "gaps,"[4] noting areas where abuse prevention, reporting, response, or obligations could be strengthened after further investigating the identified

---

[1] "DNS Abuse Small Team Report to GNSO Council," *ICANN GNSO*, 25 July 2025, https://gnso.icann.org/sites/default/files/policy/2025/draft/dns-abuse-small-team-report-04aug25-en.pdf

[2] "DNS Abuse Small Team Report to GNSO Council," *ICANN GNSO*, 25 July 2025, https://gnso.icann.org/sites/default/files/policy/2025/draft/dns-abuse-small-team-report-04aug25-en.pdf

[3] "DNS Abuse Small Team Report to GNSO Council," *ICANN GNSO*, 7 October 2022, https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf.

[4] In this context, the Small Team uses the term "gap" to denote an area flagged by the data and document review as potentially warranting further analysis, but not necessarily an "issue" in the ICANN Policy Development sense. A gap may or may not merit policy action; some may be better addressed through best practices, or no action at all. Accordingly, the Small Team recommended that these gaps be examined in the Issue Report to determine whether they are suitable for policy development or more appropriate for alternative follow-up. "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

gaps. Findings were categorized by lifecycle stage and further grouped by thematic clusters to support potential prioritization and future policy scoping.

Based on data analysis, community consultation, and input from stakeholder groups (SGs), the Small Team recommended the following three gaps be prioritized for policy work in the Issue Report:

- **Unrestricted Application Programming Interface (API) access for domain name registration for new customers:** Many registrars offer Application Programming Interfaces (APIs) or batch-registration portals that allow resellers or high-volume customers to register large numbers of domain names rapidly. According to studies such as the INFERMAL study, insufficient gating or friction for new users to access these batch registration tools can lead to the proliferation of DNS Abuse.[5]

- **Associated Domain Checks:** Malicious domains are often part of broader campaigns involving dozens or hundreds of related domains. Currently, when a registrar finds that one domain is malicious, there is no contractual requirement that the registrar must investigate whether the same registrant or account has other active domains that are also being used for similar abuse.[6]

- **Limited coordination on Domain Generation Algorithm (DGA)-based abuse:** Botnets using DGAs generate many domain names (sometimes hundreds a day) for their command-and-control.[7] Law enforcement must contact each implicated registry individually when trying to mitigate malware or botnets that use DGAs at scale, which can result in fragmented, delayed, and inconsistent responses. These are low frequency but high impact events. There is no central clearinghouse or coordination hub to quickly disseminate these domain lists to all relevant operators.[8]

The Small Team has chosen the above topics from the matrix, based on topics that seem appropriate for policy development (taking into consideration review of source data,

---

[5] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

[6] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

[7] Command and control is defined as a technique used by threat actors to communicate with compromised devices over a network. See, Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

[8] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

input/priorities received by Small Team members, and Community consultation during ICANN83), meaning that the topics are intended to be:

- important/impactful gap to solve,
- likely to gain broad consensus, and
- ideally, areas in which the potential solution(s) seem achievable, having in mind current workload and resources.

The Issue Report concludes that all of the three identified priority issues are appropriate for policy development. However, the paper suggests that only two of the three identified DNS Abuse issues should be prioritized for policy development, while one may be addressed more directly and expeditiously outside of the ICANN policy development process. This prioritization reflects where policy intervention could likely reduce DNS Abuse at scale, is broadly applicable across the gTLD space, and aligns with the community input and lifecycle-and-cluster analysis used in the updated Small Team gap matrix.

The first issue, **unrestricted API access,** seems to be a significant enabler of DNS Abuse. API abuse in the context of DNS Abuse refers to the exploitation of APIs by malicious actors to carry out harmful activities related to the DNS. These actors often exploit the interconnected nature of APIs to automate and scale their attacks, which can lead to various forms of DNS Abuse. The data review and community discussions indicate that easy access to an API creates lower marginal cost for malicious actors and can amplify phishing/malware campaigns. One of the most consistent findings in the INFERMAL study was that malicious actors are highly price-sensitive (Gaps P9 and P10).[9] This underscores how economic incentives, particularly when paired with automation, can increase vulnerability to abuse. According to the Netbeacon White Paper, introducing proportionate, risk-based friction targets one of the main drivers of abuse without impeding legitimate users.[10] While pricing is out of scope for ICANN policy making, addressing unrestricted API access could reduce DNS Abuse early in the lifecycle. Furthermore. introducing policy on this issue could avoid the task of defining exactly how many domains qualify as a “bulk registration” impacting gaps such as P4. 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.

The second issue is **associated-domain checks**. Domain name registrars, accredited by ICANN, are contractually obligated to investigate and address reports of DNS Abuse involving domains they sponsor. This obligation is outlined in the RAA. The current wording in the RAA focuses on the reported domain and actionable evidence related to it. However, malicious domains are often part of broader campaigns potentially involving dozens or hundreds of related domains. When a registrar finds that one domain is malicious, there is no contractual requirement that the registrar must investigate whether the same registrant or account has other active domains that are also being used for similar abuse. The Netbeacon White Paper suggests a PDP for an “Associated Domain Check” requirement. A PDP for Associated Domain

---

[9] “Insights and Clarifications on the INFERMAL Study,” *ICANN org,* 10 June 2025, p. 4, https://www.icann.org/en/system/files/files/insights-clarifications-infermal-study-10jun25-en.pdf.

[10] White Paper: Proposal for PDPs on DNS Abuse,” *NetBeacon Institute*, May 2025, p. 13, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

Checks could establish a contractual requirement for registrars to proactively investigate other domains registered by a particular registrant or account when abuse is identified on one of their domains.

The third and last issue focuses on **better coordination in addressing DGA attacks**. DGAs can algorithmically generate thousands of candidate domains across many TLDs. DGAs are computer programs that automatically generate domain names, usually using a long random collection of numbers and letters. In the case of “Avalanche”[11], the botnet frequently registered domains with multiple registrars, while testing others to check whether their distinctive domains were being detected and blocked. A domain that was not suspended by a registrar was re-used in later attacks. This was done at scale and pace to allow the attackers to move between different domain names to continue their activities, for example to distribute malware. Law enforcement currently faces a challenge where they must contact each implicated registry individually when attempting to mitigate malware or botnets that leverage DGAs. This fragmented approach can lead to significant delays and inconsistencies in the takedown process, allowing the attackers to maintain control over infected systems for longer periods and hinder law enforcement's ability to disrupt their operations. Addressing this could fill a coordination gap highlighted in the Netbeacon White Paper and other community discussions. By streamlining the process of submitting evidence and coordinating action, ICANN can act as a trusted hub, reducing inefficiencies and ensuring that registries are aligned and responsive to urgent abuse cases. This model would aim to speed up mitigation efforts but also bring greater consistency to DGA-related takedowns. While potentially appropriate for policy development, this item does not necessarily require further policy work and could be implemented outside the contractual requirements.

The three issues address different stages of the DNS Abuse lifecycle but can be considered complementary to each other. API safeguards can reduce the size and speed of potentially abusive registrations at the point of acquisition; associated-domain checks can enable campaign-level disruption once a single domain is confirmed to be abusive (the scope of which is potentially minimized by API safeguards); and DGA mitigation/coordination can provide a common operating picture and synchronized response for high-impact, cross-TLD botnet attacks.

These issues are (i) broadly applicable to multiple business models and geographies; (ii) within GNSO remit as they pertain to registrar/registry obligations and DNS security/stability; and (iii) sufficiently concrete to support tightly scoped policy development.

The first two topics could impose new, uniform duties that a PDP/Consensus Policy could establish and ICANN can enforce. A community best-practice document (PSWG/ RySG DGA framework) for DGA coordination already exists, but there is potential to continue strengthening best practices, e.g. recognizing ICANN as a neutral clearinghouse for DGA lists.

In summary, this Preliminary Issue Report concludes that the three priority issues proposed by the DNS Abuse Small Team are within the remit of GNSO policy development and two merit prompt attention through initiating a PDP, while one of the priority issues would be best

---

[11] https://www.europol.europa.eu/media-press/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

addressed outside policy development. The report provides background and analysis for each of these three priority issues. While there is focus on these three issues (as proposed by the DNS Abuse Small Team), it is important to note that a number of other issues are included and covered in subsequent sections of this Issue Report, and could be handled in future PDPs or other mechanisms.

## 1.2 Staff recommendation

ICANN staff has confirmed that the proposed issues are within the scope of the GNSO's Policy Development Process (see Annex G-2 of the ICANN Bylaws).

In addition, the issues are broadly applicable to multiple organizations and will have lasting value of applicability. Mitigating DNS Abuse (as defined in the RAA/RAs) directly relates to the security and stability of the DNS, and uniform policies in this area would help protect Internet users and infrastructure. Furthermore, the issues raised are broadly applicable across the gTLD space, affecting gTLD registries, registrars, registrants, and end-users globally.

## 1.3 Next steps

In accordance with the GNSO PDP rules, the Staff Manager will publish the Preliminary Issue Report for public comment to allow for Community input or additional information, or the correction or updating of any information provided so far. Following review of the public comments, the Staff Manager will update the Preliminary Issue Report and submit a summary of the comments received together with the Final Issue Report to the GNSO Council for its consideration and potential action.

# 2 Procedural Foundation

## 2.1 Grounds for submission

This Preliminary Issue Report is submitted in accordance with Step 2 of the Policy Development Process described in Annex A of the ICANN Bylaws.[12]

## 2.2 The identity of the party submitting the request

The GNSO Council has requested this Issue Report.

## 2.3 Support for the issue to initiate a PDP

On 14 August 2025, the GNSO Council passed a resolution: "The GNSO Council accepts the recommendations as outlined in the DNS Abuse Small Team report and requests that an Issue Report be initiated on the topics as outlined by the Small Team and requests that Staff create the report."[13]

## 2.4 How that party is affected by the issue

The issue of DNS Abuse is broadly impactful to the Domain Name System and has a direct impact on registrants, end-users, and the operations of registries and registrars. Recommendations that may be developed by a GNSO PDP on DNS Abuse will also be of interest to other ICANN Supporting Organizations (SOs) and Advisory Committees (ACs) because of the impact to their constituents. After ICANN83, the Governmental Advisory Committee (GAC) provided advice on the topic of DNS Abuse, noting the expectation for a PDP on DNS Abuse issues, prioritizing bulk registration of malicious domain names and the responsibility of registrars to investigate domains associated with registrant accounts that are the subject of actionable reports of DNS Abuse.[14] The SSAC published the SAC115 report proposing a general framework of best practices to streamline the DNS abuse handling process within and beyond the ICANN and broader Internet communities.[15] ALAC provided advice on the matter of DNS Abuse in 2019, proposing

---

[12] "Bylaws for Internet Corporation for Assigned Names and Numbers," *ICANN org,* 9 January 2025, http://www.icann.org/general/bylaws.htm#AnnexA.

[13] "GNSO Council Resolutions 2025-08-14," *ICANN GNSO,* 14 August 2025, https://icann-community.atlassian.net/wiki/x/RKifBg.

[14] "GAC Communiqué – Prague, Czech Republic," *ICANN GAC,* 16 June 2025, https://gac.icann.org/contentMigrated/icann83-prague-communique.

[15] "SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS," *ICANN SSAC,* 19 March 2021, https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-115-en.pdf.

eight recommendations to the ICANN Board.[16] In 2018, the DNS Abuse Review Team provided an overview on DNS abuse during the initial three years of the New gTLD Program (2014-2016), comparing rates in new and legacy gTLDs, and explored methods for evaluating the effectiveness of safeguards designed to mitigate malicious activities in the Domain Name System.[17]

## 2.5 Issue under consideration

The Small Team identified several gaps in existing DNS Abuse mitigation frameworks. These gaps highlight that despite recent significant improvements, issues remain in current DNS Abuse mitigation efforts. In this context, the Small Team uses the term "gap" to denote an area flagged by the data and document review as potentially warranting further analysis, but not necessarily an "issue" in the ICANN Policy Development sense. A gap may or may not merit policy action; some may be better addressed through best practices, or no action at all. Accordingly, the Small Team recommended that these gaps be examined in the Issue Report to determine whether they are suitable for policy development or more appropriate for alternative follow-up. The Small Team believes that many of these gaps lie squarely within the GNSO's policy development remit and merit structured policy consideration. However, it is likely that some identified gaps might not be best addressed via Consensus Policies but could be addressed via other recommendations, such as non-binding best practices, or even mechanisms outside of policy development.

The purpose of the gap overview by the Small Team was to systematically capture what could be considered a gap in DNS Abuse mitigation across the entire domain lifecycle (as introduced by the DNS Abuse Small Team in 2022), from registration through enforcement.

## 2.6 Legal scope to launch Policy Development Process

Based on the documentation above, the launch of a dedicated PDP to consider the issues identified in this Preliminary Issue Report has been confirmed by ICANN's General Counsel to be properly within the scope of the GNSO as well as the ICANN Policy Development Process.

---

[16] "ALAC Advice on DNS Abuse," *ICANN ALAC*, 24 December 2019, https://atlarge.icann.org/en/advice_statements/13747.

[17] "DNS Abuse Review – New gTLDs 2012 Program," *ICANN org,* Updated 18 February 2018, https://newgtlds.icann.org/en/reviews/cct/dns-abuse.

# 3 Discussion of Issues

## 3.1 Overview of Issues

This section provides an overview of all relevant issues related to the GNSO Council request for this Preliminary Issue Report. In addition, it provides references to relevant documentation, ongoing and completed work efforts, and other applicable information.

### 3.1.1 Introduction: Organizing the Gaps/Issues and How to Consider Them

This section provides a deeper level discussion of the DNS Abuse mitigation gaps identified by the GNSO Council's Small Team and is supported by Staff research.[18] It is organized according to the **phases of the DNS Abuse mitigation lifecycle**, as introduced earlier and in the DNS Abuse Small Team Report to Council.[19] Organizing the issues by lifecycle phase helps illustrate who is primarily responsible for abuse mitigation at each stage and where in the process the gaps occur.[20]

The phases are:
- **Phase 0: Preventative Measures** (before a domain is maliciously used – the registration stage, aiming to prevent malicious domains from entering the DNS);
- **Phase 1 & 2: Abuse Reporting** (when abuse is observed, how it is reported and routed to the appropriate party, and ensuring the reports are actionable);
- **Phase 3: Mitigation by Contracted Parties** (once an abuse report is received by a registrar/registry, the actions taken to stop the abuse, per contractual obligations or best practices);
- **Phase 4: ICANN Compliance Enforcement** (if the responsible registrar/registry fails to act, how ICANN enforces the contracts to ensure abuse is mitigated).

In addition to these lifecycle phases, the discussion includes cross-cutting categories such as:
- **Community Collaboration** (issues that require broad coordination (not just a single contracted party's action), such as handling DGA botnet domains);
- **Data & Transparency** (issues that underpin all phases, focusing on information-sharing, reporting, and research).

---

[18] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

[19] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

[20] "DNS Abuse Small Team Report to GNSO Council," *ICANN GNSO*, 7 October 2022, https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf.

For each gap or issue, the report provides:

- a description of the gap,
- its origin or source (e.g., which report or community input highlighted it, research on gap),
- why it is considered a gap (implications or consequences if the gap were to remain unaddressed).

The list of gaps and accompanying discussion of them in this Issue Report are based on the work initiated by the DNS Abuse Small Team, particularly the preliminary gap matrix developed in the course of its 2025 mandate. That matrix was constructed through an initial review of source materials as referenced in the group's assignment form. In preparing this Preliminary Issue Report, the Staff Manager has conducted additional research and review to validate, refine, and supplement the original entries. Where appropriate, gaps that initially appeared as distinct have been consolidated into one gap discussion, particularly where the substance or intent of those gaps significantly overlapped. These consolidations are indicated in the respective gap and text below. To maintain traceability and alignment with the original matrix, this report references the original Gap IDs (e.g., P1) used in the Small Team matrix.[21] This allows community members and stakeholders to map the content of the report directly to earlier work.

Finally, the report also considers the **nature of potential solutions** for each gap: whether it likely calls for a Consensus Policy (contractual requirement), or could be handled via best practices, or other means. The Issue Report's role is not to decide the solution, but to outline the possibilities. Drawing such distinctions will aid the Council in deciding the appropriate mechanism (if any) for each group of issues and may help establish a starting point.

The **nature of potential solutions** as captured in the PDP Manual notes that a PDP may recommend a wide range of outcomes to the GNSO Council, including Consensus Policies, non-binding best practices, implementation guidelines, technical specifications, and recommendations on future policy development activities. In some instances, it may be equally appropriate to pursue certain solutions outside of the PDP, including the development of best practices.[22]

Moreover, recent studies and community-driven analyses indicate that closing specific mitigation gaps could contribute meaningfully to reducing DNS abuse in gTLDs.[23] This is a shared objective across the ICANN community and is aligned with ICANN's mission to ensure the stable and secure operation of the DNS.

---

[21] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

[22] "GNSO Policy Development Process Manual," *ICANN org,* Version 2.6, pg, 57, https://gnso.icann.org/sites/default/files/filefield_38869/annex-2-pdp-manual-16may13-en.pdf.

[23] See: Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf. And "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

For reference, effective 5 April 2024, global amendments to the RAA and RA introduced **new DNS Abuse mitigation requirements**.

These updates:

- **Define DNS Abuse** for the purpose of the RAA and the RA as malware, botnets, phishing, pharming, and spam used to deliver any of the other four types of DNS Abuse.[24]
- **Require mitigation actions** to stop or disrupt well-evidenced DNS Abuse.
- **Clarify** that abuse contact information must be easy to find.
- **Require** the provision of receipt confirmation for abuse reports.

### Preventative Measures (Phase 0)

Preventative measures refer to steps taken prior to, during, or immediately after domain registration to reduce the likelihood of the domain name being used to perpetrate DNS Abuse (e.g. a malicious registration). The focus is on proactive steps that can be taken in the domain acquisition process or other proactive security practices to reduce the likelihood of harm. The underlying idea is that once a domain is activated in the DNS and starts to be used to cause harm to users, damage can happen quickly; therefore, preventing such domains from being registered or being activated in the DNS would be the best case scenario. However, preventative measures must be balanced against the need for an open and accessible domain name marketplace; overly onerous checks could hinder legitimate registrations.

The gaps identified here include:

- **P1: Unrestricted Access to Application Programming Interface (APIs) allowing for high-volume registrations**
    - **Description:** Malicious actors use ungated access to APIs to register large volumes of domains in a matter of minutes, enabling large-scale phishing, smishing, and botnet operations. Many registrars require some sort of friction before a new customer account has access to an API where it can create thousands of names at once (e.g., restrict access to an API until the customer has more than three transactions not flagged as fraudulent or engaged in DNS Abuse). Some registrars allow brand-new accounts to access these bulk registration capabilities without any meaningful checks.
    - **Research on Gap:** According to studies such as INFERMAL, insufficient gating or friction for new users to access these tools can lead to the proliferation of DNS

---

[24] SAC115 defines each of these DNS Abuse forms. ICANN used the definition of those terms (malware, botnets, phishing, pharming, and spam used to deliver abuse) named in SAC115 to shape its definition for the purpose of the RA and RAA."SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS," *ICANN SSAC,* 19 March 2021, pp. 12-13, https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-115-en.pdf.

Abuse.[25] The availability of APIs for domain registration and account management seems to be strongly associated with a higher volume of malicious registrations according to INFERMAL.[26] Specifically, registrars that provided unrestricted API-based registrations saw a significantly elevated risk of phishing domains: "API access was linked to a 401 percent increase in malicious domain registrations" relative to a baseline in the study.[27] In other words, the study found that the presence of easy automation (via APIs) can multiply the likelihood of abuse by roughly four times, all else being equal. By contrast, the study noted that registrars employing restrictions on API usage for unverified users or requiring some form of vetting saw lower abuse rates.

- **Potential Solution:** This was named as a high-priority topic by the DNS Abuse Small Team for a potential PDP. The Netbeacon Institute's White Paper noted that easy API access without vetting "allows for the rapid setup of malicious infrastructures" and suggests a PDP on adding lightweight but effective friction points on API access to ensure that registrants, particularly new or untrusted accounts, cannot immediately access high-volume domain registration tools.[28] The proposal from the Netbeacon White Paper is to introduce **friction for new registrants or accounts before they can conduct high-volume registrations**.[29] According to the Netbeacon White Paper, policy could seek to introduce friction to slow abuse at scale, such as requiring new registrants to pass a basic trust threshold at the registrar before gaining access to programmatic registration tools. Such thresholds could include (i) requiring that a registrant has held one or more domains through the Add Grace Period without action for DNS Abuse, (ii) implementing waiting periods for newly created accounts, (iii) denying access to high-speed and/or high-volume registration methods for existing customers, if the customer has had domains which the registrar has identified as being

---

[25] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

[26] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

[27] Note: Percentages like the 401 percent increase associated with API access must be interpreted within the full statistical context. GLMs account for interactions among all variables. These results do not imply a standalone causal relationship but rather an observed correlation while holding other factors constant. Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

[28] "White Paper: Proposal for PDPs on DNS Abuse," *NetBeacon Institute*, May 2025, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

[29] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, p. 13, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

maliciously registered DNS Abuse.[30] This approach would aim to balance the need to prevent abuse with the legitimate use of high-volume registration by trusted entities.[31] Furthermore, the Netbeacon White Paper research 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 have they had reports of abuse) is more robust, reliable, and easier to implement than attempts at customer verification.[32] However, the PDP should consider that effectively all transactions at wholesale registrars are via API. This policy would need to differentiate between retail API access, and API access where a signed reseller agreement is in place. Introducing friction here could avoid the task of defining exactly how many domains qualify as a "bulk registration".[33]

- **P2 and P3: Lack of Proactive/Timely Contact Verification:**
    - **Description:** ICANN's existing RAA[34] requires some validation of registration data (e.g., verifying that an email or phone number is in correct format, and verifying email/phone operability under certain circumstances), but the **effectiveness and timeliness of these checks seem to vary** according to the INFERMAL study.
    - **Research on Gap:** The INFERMAL study found that some tested registrars did not fully perform syntactic checks on contact info, and operational validation (e.g., ensuring a phone number works) was sometimes lacking.[35] Additionally, the **requirement for registrars to verify contact info (e.g., email) after registration** allows up to 15 days for the registrant to respond, which an attacker can exploit to carry out abuse before the verification deadline. The INFERMAL study results suggest that proactive or timely (e.g., during or prior to registration) verification can reduce DNS abuse by a significant amount based on the test dataset and method.[36]
    - **Potential Solution:** The GNSO Council Accuracy Small Team recommended to Council "examining the existing process for validating and verifying registration

---

[30] White Paper: Proposal for PDPs on DNS Abuse," *NetBeacon Institute*, May 2025, p. 12, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

[31] White Paper: Proposal for PDPs on DNS Abuse," *NetBeacon Institute*, May 2025, p. 7, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

[32] White Paper: Proposal for PDPs on DNS Abuse," *NetBeacon Institute*, May 2025, p. 13, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

[33] White Paper: Proposal for PDPs on DNS Abuse," *NetBeacon Institute*, May 2025, p. 10, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

[34] "2013 Registrar Accreditation Agreement," *ICANN org*, 21 January 2024, https://www.icann.org/en/contracted-parties/accredited-registrars/registrar-accreditation-agreement

[35] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, p. 9, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

[36] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, p. 14, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

data under the 2024 Registrar Accreditation agreement[37] and the potential impact on registrants if this process is modified."[38] Some members of the DNS Abuse Small Team noted it as a priority topic for a PDP. Addressing this would require further policy work. If this would be included in a future PDP on DNS Abuse, it could address work related to Accuracy as well.

- **P5. Minimal Deterrent Effect of Reactive Measures ("Uptime"):**
    - **Description:** "Uptime" refers to the duration a website, server, or application is operational and accessible to users. Shorter uptimes of malicious domains should ideally discourage attackers from using certain TLDs and registrars, as swift suspension might drive them to seek alternatives. However, it seems that even brief activity may yield valuable credentials and financial gain, potentially diminishing the impact of reactive security measures on their registrar choices.
    - **Research on Gap:** This was noted in the INFERMAL study's finding that even very fast takedowns of malicious domains (e.g., within hours) may not deter attackers sufficiently.[39] According to the study, reactive mitigation has only a limited impact on attacker behavior and may not impose enough cost on them to serve as a deterrent. While promptly suspending malicious domain names is essential for mitigating potential harm, the INFERMAL study analysis shows that longer uptime has only a marginal effect on the concentration of malicious domains and minimal impact on the attacker choice of a registrar or TLD.[40]
    - **Potential Solution:** This gap suggests that improving preventative measures has more impact on reducing DNS Abuse. Therefore, this gap does not appear to warrant any specific solution.
- **P6. Challenges in Real-Time Detection of Short-Lived Abuse:**

---

[37] The terms validation and verification within this recommendation refer to the current definitions and associated requirements within the RDDS Accuracy Program Specification of the Registrar Accreditation Agreement (RAA). Specifically, validation requirements are defined in Section 1(a) - 1(d) of the RDDS Accuracy Program Specification, and the verification requirements are defined in Section 1(f) of the RDDS Accuracy Program Specification. "2013 Registrar Accreditation Agreement," *ICANN org*, 21 January 2024, https://itp.cdn.icann.org/en/files/accredited-registrars/registrar-accreditation-agreement-21jan24-en.htm#rdds-accuracy.

[38] "GNSO Council Accuracy Small Team Summary Report," *ICANN GNSO,* 31 July 2025, https://gnso.icann.org/sites/default/files/policy/2025/draft/gnso-council-accuracy-small-team-summary-31jul25-en.pdf

[39] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, p. 4, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

[40] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, p. 14, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

  - **Description:** This issue relates to the technical challenge that many abuse detection systems (blocklists, DNS query analysis) have a lag. Some systems rely on DNS zone file updates or aggregated data that may only show a domain after it is active for a relatively long period of time.[41] However, a significant challenge known as the "fast-flux" technique is often associated with the use of "one-hour domains" or "one-day" lifespans.[42] Attackers utilize fast flux techniques to rapidly change the IP addresses associated with a domain name, making it difficult to block malicious sites using traditional IP blocking methods. These rapid changes in IP addresses also make it harder for investigations to trace the origin of malicious content. Detection can be challenging when the evidence of abuse is insufficient or takes time to gather. Depending on the timing of notification, it may be too late to gather necessary evidence and take action. Attackers constantly evolve their techniques and tactics, making it harder for existing detection systems to keep up.
  - **Research on Gap:** Traditional abuse detection systems, including blocklists and DNS query analysis, often rely on retrospective data.[43] This data can be gathered through DNS zone file updates, which are not instantaneous, or through aggregated threat intelligence that takes time to compile and disseminate.
  - **Potential Solution:** Overall, combating short-lived DNS abuse requires a multi-layered approach that combines advanced detection techniques with proactive monitoring, information sharing, and rapid response capabilities. Thus, this might be tackled outside policy (e.g., through technology improvements or threat intel sharing), but shows that, similar to the gap above, focusing or introducing more preventative measures can reduce DNS Abuse more effectively than reactive measures.

- **P7. Underuse of Predictive Algorithms for Early Detection:**
  - **Description:** Crime often involves patterns that, if recognized, could be identified and acted upon to prevent abuse (e.g., many throwaway domains registered with similar names or from the same subnet). Predictive algorithms can look at patterns like certain keywords (e.g., “login-<brand>” domains), suspicious registrar account behavior, known bad IP addresses to flag domains for review or suspension before they start abusing.[44]
  - **Research on Gap:** The Small Team’s review in 2022 indicated that apart from examples from outside the immediate ICANN community such as Classification

---

[41] Ali, Anas, Mubashar Husain, and Peter Hans, “Real-Time Detection of Insider Threats Using Behavioral Analytics and Deep Evidential Clustering,” *ArXiv*, 21 May 2025, https://arxiv.org/html/2505.15383v1.

[42] “What is DNS Fast Flux?,” *Cloudflare*, https://www.cloudflare.com/en-gb/learning/dns/dns-fast-flux/.

[43] Gañán, Carlos Hernández,, “How Choice of Reputation Blocklists Affects DNS Abuse Metrics, *ICANN org,* 7 July 2025, https://www.icann.org/en/blogs/details/how-choice-of-reputation-blocklists-affects-dns-abuse-metrics-07-07-2025-en.

[44] “DNS Abuse Small Team List of Gaps,” *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

of Compromised versus Maliciously Registered Domains (COMAR), Logo collision and EU Common Logo the Small Team was not aware of any ICANN community work being undertaken on this topic.[45] However, the Small Team noted that predictive algorithms may be useful but there is always the potential for false positives and the negative impact these may have on registrants.

  - **Potential Solution:** The Small Team in 2022 observed that the above suggestion is a possible solution that could be further explored by ICANN org and contracted parties. However, if such a solution would be developed and made available to contracted parties, incentives could be explored to encourage adoption.[46] Some companies/organizations likely use predictive systems (e.g., some large registrars have internal fraud detection and some registries collaborate with security firms to vet registrations in sensitive TLDs). Contractually requiring specific security measures based on an algorithm may be challenging, given the chance for false positives and the reality that technology-specific mandates can quickly become outdated. Given 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:**
  - **Description:** 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. The RAA contains obligations related to contactability, not confirming identity. ICANN Contractual Compliance will investigate allegations received through complaints or indications that the registration data associated with a domain name is inaccurate.
  - **Research on Gap:** The NIS[47] Cooperation Group suggests that a risk-based approach could be used to verify the name of the registrant at registration and renewal, but the group is not recommending that "all" new and renewing domains are subject to identity checks, only where they are flagged for medium or high risk.[48] The 2022 DNS Abuse Small Team noted "that 'Know Your Customer' (KYC) measures could play an important role in addressing DNS

---

[45] "DNS Abuse Small Team Report to GNSO Council," *ICANN GNSO*, 7 October 2022, p. 12, https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf.

[46] "DNS Abuse Small Team Report to GNSO Council," *ICANN GNSO*, 7 October 2022, p. 13, https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf.

[47] The Network and Information Systems (NIS) Cooperation Group was established by the NIS Directive to ensure cooperation and information exchange among EU Member States. The group provides non-binding guidelines to the EU Member States to allow effective and coherent implementation of the NIS Directive across the EU and to address wider cybersecurity policy issues. "NIS Cooperation Group," *European Commission,* https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group.

[48] "NIS Cooperation Group Recommendations for the implementation of NIS2 Directive Article 28 (Database of domain name registration data)," *NIS Cooperation Group*, September 2024, https://ec.europa.eu/newsroom/dae/redirection/document/108437.

Abuse. However, there is currently little visibility on which KYC measures may be applied by Contracted Parties and what effect these may have on DNS Abuse. Further information on this topic may help identify whether further action is helpful in this area."[49] The INFERMAL study noted certain registries verify registrants' identities to ensure compliance with local regulations and to enhance the overall security of their domain ecosystem. For instance, when the CNNIC[50] mandated formal documentation (previously known for being attacked by spammers frequently)[51] and validation for individual registrations, it significantly reduced spam domains under the .cn TLD.[52] Intuitively, attackers would avoid such TLDs and registrars. However, if these practices were implemented globally, malicious actors might adapt by resorting to identity theft for fraudulent registrations or compromising legitimate websites.[53]

  - **Potential Solution:** In order to close this gap via binding requirements, policy development would be needed. However, the practice could also be encouraged via inclusion in a non-binding best practices document.

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

  - **Description:** According to the INFERMAL study's conclusions, economic incentives, such as registration discounts, are associated with an increase in the number of malicious registrations.[54] By leveraging low-cost options, attackers can maximize their return on investment, especially given the short lifespan of these domains before they are suspended. Similar to pricing, offering free add-on services can inadvertently facilitate abuse. For example, some registrars provide free DNS hosting, free email, free SSL certificates, or free Whois privacy by default. These incentives, while valuable to legitimate users, also allow criminals to set up functioning malicious sites with almost no cost, while also being able to hide their identity.

---

[49] "DNS Abuse Small Team Report to GNSO Council," *ICANN GNSO*, 7 October 2022, p. 13, https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf.

[50] "Advantages of a .CN Domain Name," *CNNIC*, 22 September 2003, https://www.cnnic.com.cn/IS/CNym/CNymzc/201208/t20120823_35222.htm.

[51] Liu, He (Lonnie), et al., "On the Effects of Registrar-level Intervention," *LEET '11*, 29 March 2011, p. 4 https://klevchen.ece.illinois.edu/pubs/llfkmvs-leet11.pdf.

[52] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, p. 7, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

[53] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, p. 7, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

[54] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, p. 13, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

  - **Research on Gap:** The INFERMAL study's statistical analysis reveals that nearly half of maliciously registered domains cost $2 USD or less. The presence of discounts raises the likelihood of domains being registered for malicious purposes. Even if discounts are limited to new users, attackers may exploit free APIs to automate account creation and domain registration at discounted prices.[55] The study noted that free services are more likely to be abused by threat actors and based on its analysis model demonstrates that free services (web hosting and DNS) significantly increase the number of malicious registrations, indicating that they lower entry barriers for attackers, allowing them to set up and maintain malicious domains with minimal expense.[56] However, the study also noted that while initial pricing plays a role, attractiveness to attackers likely results from a combination of factors, not just pricing. If a business is engaging in a multitude of practices, there might be a compounding effect that may actively encourage attackers to choose a specific registrar/registry for their purposes.
  - **Potential Solution:** The gap here is essentially how to mitigate the "abuse side-effects" of discount regimes and other economic incentives, since pricing strategies and free add-on services are a business decision and considered outside the scope of ICANN's policymaking remit. 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.
  - **Relation to other gaps in the DNS Abuse Small Team Matrix: E4. Abuse concentrated in a small number of registrars** The gaps here are acknowledging that a small number of registrars have a disproportionately high abuse volume.[57] As noted above, if these registrars were better aware of best practices and adjusted some of their practices, abuse may drop. The gap is understanding the factors that lead to abuse concentration and addressing those factors.

- **P11. Limited Use of Abuse Feeds/Threat Data for Prevention:**
  - **Description:** This gap identifies that registrars/registries are seemingly not consistently using abuse feeds data to inform domain-level restrictions or

---

[55] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, p. 13, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

[56] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, p. 13, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

[57] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

validation rules.[58] This is somewhat related to P7 (predictive algorithms) and P6 (challenges in real-time detection of short-lived abuse).

- **Research on Gap:** Currently, use of such data is optional and varies widely. DNS Abuse measurements and incident response are often based on domains listed on Reputation Block List (RBLs). An ICANN analysis notes different blocklists have limited visibility, and there seems to be little overlap between them, creating blind spots in abuse detection and measurement.[59] Open-source lists, maintained by volunteer communities or public projects, rely on user reports and open feeds. While transparent and broadly accessible, they often miss abuse that escapes their contributors' notice. In contrast, commercial blocklists, curated by security vendors, leverage proprietary data and advanced analytics for deeper, faster insights into emerging attacks. However, their visibility is shaped by collection infrastructure, customer networks, and intelligence partnerships, leading to unique blind spots of their own.[60] This fragmentation can have far-reaching implications for how DNS Abuse metrics and global trends are interpreted.
- **Potential Solution:** While these data sources can be a helpful tool, imposing their usage may not be ideal; integrating into best practices would help contracted parties benefit from the usage of data sources as appropriate for their business. This gap was named as high priority by some members of the DNS Abuse Small Team. Given limitations in data feeds (e.g., timing lag and blind spots), it is difficult to envision a practical "uniform or coordinated resolution" for their usage. To mitigate the fragmentation to a degree, ICANN's Domain Metrica system aggregates data from multiple RBLs to assess abuse rates across registries and registrars. ICANN Domain Metrica, launched in February 2025, aims to improve the way domain data is captured, measured, analyzed, and shared.[61]
- **Relation to other gaps in the DNS Abuse Small Team Matrix: DT1, Lack of Transparency on Abuse Trends:** Some SGs noted there is not a comprehensive, agreed-upon public metric or reporting of DNS Abuse per registry/registrar. Some SGs have called for more publicly available data on abuse trends.[62] Some

---

[58] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

[59] Lloyd, Siôn, Carlos Hernández Gañán, and Samaneh Tajalizadehkhoob, "RBL Evaluation Methodology," *ICANN org*, 11 December 2023 https://www.icann.org/en/system/files/files/octo-037-11dec23-en.pdf.

[60] Gañán, Carlos Hernández, "How Choice of Reputation Blocklists Affects DNS Abuse Metrics, *ICANN org,* 7 July 2025, https://www.icann.org/en/blogs/details/how-choice-of-reputation-blocklists-affects-dns-abuse-metrics-07-07-2025-en.

[61] "ICANN Domain Metrica: A Measurement Platform," *ICANN org,* https://www.icann.org/octo-ssr/metrica-en.

[62] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

such reporting exists: ICANN’s Domain Metrica project provides daily data on abuse rates per TLD. This might be better addressed under best practices or community collaboration.

In summary, **Phase 0 preventive measures gaps** highlight that the current DNS registration system is relatively open and with limited friction requirements, which has the benefit of ease of use, but the drawback of being sometimes easily exploited by threat actors. The identified gaps point toward introducing targeted friction, smarter screening and addressing business practices that may inadvertently encourage abuse. As the report considers policy development, one key question is: which of these should be mandatory Consensus Policies vs. which are better as optional best practices? The Small Team and Staff acknowledge that **not all preventive measures may be appropriate for Consensus Policy** (due to technical, legal, or operational practicality reasons). However, including these gaps here ensures they are not overlooked, and it allows the GNSO Council or a future Working Group to decide what to recommend formally or informally.

### Abuse Reporting (Phases 1–2)

In the DNS Abuse lifecycle, “Phase 1” can be described as the stage where an abuse event is noticed by someone (an Internet user, a security researcher, law enforcement, etc.) and needs to be reported to the party that can take action, and “Phase 2” involves ensuring the report itself is well-formed and contains what’s needed for action.[63] The 2022 Small Team separated these, but for this report`s discussion these two phases were combined under **Abuse Reporting** generally. Effective abuse mitigation depends on an efficient flow of information: the right complaint has to reach the right actor with the right evidence. If any of those elements fail, abuse may not be resolved promptly or efficiently.

The gaps identified here include:

- **A1. Unactionable Complaints to ICANN:**
    - **Description:** Between 70% and over 80% of abuse complaints ICANN Contractual Compliance have closed since the new DNS Abuse mitigation requirements became effective did not result in investigations being initiated with a registrar or registry operator. Most complaints refer to phishing, either alone or in combination with other types of abuse.[64] The CPH/CSG abuse reporting workshop at ICANN 82 suggested there’s still room for improvement on how to report phishing to registrars (and registries when appropriate). Phishing reports that are incomplete, or incorrectly evidenced, can create a bottleneck in contracted parties' anti-abuse team queues.

---

[63] “DNS Abuse Small Team Report to GNSO Council,” *ICANN GNSO*, 7 October 2022, https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf.

[64] Castillo, Leticia, “ICANN's Enforcement of DNS Abuse Requirements Six Months” *ICANN org*, 8 November 2024, https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf. And Castillo, Leticia, Rómulo Chacín, and Charmaine Lim, “Enforcement of DNS Abuse Mitigation Requirements - A Look at the First Year,” *ICANN org*, 23 April 2025, https://icanncrm.my.salesforce.com/sfc/p/#1a000000Y7OU/a/Qk000001geDN/9sof6KwBYa_N6kv4nnFTAiWuHValPVrAZYrnTXY8gGc.

  - **Research on Gap:** The complaints ICANN Contractual Compliance closed without initiating an investigation with a contracted party (CP) lacked evidence required by ICANN, including any indicator that the domain name was engaged in DNS Abuse or that the reported activity was ever reported to or known by the CP. Other complaints involved country-code top level domain (ccTLD) names, were duplicative or related to domain names that had already been mitigated or were no longer registered, while other complaints involved customer service disputes between the complainant and a registrar or a third party, among other issues.[65] This indicates a lack of understanding among many complainants about the proper channel or how to properly report DNS Abuse in a way that can be promptly acted on.
  - **Potential Solutions:** This gap might be addressed through best practices or educational initiatives rather than policy development. For instance, the CPH "Guide to Abuse Reporting" could help users send actionable reports to the right place.[66] Additionally, ICANN Contractual Compliance has conducted presentations[67] on how to submit actionable complaints to ICANN and is preparing to publish related guidelines shortly. The 2022 Small Team recommended encouraging parties to improve abuse reporting tools, which has happened to some extent already. For instance, there is Netbeacon Reporter, a centralized abuse reporting platform launched by Netbeacon, intended to streamline reporting and route it properly.[68] This gap was named as a high-priority topic by some DNS Abuse Small Team members.

- **A3. Malicious vs. Compromised - Clarifying Responsibility:**
  - **Description:** A distinction is made between a maliciously registered domain, where the domain itself was registered with bad intent, versus compromised legitimate domains, where a legitimate domain/account gets hacked to host phishing or malware unbeknownst to the owner. The mitigation pathways differ for malicious registrations, where the registrar/registry can suspend or delete the domain. For compromised domains, the registrar cannot fix the hacked website; the solution often lies with the hosting provider or the registrant cleaning their site. If policies are crafted without this distinction, it may either overstep (e.g., expecting registrars to fix compromised domain names that they

---

[65] Castillo, Leticia, "ICANN's Enforcement of DNS Abuse Requirements Six Months" *ICANN org*, 8 November 2024, https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf. And Castillo, Leticia, Rómulo Chacín, and Charmaine Lim, "Enforcement of DNS Abuse Mitigation Requirements - A Look at the First Year," *ICANN org*, 23 April 2025, https://icanncrm.my.salesforce.com/sfc/p/#1a000000Y7OU/a/Qk000001geDN/9sof6KwBYa_N6kv4nnFTAiWuHValPVrAZYrnTXY8gGc.

[66] "CPH Guide to Abuse Reporting Practices v1.0," *ICANN RrSG and RySG*, 2022, https://rrsg.org/wp-content/uploads/2022/01/CPH-Guide-to-Abuse-Reporting-v1.0.pdf

[67] Castillo, Leticia, Rómulo Chacín, and Charmaine Lim, "Enforcement of DNS Abuse Mitigation Requirements - A Look at the First Year," *ICANN org*, 23 April 2025, https://icanncrm.my.salesforce.com/sfc/p/#1a000000Y7OU/a/Qk000001geDN/9sof6KwBYa_N6kv4nnFTAiWuHValPVrAZYrnTXY8gGc.

[68] "NetBeacon Reporter," *NetBeacon Institute*, https://netbeacon.org/reporting/.

cannot fix) or leave gaps (e.g., not adequately addressing malicious domains firmly enough because of wariness of compromise scenarios).

- **Research on Gap:** In 2022, the Small Team suggested that any policy efforts explicitly scope to malicious registrations (which are within ICANN's remit) and avoid areas that require content takedown or website cleanup (which are not in ICANN's remit).[69] The new DNS Abuse contract obligations actually require mitigation for both malicious or compromised domain names but allow flexibility in how (e.g., the contracted party is not expected to remove content but could, for instance, suspend a compromised domain after notifying the registrant if that is the best course of action).
- **Potential Solution:** The 2022 Small Team suggests distinguishing between malicious vs. compromised registrations when considering what topics may fall within the scope of ICANN to address. Taking this approach would ensure that responsibility for taking action on malicious registrations is within the remit of contracted parties and/or ICANN, while action on compromised registrations may require involvement of actors that are not subject to ICANN agreements.[70] This gap identification is thus about ensuring clarity of scope in response. It may not become a standalone policy item but will inform how other policies are crafted. For the Issue Report, it was included to acknowledge the nuance.

In summary, **reporting-phase issues** are largely about communication and ensuring the system to alert abuse is efficient. Many solutions here might be best practices, improved tools, and possibly making sure every registrar has an abuse web form or requiring timely automated acknowledgments to reporters. The GNSO can consider if a PDP's scope should include such "operational" improvements or if it should defer to community-led initiatives like best practices. In addition to preventing DNS Abuse e, improving reporting of DNS Abuse is essential to mitigating DNS Abuse. Evidence based, well-formed and appropriately routed reports underpin the rest of DNS Abuse mitigation.

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

Phase 3 concerns what the **well-positioned party** does once it has a DNS abuse report. In the context of ICANN policy, this typically means the registrar (or registry) that sponsors the abusive domain, since ICANN's contracts are with those parties. This phase corresponds to the new duties in the RAA/RAs that took effect in April 2024, which require prompt action to stop or disrupt DNS Abuse given evidence. The Small Team's gap list labels this category "Contractual Obligations – Well-positioned party takes action as necessary."

The gaps identified here include:

- **C1. Limited Transparency in Mitigation Actions taken:**

---

[69] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

[70] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

  - **Description:** After a registrar or registry acts on an abuse report (e.g., suspends a domain, or decides not to suspend), that information is generally not shared for various reasons, which can create difficulties in understanding the DNS Abuse landscape or for a "reporter" to understand what has happened to their report.

  - **Research on Gap:** The Netbeacon Institute noted a lack of detailed reporting on mitigation actions taken from contracted parties.[71] In their analysis of the ICANN contract amendments from 2024, Netbeacon noted measurement challenges, where their methodology was unable to determine whether or not mitigation occurred or which party took action. The presence of this "grey area" could mean that statistics on mitigation might be either overestimating or underestimating outcomes.[72]

  - **Potential Solution:** If the intention is to create minimum reporting requirements, this could be addressed by policy development. Another path could be developing best practices in this area. This gap is related to Gap C7, which notes registrants should be notified on "what action was taken".

  - **Relation to other gaps in the DNS Abuse Small Team Matrix: A2 and E1 Lack of Measurement Challenges: "Uncategorized" Abuse Outcomes and Disparate Registrar Abuse Mitigation Responses:** This might be better addressed under non-binding best practices or community collaboration. ICANN Compliance publishes monthly and ad hoc reports dedicated to DNS Abuse mitigation enforcement. As noted in its blog post accompanying the launch of these reports, ICANN Compliance welcomes community feedback.[73] Any feedback received is reviewed, and, where feasible, additional enhancements to ICANN metrics and reporting are implemented.[74]

- **C2. No Requirement to Check for Associated Domains:**

  - **Description:** Malicious domains are often part of broader campaigns involving dozens or hundreds of related domains. When a registrar finds that one domain is malicious, there is no contractual requirement that the registrar must investigate whether the same registrant or account has other active domains that are also being used for similar abuse.

---

[71] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

[72] "How Have the gTLD Contractual Amendments Impacted DNS Abuse," *NetBeacon Institute,* 16 December 2024, https://netbeacon.org/how-have-the-gtld-contractual-amendments-impacted-dns-abuse/.

[73] Castillo-Sojo, Leticia, "ICANN Launches Reports on the Enforcement of DNS Abuse Requirements," *ICANN org,* 28 June 2024, https://www.icann.org/en/blogs/details/icann-launches-reports-on-the-enforcement-of-dns-abuse-requirements-28-06-2024-en.

[74] Castillo, Leticia, "Responses to the GNSO Council Small Team on DNS Abuse," *ICANN org*, 26 June 2025, https://docs.google.com/document/d/1gTq-l7irOAt252jq2IvmJY6NGYIg2RliKO6jhKYI6jI/edit?tab=t.0.

  - **Research on Gap:** The Netbeacon White Paper suggested an "Associated Domain Check" requirement via a PDP.[75] Without this requirement, an attacker might only lose one domain at a time, continuing to use the rest until each is individually reported. If registrars proactively pivot on the information, it could curtail whole DNS Abuse campaigns. Some registrars likely do this voluntarily, but others may not due to lack of resources or fear of overreaching. The RAA currently only requires registrars to evaluate individual domain names when they obtain evidence that the domain name is being used for DNS Abuse.[76] This current "one-at-a-time" approach limits the mitigation of related domains operated by the same actor, even when those domains are part of an identifiable campaign.
  - **Potential Solution:** This gap was noted as high-priority for a consensus policy by the 2025 DNS Abuse Small Team. The Netbeacon White Paper proposes for a PDP to examine whether registrars, upon obtaining actionable evidence that a domain name is used for DNS Abuse, should be required to review other domain names within the same account and/or registered by the same registrant. This "pivot" approach could help identify and mitigate related DNS Abuse more effectively, particularly in organized campaigns (including those registered in bulk to conduct such campaigns).[77] Once a registrar identifies additional domains engaged in DNS Abuse in the customer account, its existing obligations in the RAA (set forth in Section 3.18) will require the registrar to mitigate or otherwise disrupt the abuse, provided there is actionable evidence associated with each additional identified abusive domain. This approach could also create an incentive structure: registrars that permit unrestricted access to automated registration tools (e.g., ungated APIs) for high-volume customers, or employ other low-friction practices, would now bear a cost for enabling malicious portfolios. Furthermore, investigating multiple domains separately can be more resource intensive (in terms of time and resources) than investigating them all in one single case. This is why the Netbeacon White Paper believes that the Associated Domain Check could also have a meaningful preventative impact (in relation to P1) on the presence of malicious campaigns.[78] It will be particularly important for this topic to ensure that any policy recommendations will be implementable and contractually enforceable; the potential solutions and their feasibility must be considered during the PDP deliberations.

- **C3. Lack of Standard Dispute/Recourse Mechanism for Registrants:**
  - **Description:** When a domain name is suspended due to DNS Abuse, registrants currently lack a process to request that the registrar or registry review its decision. While swift action is often necessary to combat DNS Abuse, the

---

[75] White Paper: Proposal for PDPs on DNS Abuse," *NetBeacon Institute*, May 2025, p. 14, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

[76] "2013 Registrar Accreditation Agreement," *ICANN org*, 21 January 2024, https://itp.cdn.icann.org/en/files/accredited-registrars/registrar-accreditation-agreement-21jan24-en.htm

[77] White Paper: Proposal for PDPs on DNS Abuse," *NetBeacon Institute*, May 2025, p. 6, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

[78] White Paper: Proposal for PDPs on DNS Abuse," *NetBeacon Institute*, May 2025, p. 13, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

absence of a clear channel for registrants to seek recourse (particularly in the case of mistaken or disputed suspensions) can lead to unnecessary harm, reputational damage, or loss of legitimate services.[79]

  - **Research on Gap:** The Netbeacon White Paper notes that suspensions for DNS Abuse are sometimes contested by registrants, particularly when decisions are made based on limited or incomplete information. Nonetheless, it seems that across the industry, there is no standard expectation that a registrar or registry must provide a process for recourse. In many cases, registrants are left with no way to communicate their perspective, even when legitimate harm is done.[80]

  - **Possible solutions:** This gap was named as a high-priority topic by some members of the DNS Abuse Small Team. The Netbeacon White Paper lists "Registrant Recourse Mechanisms" as one of its proposed PDPs.[81] According to the White Paper, this PDP would aim to establish a baseline process for registrant recourse, ensuring that registrars and registries provide a means for registrants to submit evidence and request a review of a suspension. Registries and registrars would then be required to review any relevant and actionable evidence submitted by the registrant in order to consider whether to lift a suspension. This would not compel the lifting of any suspension, but it would ensure registrants have a meaningful opportunity to be heard, without undermining DNS Abuse mitigation efforts. The White Paper notes that an outcome of the PDP could have the following elements (i) maintain a publicly available webform or email address through which registrants can request review, (ii) be willing and able to accept and review evidence submitted by the registrant, (iii) evaluate the submission in good faith, with the discretion to maintain or lift the suspension based on the merits of the evidence.

- **C4. Unregulated Subdomain Abuse:**

  - **Description:** This gap refers to the scenario where the registrant uses their domain to offer subdomains to the public (either free or paid). The problem that may arise is that the registrar/registry deals with the main domain, but not the subdomains. Threat actors have shifted to exploiting services that generate subdomains. A threat actor could register one domain and then host dozens of phishing sites on subdomains, evading per-domain mitigation focus. The registry/registrar might see only one domain which by itself might not get reported if, say, each subdomain usage is short-lived. If a registrar or registry suspends a second-level domain in response to DNS Abuse, it risks disabling thousands, even hundreds of thousands of legitimate subdomains and any

---

[79] White Paper: Proposal for PDPs on DNS Abuse," *NetBeacon Institute*, May 2025, p. 17, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

[80] White Paper: Proposal for PDPs on DNS Abuse," *NetBeacon Institute*, May 2025, p. 12, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

[81] "White Paper Proposal for PDPs on DNS Abuse," *NetBeacon Institute,* 21 May 2025, https://netbeacon.org/white-paper-proposal-for-pdps-on-dns-abuse/.

connected services or infrastructure.[82] Subdomain hosting services are outside ICANN's direct remit.

- **Research on Gap:** The 2024 Interisle Phishing Landscape Report shows that 24% of all phishing attacks take place via subdomains.[83] The same report documents 454,948 phishing attacks created on just 750 second-level domains operated by subdomain providers.[84] A DNS Research Federation analysis found that 36.27% of phishing attacks use subdomain infrastructure belonging to a fraction of domain names pointing to a concentrated threat vector with limited oversight.[85] According to the Netbeacon White Paper, subdomain hosting services remain outside ICANN's direct remit, and registries and registrars often have no recourse unless the registrant's own policies provide a way to act.[86]

- **Potential Solution:** The Netbeacon White Paper suggests creating obligations for second-level registrants that operate services generating subdomains used by third parties. The aim here would be to create tools for registries and registrars to engage with and require action from registrants who offer services that generate subdomains engaged in DNS Abuse. The policy would not seek to restrict third-level domains directly. Instead, it would equip registrars and registries with tools - through contractual obligations - to better hold registrants accountable when subdomain infrastructure is used for abuse.[87] This proposal would require registrar and registry policies (i.e., terms of service or acceptable use policies) to include the following requirements for registrants operating services that generate subdomains used by third parties: (i) maintain a publicly available, monitored abuse reporting mechanism, such as an email address or web form, (ii) prohibit DNS Abuse on any associated subdomains in their own terms of service or similar policy, (iii) review and respond to credible abuse complaints concerning subdomain misuse, and (iv) implement internal processes or technical controls to mitigate abuse on third-level domains.[88]

---

[82] White Paper: Proposal for PDPs on DNS Abuse," *NetBeacon Institute*, May 2025, p. 14, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

[83] "Phishing Landscape 2024: An Annual Study of the Scope and Distribution of Phishing," *Interisle*, 23 July 2024, https://interisle.net/insights/phishing-landscape-2024-an-annual-study-of-the-scope-and-distribution-of-phishing.

[84] "Phishing Landscape 2024: An Annual Study of the Scope and Distribution of Phishing," *Interisle*, 23 July 2024, https://interisle.net/insights/phishing-landscape-2024-an-annual-study-of-the-scope-and-distribution-of-phishing.

[85] Deacon, Alex, "Use of Subdomain Providers Gains Popularity as a Mechanism to Launch Phishing Attacks," *DNS Research Federation*, 14 August 2023, https://dnsrf.org/blog/use-of-subdomain-providers-gains-popularity-as-a-mechanism-to-launch-phishing/index.html.

[86] White Paper: Proposal for PDPs on DNS Abuse," *NetBeacon Institute*, May 2025, p. 14, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

[87] White Paper: Proposal for PDPs on DNS Abuse," *NetBeacon Institute*, May 2025, p. 14, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

[88] White Paper: Proposal for PDPs on DNS Abuse," *NetBeacon Institute*, May 2025, p. 14, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

- **C6 and C7. Due Diligence and Transparency in Mitigation:**
    - **Description:** The Non-Commercial Stakeholder Group (NCSG) provided detailed input on how mitigation should be conducted to ensure fairness and minimize collateral damage. According to the NCSG, before taking action against a domain, the registrar should perform a proportionate investigation and ensure there is specific, actionable evidence of abuse.[89] They caution against instant suspensions and suggest to consider if a less drastic measure than suspension could suffice (e.g., maybe temporarily redirect or contact the registrant first if appropriate).[90] This NCSG perspective is about codifying a norm of careful assessment, which could possibly be a best practice. As noted in Gap C1, the NCSG suggests that if a domain is suspended or action taken, the registrar should promptly notify the registrant with clear information: the reason, what action was taken, who initiated it (registrar itself, law enforcement request, etc.), and explanation in plain language.[91]
    - **Potential Solution:** These considerations do not necessarily represent a gap in DNS Abuse mitigation since the scope of these is currently unclear due to the lack of data. Without fully understanding the scope of the issue, it's difficult to assess the best mechanism to mitigate the potential harms.
- **C8. Inconsistent Responses - Seeking Standardization:**
    - **Description:** The Commercial Stakeholders Group (CSG) noted in the DNS Abuse Small Team gap matrix that similar abuse complaints get very different responses depending on the registrar or registry involved.[92] For example, one registrar might respond within hours with suspension and a detailed reply, while another might take days and give a boilerplate answer or none. Thus, calling for more standardization of responses and timing, such as Service Level Agreements (SLAs) or at least guidelines so that the industry's performance becomes more consistent.[93]
    - **Potential Solution:** The amended ICANN contracts deliberately did not include rigid timelines, to allow flexibility. Instead, they say "promptly" and allow for case-by-case circumstances to dictate appropriate actions (e.g., the mitigation

---

[89] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

[90] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

[91] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

[92] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

[93] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

path for a compromised domain name may be very different than for a maliciously registered domain).[94] Different reports (even if they appear similar to some) and circumstances will naturally yield different responses, timing, and actions – including the level of detail provided in each response. This intentional flexibility in the agreements makes the establishment of SLAs challenging. Pursuing non-binding best practices may be more appropriate.

- ○ **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.** This gap came from the ICANN81 Contracted Party House (CPH)/CSG discussion: certain stakeholders want a hard rule that, say, within 24 hours of a valid abuse report, the registrar must take action (suspend or disable the domain).[95] Furthermore, some abuse reporters often note that they submit reports and do not hear back about the outcome, leading them to wonder if it was addressed. A standardized approach could be part of the abuse reporting tools (e.g., Netbeacon is already trying to show reporters the status if the registrar updates it).

Many of these gaps intersect with the changes made in the recent ICANN contract amendments. Some items like associated domain checks, recourse, and subdomains are not covered by the amendments and could be considered for new policy. Others might refine the implementation of the existing obligations and be well-suited for non-binding best practices.

### Enforcement by ICANN Contractual Compliance (Phase 4)

Phase 4 is when ICANN's Contractual Compliance department enforces the contracts if the abuse is not being properly mitigated by the contracted party. ICANN's Enforcement of DNS Abuse Mitigation Requirements details Contractual Compliance enforcement actions under the new DNS Abuse mitigation requirements. Upon their effective date, ICANN Contractual Compliance commenced vigorous enforcement of these new requirements. It is important to note that the enforcement of contractual requirements is one aspect of ICANN's multifaceted DNS Abuse Mitigation Program.[96] ICANN Contractual Compliance has processes and systems in place for complaint-based enforcement, along with a dedicated audit program featuring two audit rounds per year. The gaps in this phase touch upon the Compliance area, but are outside of ICANN Contractual Compliance's current scope. However, closing these gaps could result in impact on this phase and accordingly on Enforcement and Compliance.

The gaps identified here include:

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

---

[94] "Advisory: Compliance With DNS Abuse Obligations in the Registrar Accreditation Agreement and the Registry Agreement," *ICANN,* 5 February 2024, 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.

[95] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

[96] "DNS Abuse Mitigation Program," *ICANN org*, 3 October 2024, https://www.icann.org/dnsabuse.

  - **Description:** Currently, if a registrar repeatedly violates terms, ICANN Compliance goes through an escalated breach notice process. In case of recurring non-compliance from a party, ICANN escalates notices which, if not addressed, move immediately to a breach notice. ICANN can also suspend a registrar's ability to register new domains. The Small Team noted that beyond issuing breach notices (and eventually terminating if uncured), there are no intermediate penalties aside from termination.
  - **Research on Gap:** ICANN Compliance issues a formal Notice of Breach only after exhausting the information resolution stage of its process.[97] ICANN enforces all obligations through a clearly established process that ensures consistent and equal treatment for everyone. This process is publicly explained and consists of two stages: an informal resolution stage and a formal resolution stage. Most complaints are resolved confidentially during the informal stage, where Contracted Parties (CPs) demonstrate compliance or remediate a noncompliance before reaching the formal Notice of Breach stage, which can lead to termination or suspension of their agreements. Three Notices of Breach within 12 months allow ICANN to suspend or terminate a registrar's accreditation. Repeated Notices of Breach, under certain conditions, may also prevent renewal or assignment of an agreement. In some cases, remediation extends beyond the individual domain names originally reported. Remediation plans are required when it is determined that a CP lacks the necessary understanding, systems, and/or processes to consistently meet DNS Abuse mitigation requirements. These plans address the root cause of noncompliance and are not only requested when a CP is issued a formal Notice of Breach; enforcement and remediation most often occur at the informal resolution stage of the compliance process. This process also allows for expedited action, up to and including the issuance of a Notice of Breach, in cases of repeated noncompliance for previously remediated matters. Through its established process, as detailed in the last ICANN update on DNS Abuse mitigation requirements, ICANN Contractual Compliance launched 330 investigations during the first year of the DNS Abuse mitigation requirements' effectiveness. These efforts led directly to the mitigation of nearly 10,000 malicious domains, and hundreds of thousands more were addressed through the implementation by CPs of systems and processes resulting from compliance cases, among other outcomes. ICANN Compliance's processes are intentionally measured and gradual, with intermediate steps designed to allow for collaboration and remediation prior to termination. It is therefore unclear what additional intermediate penalties are envisioned.
  - **Potential Solution:** Introducing sanctions would require further policy work and would likely need to define "recurring non-compliance".

- **E3. Delayed ICANN Enforcement Actions:**

---

[97] Castillo, Leticia, "ICANN's Enforcement of DNS Abuse Mitigation Requirements: A Look at the First Six Months, " *ICANN org,* 8 November 2024, https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf.

- **Description:** This gap refers to the pace of Contractual Compliance enforcement-related activity. For instance, after the new DNS Abuse obligations took effect in April 2024, the first breach notices came in mid-July and September.[98] Some felt this was slow given likely non-compliance earlier.

- **Research on Gap**: As shared in multiple presentations, including the last webinar on DNS Abuse Mitigation requirements, ICANN initiated 330 investigations under these new obligations during their first year of effectiveness. These investigations led directly to the mitigation of nearly 10,000 malicious domains, and hundreds of thousands more were addressed through the implementation by CPs of systems and processes resulting from compliance cases, among other outcomes. It is important to note that Notices of Breach represent only a small portion of enforcement activities and are not the sole indicator of enforcement. Most mitigation and remediation occur during the informal resolution stage of the compliance process, without the need for a formal Notice of Breach. Details of these informal actions are not published individually, but they are included in aggregate in monthly and other ad hoc reports.[99] ICANN Contractual Compliance began enforcing the DNS Abuse Amendments immediately upon their effective date, with no delay.

- **Potential Solution**: ICANN Contractual Compliance began enforcing the DNS Abuse Amendments immediately upon their effective date, with no delay, and has been reporting on its progress regularly. According to the ICANN Org reply to the Small Team, ICANN Compliance has the tools, processes, and commitment needed to enforce the current requirements in the RAA and RA, and is prepared to evolve alongside the needs of the community. While enforcement began on 5 April 2024 without delay, ICANN is also developing new tools and strategies. These include proactive enforcement initiatives that will be fully integrated into ICANN's daily operations, with all relevant data captured for public reporting, as well as expanded educational and communication resources for reporting parties.[100] These enhancements are not addressing a gap or delay, but rather building on the strong foundation already established.

### Community Collaboration (Cross-Cutting)

DNS Abuse mitigation often requires cooperation beyond just the registrar, registry, and reporter. Some abuse types or preventive efforts call for the broader ICANN community, law enforcement, and others to work together.

---

[98] Castillo, Leticia, "ICANN's Enforcement of DNS Abuse Mitigation Requirements: A Look at the First Six Months, " *ICANN org,* 8 November 2024, https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf.

[99] "Contractual Compliance Twelve-Month Trends on DNS Abuse Reporting," *ICANN org* https://compliance-reports.icann.org/dnsabuse/dashboard/trends-list.html.

[100] Castillo, Leticia, "Responses to the GNSO Council Small Team on DNS Abuse: ICANN Contractual Compliance," *ICANN org,* 26 June 2025. https://icann-community.atlassian.net/wiki/spaces/gnsocouncilmeetings/pages/178389129/DNS+Abuse+Small+Team+2024-2025

The gaps identified here include:

- **CC1. Lack of Coordination during Domain Generation Algorithm (DGA) Botnet Attacks:**
    - **Description:** DGAs are often used by criminals to prevent their online activity being detected. DGAs are computer programs that automatically generate domain names, usually using a long random collection of numbers and letters. This is done at scale and pace (and across multiple TLDs or registries in varying jurisdictions and locations) to allow the attackers to move between different domain names to continue their activities, for example to distribute malware. The intention is to evade security countermeasures that are designed to prevent attackers from reaching victims, such as blocking the domain on a network.[101] Currently, law enforcement must contact each implicated registry individually when trying to mitigate malware or botnets that use DGAs at scale, which can result in fragmented, delayed, and inconsistent responses. According to the Netbeacon Whitepaper, these are low frequency but high impact events and streamlining the response could make it easier and faster for law enforcement to deal with large-scale criminal abuse campaigns. There is no central clearinghouse or coordination hub to quickly disseminate these domain lists to all relevant operators.[102]
    - **Research on Gap:** As noted in the Public Safety Working Group (PSWG) and gTLD Registries' publication, in respect of one particular botnet (Avalanche): The operation included close cooperation from over 40 top-level domain registries globally (both gTLDs and ccTLDs). In all, approximately 800,000 domain names were seized, blocked and/or sinkholed each year of the operation's existence (2016-2019). And yet, Avalanche's use of DGAs persists and has since required law enforcement to go before the courts on an annual basis to refresh authority for seizure of the list of domains expected to be generated by the DGA that year. In turn, law enforcement must then again provide the collaborating registry operators with those seizure orders requiring their action on an annual basis to prevent the dangerous domains from being made available to the public.**[103] A voluntary approach taken in addressing this gap is the** "Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets". This framework is intended to explain how domain names can support malware and botnets through these DGAs, and the unique mitigation practices that are essential to addressing the resulting DNS Abuse. This framework has been jointly drafted by the Governmental Advisory Committee Public Safety Working Group (PSWG) and the Registries Stakeholder Group (RySG). The framework is

---

[101] "Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets," *RySG*, https://www.rysg.info/wp-content/uploads/assets/Framework-on-Domain-Generating-Algorithms-DGAs-Associated-with-Malware-and-Botnets.pdf.

[102] "Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets," *RySG*, https://www.rysg.info/wp-content/uploads/assets/Framework-on-Domain-Generating-Algorithms-DGAs-Associated-with-Malware-and-Botnets.pdf.

[103] "Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets," *RySG*, https://www.rysg.info/wp-content/uploads/assets/Framework-on-Domain-Generating-Algorithms-DGAs-Associated-with-Malware-and-Botnets.pdf.

voluntary and non-binding and does not reflect any consensus policy affecting gTLD registries.[104]

  - **Potential Solution:** This was mentioned as a high-priority topic by the DNS Abuse Small Team for a potential PDP. The NetBeacon White Paper proposes a PDP on “Establishing a Centralized ICANN Coordination Role for DGA-Related Malware and Botnet Mitigation.” It proposes that ICANN serve as a centralized clearinghouse for DGA abuse reports. By streamlining the process of submitting evidence and coordinating action, ICANN can act as a trusted hub, reducing inefficiencies and ensuring that registries are aligned and responsive to urgent abuse cases. This model aims to speed up mitigation efforts but also bring greater consistency to DGA-related takedowns. ICANN would serve as a “hub” for verified law enforcement court orders.[105] Proposed policy elements include: (i) establish ICANN as a trusted escalation and coordination point for DGA-related abuse, receiving reports from law enforcement (or other trusted third party[106]), (ii) define a standardized intake and validation process within ICANN for DGA evidence submissions, (iii) enable ICANN to issue SRW (Security Response Waivers)[107] or pre-authorized notices to implicated registries to allow prompt action in accordance with contractual obligations, (iv) create a notification and coordination protocol for impacted registries to respond simultaneously based on centralized guidance, and (v) provide contractual clarity to ensure registries and registrars can rely on ICANN's role in good faith without fear of violating contractual requirements. NetBeacon noted in its White Paper: “It is not strictly necessary that the below go through a PDP process. ICANN could voluntarily adopt the role we propose. A PDP would clarify, however, that the Community supports ICANN performing this function.” While potentially appropriate for policy development, this item does not necessarily require further policy work and can be implemented outside the contractual requirements.

- **CC2. No Mechanism to Update DNS Abuse Definitions (Periodic Review):**
  - **Description:** ICANN's definition of DNS Abuse is precise, focused primarily on specific categories of malicious activities that deceive and misdirect users, namely: “malware, botnets, phishing, pharming, and spam (when spam is used as a delivery mechanism for any of the other four types of DNS Abuse).” These

---

[104] “Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets,” *RySG*, https://www.rysg.info/wp-content/uploads/assets/Framework-on-Domain-Generating-Algorithms-DGAs-Associated-with-Malware-and-Botnets.pdf.

[105] White Paper: Proposal for PDPs on DNS Abuse,” *NetBeacon Institute*, May 2025, p. 19, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

[106] For example, with Conficker, it was the Conficker Working Group, see: Joffe, Rodney, “Conficker Working Group – Archive of Materials,” *Senki*, January 2011, https://www.senki.org/operators-security-toolkit/security-organizations/conficker-working-group-archive-of-materials/.

[107] Using the SRW service, registrars can request a contractual waiver for actions it might take, or has taken, to mitigate or eliminate an incident. “Security Response Waiver Requests for Registrars,” *ICANN org,* https://www.icann.org/en/contracted-parties/accredited-registrars/resources/security-response-waiver-requests.

activities can compromise the security and stability of the DNS. New abuse types or edge cases might not clearly fall under the definition, such as "impostor" domains that mimic famous and well-known brands and actions associated with them (e.g., "login", "security", etc.).[108]

- **Research on Gap:** ICANN and the community focused on the definition that fits into the ICANN Bylaws and DNS Abuse types that impact the security and stability of the DNS. Furthermore, it focused on the aspects that can be best addressed by contracted parties. However, the SSAC's SAC115 (2021) recommended acknowledging that any fixed list of DNS abuse definitions will need updates as it can be limiting.[109]

- **Potential Solution:** This gap was named as a high-priority topic by some members of the DNS Abuse Small Team. Definitional discussions can be particularly challenging and it may be helpful to have a structure or framework under which these conversations can take place. For instance, potential considerations could include: (i) agreeing on the attributes that make a particular form of DNS Abuse appropriate to consider within ICANN's remit, and then (ii) measure emerging vectors against those attributes. The SSR2 Review's recommendation 10.2 suggested establishing a cross-community working group (CCWG) to periodically review and potentially update DNS Abuse-related definitions.[110] It is important to note that the contract amendments resulted from the November 2022 proposal the CPH sent to ICANN org to collaborate and enhance the existing contracts by creating clear obligations to stop or otherwise disrupt DNS Abuse. This proposal came with certain guideposts, including to not include matters pertaining to website content. It is equally important to note that while the new obligations are specific to DNS Abuse as defined in the amendments, they do not negate the existing obligations in Section 3.18 of the RAA. Section 3.18.1 of the RAA requires that registrars take reasonable and prompt steps to investigate and respond appropriately to any (emphasis added) report of abuse. This obligation remains in effect and will continue to be enforced. It is clear that the items listed in the proposed definition of DNS Abuse within the amendments are within ICANN's remit. It is in line with the ICANN Bylaws (Sections 1.1 and 1.2.) as well as ICANN's Strategic Plan, which states that a "coordinated approach is necessary to effectively identify and mitigate DNS security threats and combat DNS abuse." However, many other examples of abuse discussed in some sectors of the community and the Public Comments, while malicious, are deemed outside of ICANN's remit as they pertain to content, such as certain forms of fraud, copyright or trademark infringement, and scams perpetrated through websites. These harms often require legal expertise and due process to the registrant. Intellectual property disputes are

---

[108] Cole, Mason, "Attacking DNS Abuse: The Next Amendments Needed," *CircleID,* 4 November 2024, https://circleid.com/posts/attacking-dns-abuse-the-next-amendments-needed.

[109] "SAC 115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS," 19 March 2021, https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-115-en.pdf.

[110] "Second Security, Stability, and Resiliency (SSR2) Review Team Final Report," *ICANN org*, 25 January 2021, https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf.

complex, involving considerations such as fair use, free speech, and laws from multiple jurisdictions, and CPs are not the proper venue to adjudicate these disputes. Other frameworks exist to address some forms of intellectual property infringement.[111]

- ○ **Relation to other gaps in the DNS Abuse Small Team Matrix: C5. Imposter Domain Names (Exact Matches to Trusted Names):** Domains that exactly match a known brand or person (especially in new gTLDs or different TLDs) which are then used for abuse. Currently, there is no requirement that registries/registrars prevent or mitigate domains that are exact matches to famous names or sensitive keywords as these are outside the current ICANN definition of DNS Abuse.[112] During ICANN81 the CPH and CSG held a session[113] discussing this topic and how the DNS Abuse definition established by the ICANN contract amendments is not sufficient to address this type of DNS Abuse.[114]

These "Community Collaboration" gaps likely do not require consensus policies in the sense of binding contracted party obligations immediately. They are more about facilitating cooperation, establishing community structures, and ensuring ICANN evolves alongside an evolving DNS Abuse landscape. The Council might decide to address them in parallel or as non-binding best practices.

### Data & Transparency (Cross-Cutting)

Similar to the category above, this is not a normal domain lifecycle phase as introduced by the DNS Abuse Small team in 2022. But DNS Abuse mitigation often requires data and research in order for registrars/registries to better understand what drives DNS Abuse and for the ICANN community to develop policies.

The gaps identified here include:

- **P4. Lack of Data on "Bulk Registrations":**
  - o **Description:** The Small Team in 2022 noted that the community lacks clarity on which "bulk registrations" are malicious versus legitimate. Furthermore, it noted a lack of definition for "bulk registration," especially as it relates to some sort of contractual enforcement. Many businesses register portfolios of similar names or when planning for a launch of a new campaign. However, "bulk registration" can also be a known tactic of bad actors.

---

[111] "Public Comment Summary Report: Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations," *ICANN org,* 31 August 2023, https://itp.cdn.icann.org/en/files/registry-agreement/public-comment-summary-report-amendments-base-gtld-ra-raa-modify-dns-abuse-contract-obligations-31-08-2023-en.pdf.

[112] "DNS Abuse Mitigation Program," *ICANN org*, 3 October 2024, https://www.icann.org/dnsabuse.

[113] "Joint Session: CPH & CSG Work Session – ICANN81," 10 November 2024, https://icann-community.atlassian.net/wiki/spaces/gnsocouncilmeetings/pages/111123187/Joint+Session+CPH+CSG+Work+Session+-+ICANN81.

[114] Cole, Mason, "Attacking DNS Abuse: The Next Amendments Needed," *CircleID,* 4 November 2024, https://circleid.com/posts/attacking-dns-abuse-the-next-amendments-needed.

  - **Research on Gap:** There seems to be limited empirical data on the scale of "bulk-registration" abuse. Without data, it's hard to craft proportional solutions. This was flagged in the 2022 Small Team Report, which called for further exploration of "bulk registrations" and their role in DNS Abuse.[115] Furthermore, the 2022 Small Team noted 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.[116] However, the recognition of patterns in the case of abusive "bulk registration" (e.g., over 100) could help reduce malicious registration, or at least reduce incentives.
  - **Potential Solution:** In 2022, the DNS Abuse Small Team recommended working with registrars, ICANN org, and DNS Abuse Research Institute to study "bulk registrations" and develop possible mitigations.[117] As such, 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.

- **DT2. Lack of Empirical Research on Abuse Factors:**
  - **Description:** Aside from the INFERMAL study, there have been relatively few studies connecting specific policies or practices to levels of DNS abuse. While progress is being made, this Preliminary Issue Report and the 2025 DNS Abuse Small Team acknowledges not everything is well-quantified.[118]
  - **Research on Gap:** According to the INFERMAL study, no existing study has systematically analyzed the factors driving DNS abuse, leaving a critical gap in understanding how different variables influence malicious registrations.[119]
  - **Potential Solution:** The INFERMAL study, commissioned by ICANN, represents a study aiming to address this gap. A PDP working group focusing on DNS Abuse might identify data it needs and request a study, gather input, or document where knowledge is lacking so that future work can address it.

---

[115] "DNS Abuse Small Team Report to GNSO Council," *ICANN GNSO*, 7 October 2022, p. 4, https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf.

[116] "DNS Abuse Small Team Report to GNSO Council," *ICANN GNSO*, 7 October 2022, p. 12, https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf.

[117] "DNS Abuse Small Team Report to GNSO Council," *ICANN GNSO*, 7 October 2022, p. 4, https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf.

[118] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

[119] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, p. 1, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

## 3.1.2 Considerations

**Discussion of Issues:**
It is important to note that none of the practices or mechanisms identified in this report are inherently abusive. These tools and operational models are widely used and valued by legitimate registrants, including service providers operating at scale. This report is to analyse and discuss issues in mitigation efforts that, if addressed, can help reduce DNS Abuse through prevention or remediation. Thus, the aim is to make it significantly more difficult for malicious actors to exploit these mechanisms to carry out large-scale or coordinated DNS Abuse. The approach taken reflects the understanding that threat actors are highly adaptive; therefore, addressing existing mitigation gaps requires a balance between protective measures and operational flexibility.

**Source documents referenced in the Preliminary Issue Report:**
While this report draws on multiple sources (see Section 3.1.1), it references the INFERMAL study and the Netbeacon PDP White Paper more frequently because the INFERMAL study was commissioned by ICANN org and provides recent empirical findings on malicious registrations and domain registration practices; the NetBeacon paper reflects community-informed proposals aligned to the same problem space. Both were considered by the 2025 Small Team alongside other materials, and are cited here as two among several inputs, not as exclusive authorities.

**DNS Abuse Small Team Gap Matrix:**
The list of gaps and accompanying discussion of them in this Issue Report are based on the work initiated by the DNS Abuse Small Team, particularly the preliminary gap matrix developed in the course of its 2025 mandate. That matrix was constructed through an initial review of source materials as referenced in the group's assignment form. In preparing this Issue Report, the Staff Manager has conducted additional research and review to validate, refine, and supplement the original entries. Where appropriate, gaps that initially appeared as distinct have been consolidated into one gap discussion, particularly where the substance or intent of those gaps significantly overlapped. These consolidations are indicated in the respective gap and text below. To maintain traceability and alignment with the original matrix, this report references the original Gap IDs (e.g., P1) used in the Small Team matrix.[120] This allows community members and stakeholders to map the content of the report directly to earlier work.

**Nature of gap solutions proposed:**
The **nature of potential solutions** as captured in the PDP Manual notes that a PDP may recommend a wide range of outcomes to the GNSO Council, including Consensus policies, Best Practices, Implementation Guidelines, Technical Specifications and Recommendations on future policy development activities. In some instances, it may be equally appropriate to pursue certain solutions outside of the PDP.[121]

**Consideration for a PDP:**

---

[120] "DNS Abuse Small Team List of Gaps," *ICANN GNSO,* 25 July 2025, https://docs.google.com/spreadsheets/d/18PdZnH3OQ65NT9g0lGE6Y2toFaCrtxyf/edit?gid=1836517289#gid=1836517289.

[121] "GNSO Policy Development Process Manual," *ICANN org,* Version 2.6, p. 57, https://gnso.icann.org/sites/default/files/filefield_38869/annex-2-pdp-manual-16may13-en.pdf.

Staff recommends that the GNSO Council proceed to initiate a PDP to address the DNS Abuse mitigation gaps outlined in this report.

**Single PDP vs. Subsequent PDPs:** One key decision is whether to handle this as a single comprehensive PDP or as multiple narrower PDPs. Staff identifies pros and cons to each:

- Single PDP: This would allow holistic consideration of all related issues under one working group and one Charter. It could attempt to ensure that interdependencies (like how reporting standards feed into enforcement) are managed cohesively. However, a single PDP might become unwieldy given the scope, potentially leading to a very long duration and difficulty reaching consensus on every sub-topic. There's a risk of overload that could stall progress. Note that in the context of a single PDP, the concept of phases could be introduced, which would allow for the delivery of intermittent outcomes and mitigate the lengthiness to some degree.

- Multiple PDPs: Breaking the work into a set of targeted and concurrent PDPs (for example: PDP A on two priority issues, PDP B on subsequent priority gaps, etc.) could make each effort more focused and faster on its topic. The downside is managing multiple simultaneous PDP WGs, which can strain community volunteer and staff resources. Coordination would also be needed to ensure no gaps or overlaps between them. Given community feedback to date, there appears to be interest in a narrowly scoped approach. To that end, staff recommends initiating a single PDP, focusing on the three priority issues, with the option to initiate additional PDPs subsequently (phased approach). This approach balances urgency with manageability.

- In addition, the Council could decide to employ sub-working groups or work tracks. For instance, a single PDP WG could have distinct teams addressing each phase or set of topics and then coordinate final recommendations. This was done in past PDPs (e.g., the New gTLD Subsequent Procedures PDP had multiple work tracks under one umbrella). Even with strong project management principles applied, this approach is extremely resource intensive and splits the attention of the community and staff alike.

- What Should Be Consensus Policy vs. Other Outcomes: It's important to note that not all identified gaps may result in new Consensus Policy (binding contract changes). The PDP(s) can also recommend best practices, guidelines, or other community actions where appropriate. For example, issues like DGA coordination (CC1) might be addressed by community initiatives rather than contractual terms.

## 3.1.3 Relevant Documentation and Reports

- DNS Abuse Small Team Report 2025
- DNS Abuse Small Team Report 2022
- ICANN's Enforcement of DNS Abuse Mitigation Requirements - A look at the first 6 months
- NetBeacon White Paper
- INFERMAL Study

  - ▪ NetBeacon Analysis: How have the gTLD contractual amendments impacted DNS Abuse?

## 3.2 Potential issues to be considered in a PDP on DNS Abuse

### 3.2.1 Issues to be considered

The below table shows an overview of the issues, where proposed mechanisms to address them would be through Consensus Policy and a potential PDP. While this report covered all identified gaps by the DNS Abuse Small Team, the two priority topics for policy development highlighted by the Preliminary Issue Report are:

(1) Unrestricted API Access,
(2) Associated Domain Checks

These areas represent issues in current DNS Abuse mitigation efforts and are considered suitable for early policy work. Note, the third priority topic identified by the DNS Abuse Small Team, Coordinated Mitigation of DGA-Based Botnet Domains, is suggested in this Preliminary Issue Report to be pursued more directly and expeditiously outside of policy development.

#### Consideration of Remaining Gaps for Subsequent PDP Phases

While the first PDP could concentrate on the three priority gaps, the **remaining gaps** identified in Recommendation 4[122] of the DNS Abuse Small Team also garnered significant support across SGs and ACs. These topics could be considered in later policy development phases, subject to available resources, community bandwidth, and Council priorities.

- Unactionable Complaints (A1)
- Limited Use of Abuse Feeds/Threat Data for Prevention (P11)
- No Mechanism to Update DNS Abuse Definitions (Periodic Review) (CC2)
- Lack of Standard Dispute/Recourse Mechanism for Registrants: (C3)

### 3.2.2 Possible Impact on Human Rights

Consideration of this issue may impact human rights (e.g., enhance freedom of expression). For further information about ICANN and the ICANN Community's work on human rights, please see https://community.icann.org/x/RAPCCw. It is important to note that a Human Rights Impact Assessment (HRIA) will be included in the PDP by default.

### 3.2.3 Objectives of a possible PDP

---

[122] "DNS Abuse Small Team Report to GNSO Council," *ICANN GNSO*, 25 July 2025, https://gnso.icann.org/sites/default/files/policy/2025/draft/dns-abuse-small-team-report-04aug25-en.pdf

A PDP on DNS Abuse Mitigation aimed at the two priority gaps would pursue closing the DNS Abuse mitigation gaps related to:

**(i) Unrestricted API access** to introduce friction to slow abuse at scale, such as requiring new registrants to pass a basic trust threshold at the registrar before gaining access to programmatic registration tools;
**(ii) Associated-domain checks** to introduce a requirement for registrars to review other associated domains, upon receiving a valid abuse report, for example by investigating domains in the same user account, or linked to the same registrant.

## 3.2.4 Specific questions to be considered in a possible PDP

**1. Unrestricted API access**

- What minimum safeguards must registrars be required to implement before granting access to high-speed or high-volume domain registration tools (e.g., APIs) to new customer accounts?
- How can "trustworthiness" be defined or operationalized in a way that is based on customer behavior rather than identity?
- What types of friction (e.g., waiting periods, registration history, and DNS Abuse checks) are both effective and reasonable for registrars to implement?
- Must an existing customer account lose access to high-speed or high-volume domain registration tools (e.g., APIs) for registration if the registrar confirms that the customer has maliciously registered a domain for DNS Abuse in its account?

**2. Associated-Domain Checks (Domains Linked to Confirmed Abuse)**

- Must registrars be required to investigate other domains associated with a customer account, registrant email address, or other identifying information when a domain under that account is reported and confirmed to be engaged in malicious DNS Abuse?
- What criteria should be used to define "association" between domains (e.g., customer account ID, registrant email, payment method)?
- How should the obligation be scoped for wholesale registrars where customer account information may not be available to the registrar? Would identifying associated domains by registrant email or another field be sufficient in these cases?

## 3.2.5 Other factors relevant to the decision whether to initiate a PDP

None identified.

# 4 Staff Recommendation

## 4.1 General Counsel recommendation

### 4.1.1 Scope considerations

Based on the documentation above, the launch of a dedicated PDP to consider the issues identified in this Preliminary Issue Report has been confirmed by ICANN's General Counsel to be properly within the scope of the GNSO as well as the ICANN Policy Development Process. In reaching that determination, the General Counsel's office and ICANN Policy Support staff have considered the factors in the following sections:

### 4.1.2 Whether the issue is within the scope of ICANN's mission statement

ICANN's mission is to ensure the stable and secure operation of the Internet's unique identifier systems, and this includes facilitat[ing] the coordination of the operation and evolution of the DNS root name server system" and "coordinat[ing] the development and implementation of policies for which uniform or coordinated resolution is reasonably necessary to facilitate the openness, interoperability, resilience, security and/or stability of the DNS." Annex G-1 and Annex G-2 of the ICANN Bylaws (which enumerate the topics appropriate for GNSO policies) has been consulted to ensure that each of the three gaps falls within the realm of "names policy" that can be enforced upon contracted parties. For example, policies governing registrar accreditation practices, registrant validation, and abuse reporting/response requirements are well within GNSO scope.

### 4.1.3 Whether the issue is broadly applicable to multiple situations or organizations

The issues are important to multiple stakeholder groups and end-users; mitigating DNS Abuse is broadly beneficial to the security and stability of the DNS, and thus a proper subject for GNSO policy considering the criteria of global applicability and lasting value.

### 4.1.4 Whether the issue is likely to have lasting value of applicability

The three priority issues identified are not limited to any single registry, registrar, business model, geography, or user community. Given this breadth of impact, a PDP on these topics would have system-wide relevance and lasting value for a wide range of organizations and use-cases.

### 4.1.5 Whether the issue implicates or affects ICANN Consensus Policy

The review of DNS Abuse mitigation gaps does not appear to impact existing ICANN Consensus Policy, but this question will be further considered during policy development. Furthermore, a PDP on DNS Abuse may create new ICANN Consensus Policy, as the issues identified in this report fall outside current policy obligations.

## 4.2 Policy Support Staff recommendations

ICANN Staff confirms that the issue of DNS Abuse is within the scope of the GNSO’s Policy Development Process as outlined in the ICANN Bylaws. The issue is one in which “uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet or DNS.”

# 5 Next Steps

In accordance with the GNSO PDP rules, Staff will publish the Preliminary Issue Report for Public Comment to allow for community input on additional information, or the correction or updating of any information provided so far. Following review of the public comments, Staff will update the Preliminary Issue Report and submit a summary of the comments received together with the Final Issue Report to be forwarded to the GNSO Council for its consideration. The GNSO Council will then vote on the Staff recommendations, as to whether or not to initiate a PDP on DNS Abuse and, if so, whether or not to adopt or amend (e.g., by forming a Drafting Team to review) the Charter appended to the Final Issue Report – a draft version of which can be found in Annex A of this Preliminary Issue Report. It should be noted that the GNSO Council is not bound by Staff recommendations, and, if it chooses to do so, may pursue alternative actions to those proposed in this Preliminary or indeed the Final Issue Report.

ICANN | GNSO

Generic Names Supporting Organization

# 6 Annex A Preliminary Charter

| | | |
|---|---|---|
| **WG Name:** | **TBD** | |
| **Section I: Working Group Identification** | | |
| **Chartering Organization(s):** | Generic Names Supporting Organization (GNSO) Council | |
| **Charter Approval Date:** | <Enter Approval Date> | |
| **Name of WG Leadership:** | <Enter Elected WG Leadership> | |
| **Name(s) of Appointed Liaison(s):** | <Enter Liaison> | |
| **WG Workspace URL:** | <Enter Active Project URL from GNSO Site> | |
| **WG Mailing List:** | <Enter Mailman archive link> | |
| **GNSO Council Resolution:** | **Title:** | Initiation of the Policy Development Process on DNS Abuse Mitigation |
| | **Ref # & Link:** | <Enter Resolution link> |

| | |
|---|---|
| **Important Document Links:** | **Procedural Documents:**<br>● Annex A-1: GNSO Expedited Policy Development Process<br>● Expedited GNSO Policy Development Process Manual<br>● GNSO Working Group Guidelines<br>**Non Exhaustive List of Substantive Documents:**<br>● DNS Abuse Small Team Report 2025<br>● DNS Abuse Small Team Report 2022<br>● ICANN's Enforcement of DNS Abuse Mitigation<br>● Requirements - A look at the first 6 months<br>● NetBeacon White Paper<br>● INFERMAL Study<br>● NetBeacon Analysis: How have the gTLD contractual amendments impacted DNS Abuse? |
| **Section II: Mission, Purpose, and Deliverables** | |
| **Mission & Scope:** | |

**Background**

In early 2025, the GNSO Council reconvened its DNS Abuse Small Team with a revised assignment form to re-examine DNS Abuse mitigation considering new developments, research, and data. The previous Small Team (2021–2022) had identified obligation gaps and issued recommendations, some of which were addressed through contractual amendments to the RA and RAA. Those amendments (effective since April 2024) strengthened abuse mitigation obligations, and ICANN Contractual Compliance has since reported initial data on their impact. With these measures in place and new research available, the Small Team was tasked to consider new insights and discuss potential next steps on DNS Abuse. Drawing from community input, compliance data, and external studies, the team was tasked with identifying remaining gaps and assessing whether further policy development is warranted.

The DNS Abuse Small Team conducted a review of data and source documents noted in their assignment form, focusing on identifying potential gaps in DNS Abuse mitigation efforts across multiple phases of the DNS Abuse lifecycle (as proposed by the Small Team in 2022). The Small Team compiled a matrix of DNS Abuse "gaps," noting areas where abuse prevention, reporting, response, or obligations could be strengthened after further investigating the identified gaps. Findings were categorized by lifecycle stage and further grouped by thematic clusters to support potential prioritization and future policy scoping.

Based on data analysis, community consultation, and input from stakeholder groups (SGs), the Small Team recommended the following three gaps be prioritized for policy work in the Issue Report:

- **Unrestricted Application Programming Interface (API) access for high-volume registrations:** Many registrars offer Application Programming Interfaces (APIs) or batch-registration portals that allow resellers or high-volume customers to register large numbers of domain names rapidly. According to studies such as the INFERMAL study, insufficient gating or friction for new users to access these batch registration tools can lead to the proliferation of DNS Abuse.
- **Associated Domain Checks:** Malicious domains are often part of broader campaigns involving dozens or hundreds of related domains. Currently, when a registrar finds that one domain is malicious, there is no contractual requirement that the registrar must investigate whether the same registrant or account has other active domains that are also being used for similar abuse.
- **Limited coordination on Domain Generation Algorithm (DGA)-based abuse:** Botnets using DGAs generate many domain names (sometimes hundreds a day) for their command-and-control. Law enforcement must contact each implicated registry individually when trying to mitigate malware or botnets that use DGAs at scale, which can result in fragmented, delayed, and inconsistent responses. These are low frequency but high impact events. There is no central clearinghouse or coordination hub to quickly disseminate these domain lists to all relevant operators.

The Small Team has chosen the above topics from the matrix, based on topics that seem appropriate for policy development (taking into consideration review of source data, input/priorities received by Small Team members, and Community consultation during ICANN83), meaning that the topics are:

- important/impactful to solve,
- likely to gain broad consensus, and

- ideally, areas in which the potential solution(s) seem achievable, having in mind current workload and resources.

The Issue Report, which was requested by the GNSO Council on 14 August 2025 after it reviewed and adopted the Small Team recommendations, concluded that all of the three identified priority issues are appropriate for policy development. However, the report suggests that only two of the three identified DNS Abuse Issues should be prioritized for policy development, while one could potentially be addressed more directly and expeditiously outside of the policy development process. This prioritization reflects where policy intervention could likely reduce DNS Abuse at scale, is broadly applicable across the gTLD space, and aligns with the community input and lifecycle-and-cluster analysis used in the updated Small Team gap matrix.

Informed by the DNS Abuse Small Team`s recommendations and the Community`s support for a narrowly scoped Policy Development Process (PDP), the Council initiated a PDP limited, at this stage, to the two issues named below:

- **Unrestricted Application Programming Interface (API) access for high volume registrations**
- **Associated Domain Checks**

**Scope & Charter Questions**

## Scope:

This PDP is limited to examining two DNS Abuse mitigation gaps:

**Unrestricted Application Programming Interface (API) access for high-volume registration**

- **Description:** Malicious actors use ungated access to APIs to register large volumes of domains in a matter of minutes, enabling large-scale phishing, smishing, and botnet operations. Many registrars require some sort of friction before a new customer account has access to an API where it can create thousands of names at once (e.g., restrict access to an API until the customer has more than three transactions not flagged as fraudulent or engaged in DNS Abuse). Some registrars allow brand-new accounts to access these bulk registration capabilities without any meaningful checks. According to studies such as INFERMAL, insufficient gating or friction for new users to access these tools can lead to the proliferation of DNS Abuse. The availability of APIs for domain registration and account management seems to be strongly associated with a higher volume of malicious registrations according to INFERMAL.[123] Specifically, registrars that provided unrestricted API-based registrations saw a significantly elevated risk of phishing domains: "API access was linked to a 401 percent increase in malicious domain registrations" relative to a baseline in the study. In other words, the study found that the presence of easy automation (via APIs) can multiply the likelihood of abuse by roughly four times,

---

[123] Nosyk, Yevheniya, et al. "INFERMAL: Inferential Analysis of Maliciously Registered Domains," *ICANN org*, 8 November 2024, https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf.

all else being equal. By contrast, the study noted that registrars employing restrictions on API usage for unverified users or requiring some form of vetting saw lower abuse rates.

**Associated Domain Checks**

- **Description:** Malicious domains are often part of broader campaigns involving dozens or hundreds of related domains. When a registrar finds that one domain is malicious, there is no contractual requirement that the registrar must investigate whether the same registrant or account has other active domains that are also being used for similar abuse. The NetBeacon White Paper strongly advocates for an "Associated Domain Check" requirement via a PDP.[124] Without this requirement, an attacker might only lose one domain at a time, continuing to use the rest until each is individually reported. If registrars proactively pivot on the information, it could curtail whole campaigns. Some registrars likely do this voluntarily, but others may not due to lack of resources or fear of overreaching. The RAA currently only requires registrars to evaluate individual domain names when they obtain evidence that the domain name is being used for DNS Abuse.[125] This current "one-at-a-time" approach limits the mitigation of related domains operated by the same actor, even when those domains are part of an identifiable campaign.

## Charter Questions:

### 1. Unrestricted API access

This PDP would look to introduce safeguards to ensure that registrants, particularly new or untrusted accounts, cannot immediately access high-volume domain registration tools (e.g., APIs) until they have demonstrated basic trustworthiness. The goal is to slow the ability of malicious actors to rapidly register large volumes of domains used in phishing, malware, and other DNS Abuse campaigns and create preventative barriers to criminal campaigns that seek to register malicious domains in bulk.

- What minimum safeguards must registrars be required to implement before granting access to high-speed or high-volume domain registration tools (e.g., APIs) to new customer accounts?
- How can "trustworthiness" be defined or operationalized in a way that is based on customer behavior rather than identity?
- What types of friction (e.g., waiting periods, registration history, and DNS Abuse checks) are both effective and feasible for registrars to implement?
- Must an existing customer account lose access to high-speed or high-volume domain registration tools (e.g., APIs) for registration if the registrar confirms that the customer has maliciously registered a domain for DNS Abuse in its account?
- What thresholds must registrars introduce before granting access to high-speed or high-volume registration methods?
    - Such thresholds could include:
        (i) Requiring that a registrant has held one or more domains through the Add Grace Period without action for DNS Abuse.

---

[124] White Paper: Proposal for PDPs on DNS Abuse," Netbeacon Institute, May 2025, p. 14, https://netbeacon.org/wp-content/uploads/2025/05/2025-05-NetBeacon-PDP-Whitepaper-Final.pdf.

[125] "2013 Registrar Accreditation Agreement," ICANN org, 21 January 2024, https://itp.cdn.icann.org/en/files/accredited-registrars/registrar-accreditation-agreement-21jan24-en.htm

(ii) Implementing waiting periods for newly created accounts.
(iii) Denying access to high-speed and/or high-volume registration methods for existing customers, if the customer has had domains which the registrar has identified as being maliciously registered DNS Abuse.)

- What specific requirements must registrars implement and enforce for new and untrusted customers, and what are the reporting requirements?
- What aspects should be consensus policy requirements and what aspects can be subject to best practices, or potentially left to the discretion of the contracted party?

**Considerations:**

- Effectively all transactions at wholesale registrars are via API. As noted in the Associated Domains Check, this policy should explicitly identify whether registrars may or must differentiate between retail API access and API access where a signed reseller agreement is in place.
- Whether friction can be implemented based on customer activity rather than customer identity. Friction based on activity (e.g., how old is the account and have they had reports of abuse) may be more robust, reliable, and easier to implement than attempts at customer verification.

**2. Associated-Domain Checks**

This PDP would seek to create an obligation for registrars to investigate other domains associated with a customer account or registrant where at least one domain of that registrant is found to be engaged in DNS Abuse. By identifying and acting on malicious domain portfolios - often part of coordinated campaigns - this policy could significantly reduce abuse uptime and disrupt large campaigns used for phishing and other DNS Abuses. The Associated Domain Check would seek to solve a gap by requiring all registrars to “pivot” from a known abusive domain to others connected to the same customer account, registrant email address or other piece of information.

- Must registrars be required to investigate other domains associated with a customer account, registrant email address, or other identifying information when a domain under that account is reported and confirmed to be engaged in malicious DNS Abuse?
- What criteria should be used to define “association” between domains (e.g., customer account ID, registrant email, payment method)?
- How should the obligation be scoped for wholesale registrars where customer account information may not be available to the registrar? Would identifying associated domains by registrant email or another field be sufficient in these cases?
- Must "associated domain checks" address malicious portfolios that are spread across multiple registrars to evade detection?
- Defining "investigation": What constitutes a "reasonable investigation" by a registrar? What steps and depth of analysis are required?
- What specific requirements are necessary to implement this policy and what parts can be subject to best practices, or potentially left to the discretion of the contracted party?
- What reporting obligations will registrars have to ICANN? What metrics will be used to evaluate the policy's effectiveness?

- How will ICANN Compliance oversee and enforce the new obligations? What types of evidence and reports will registrars be required to submit to demonstrate their compliance?

**Considerations:** It's important to note that at wholesale registrars, effectively, all registrations are done via API. Accordingly, a requirement for a wholesale registrar to examine all domains in a wholesale account would be an untenable solution. Instead, where a domain is covered by a signed reseller agreement, one way this could be addressed would be that the obligation could be for the registrar to search for other domains linked to registrant email, rather than customer account, or other relevant indicators.

**Impact on Human Rights**

The WG is expected to consider the potential impact of any recommendations on human rights. Based on the information included in the request for an Issue Report and the Issue Report, the WG is expected to further consider whether there is a likely human rights impact, and if so, who are the groups expected to be impacted and the expected severity of the impact (high / medium / low). If an impact is anticipated, the WG is expected to address the following questions: 1) is the proposed action necessary to achieve the desired outcome, 2) is the proposed action proportionate, 3) is the proposed action legitimate.

**Deliverables:**

To develop, at a minimum, an Initial Report and a Final Report regarding the WG's recommendations on issues relating to DNS Abuse Mitigation, following the processes described in Annex A of the ICANN Bylaws and the GNSO PDP Manual.

If the WG concludes with any recommendations, the WG shall (or recommend the subsequent policy Implementation Review Team to) conduct a policy impact analysis and identify a set of metrics to measure the effectiveness of the policy change, including source(s) of baseline data for that purpose:

- Identification of policy goals
- Identification of metrics used to measure whether policy goals are achieved
- Identification of potential problems in attaining the data or developing the metrics
- Identification of potential impact of its recommendations on any currently existing requirements on registrars and registry operators
- A suggested timeframe in which the measures should be performed
- Define current state baselines of the policy and define initial benchmarks that define success or failure
- Metrics may include but not limited to (Refer to the Hints & Tips Page):
    - ICANN Compliance data
    - Industry metric sources
    - Community input via public comment
    - Surveys or studies

**Data and Metric Requirements:**

The WG should as soon as practicable:

1. Determine a set of questions which, when answered, provide the insight necessary to achieve the policy goals.
2. Determine whether certain data is required to help understand a specific issue or answer a charter question.
3. Determine a set of data and metrics which can be collected and analyzed to help answer the specific question.
4. Submit a Working Group Metrics Request Form (see GNSO Working Group Guidelines Section 4.5), if data gathering at the charter drafting phase or during the working phase is deemed necessary.

WG leaders shall review the Guidance document below to understand the need for performing due diligence before submitting a data gathering request to the GNSO Council.

## Section III: Project Management

### Work Product Requirement:

The WG leadership, in collaboration with the WG support staff and GNSO Council liaison, shall use a standard set of project management work products that help plan, guide, track, and report the progress of the WG from start to finish, and include the necessary data and information to assess the progress of the WG. These work products include but not limited to:

- Work Plan
- Summary Timeline
- Project Situation Report
- Project Plan
- Action Items

See the full suite of work products in the GNSO Project Work Product Catalog.

### Project Status & Condition Assessment:

The WG leadership, in collaboration with the WG support staff and the GNSO Council liaison, shall assess the Status and Condition of the project at least once a month. Such frequency is required in preparation for the GNSO Council monthly meeting, where At-Risk or In-Trouble projects are subject to review by GNSO Council leadership, and in some instances may be deliberated by the full GNSO Council.

The WG leadership, in collaboration with the WG support staff and the GNSO Council Liaison, shall use an escalation procedure, which defines specific conditions that trigger the execution of a repeatable mitigation plan. The objective of this exercise is to return the project to an acceptable state ultimately achieving its planned outcomes.

### Project Change Request:

The WG shall submit a Project Change Request (PCR) Form to the GNSO Council when its deliverable and baseline delivery date are revised. The PCR shall include a rationale for why these changes were made, their impacts on the overall timeframe of the PDP or any other interdependencies, and a proposed remediation plan.

The use of the PCR mostly occurs when primary deliverable dates are changed due to unforeseen or extreme circumstances. However, it can also be used to document changes in the deliverable requirements that may not have been identified in the chartering process.

When the PCR is required, it should be completed by the WG Chair and it will likely be presented to the GNSO Council for approval.

### Resources Tracking:

The purpose for resource tracking is to deliver its work according to the work plan and be responsible for managing these resources.

For projects where dedicated funds are provided outside of budgeted policy activities, the WG shall provide regular budget versus actual expense reporting updates using a GNSO approved tool to allow for a better tracking of the use of resources and budget.

## Section IV: Formation, Staffing, and Organization

### Working Group Model:

| |
|---|
| **Working Group Model:** Representative<br>**Rationale:** The "Representative" is chosen to enable the WG to conduct and conclude its work in an efficient/effective manner.<br>A limited number of ICANN community members have prerequisite knowledge, background, or expertise in the subject matter. As a result, a limited number of Members appointed by specified community groups, who must possess a level of expertise as detailed in the "Membership Criteria" section in this charter, should drive the deliberations of the WG and participate in the consensus designation process for final recommendations. |
| **Membership Structure:** |

**Role Descriptions:** All Members participating in the Working Group are expected to abide by the Statement of Participation, which is enforceable by the WG Chair and GNSO Council Leadership Team. See Section V. for details.

- **Members:** Members are expected to participate during the course of deliberations and in any WG consensus calls. Members are expected to represent the view of their appointing organization, and may be called on to provide the official position of their appointing organization. Members are required to have a level of expertise in the relevant issues and ICANN policies and procedures as that may be impacted.

- **Observers:** Anyone interested in this PDP may join as an observer. Observers are provided with read-only access to the mailing list and are not invited to attend meetings.

- **GNSO Council Liaison:** The GNSO Council shall appoint one (1) Liaison who is accountable to the GNSO. The GNSO Council Liaison must be a member of the Council, and the Council recommends that the Liaison should be a Council member and be able to serve during the life of this WG. See detailed description in the “GNSO Council Liaison” section below.

- **ICANN Org Liaison(s):** ICANN Org shall appoint at least one (1) Liaison, who is expected to provide timely input on issues that may require ICANN Org input such as implementation-related queries and issues that might benefit from their subject matter expertise. The ICANN Staff Liaison(s) is not expected to advocate for any position and will not participate in any PDP Team consensus calls.

- **ICANN Board Liaison:** While not required, the ICANN Board is encouraged to appoint a liaison to this PDP. The liaison should participate in accordance with the Guidelines for Board Members Serving as Liaisons to ICANN Community Groups.

**Membership Structure:**

Some groups may choose not to appoint any Members to the WG. The table below indicates the maximum number of Members that groups may appoint.

| Group | Member (up to) | Liaison |
|---|---|---|
| RySG | 2 | |
| RrSG | 2 | |
| IPC | 2 | |
| BC | 2 | |
| ISPCP | 2 | |

| | | |
|---|---|---|
| NCSG | 2 | |
| ccNSO | 2 | |
| ALAC | 2 | |
| GAC | 2 | |
| SSAC | 2 | |
| RSSAC | 2 | |
| GNSO Council | | 1 |
| ICANN Org GDS | | At least 1 |
| ICANN Board | | 1 |

The GNSO Secretariat is expected to circulate a “Call For Volunteers” in accordance with the group structure determined by the GNSO Council:

- Publication of announcement on relevant ICANN web sites including but not limited to the GNSO and other Supporting Organizations and Advisory Committee web pages; and
- Distribution of the announcement to GNSO Stakeholder Groups, Constituencies and other ICANN Supporting Organizations and Advisory Committees

**Membership Criteria:**

### A. Expected Skills for Working Group Members

WG members shall review the full text of the Working Group Member Skills Guide to understand the responsibilities and skills that they are expected to have in order to fully participate in the WG activities.

Collectively as a group, the WG Members MUST possess:

- Understanding of the Latin RZ-LGR, the new gTLD string similarity process, and Latin script diacritics.
- If possible, a practical understanding of what may be involved in a single registry operator running and ASCII and Latin script diacritic simultaneously.
- Familiarity with GNSO policy development processes; direct experience is strongly preferred;
- Commitment to participating in Working Group meetings on a regular and ongoing basis;
- Highly effective oral, written, and interpersonal communication skills (in simple, comprehensible English);
- Ability to create factual, relevant and easily understandable messages, and able to succinctly deliver them to the Working Group;
- Research skills with the ability to discern factual, factually relevant, and persuasive details and sources;
- Commitment to manage a diverse workload, while collaborating with a Working Group of individuals with different backgrounds and interests in driving objectives;
- Knowledge of Working Group discussions, actions taken at meetings, and deliverables;
- Understanding of the perspectives and interests of the members' own stakeholder group or constituency;
- Understanding of what consensus means and how consensus-building process works;
- Commitment to facilitate consensus by listening, explaining, mediating, proposing clear actions, and helping other members;
- Commitment to avoid blocking consensus by looking beyond the stakeholder group or constituency affiliation of other Working Group members and judging proposals/positions on their merits;
- Commitment to avoid re-litigating closed issues or deliberate obfuscation;
- Commitment to review the Consensus Playbook and attend potential training related to the Playbook, facilitate consensus building by employing the tools and techniques as detailed in the playbook;
- Maintain high personal levels of ethical conduct and integrity, including transparency of affiliation in the SOI, in treatment of others and respecting the professional reputation of all in the ICANN community.

### B. Joining of New Members After Project Launch

New Members will only join after the launch of the PDP if a current Member is no longer able to continue in its membership. New WG Members should be mindful that, once input/comment periods have been closed, discussions or decisions should not be resurrected unless there is group consensus that the issue should be revisited in light of new information that has been introduced. If the reopening is perceived as abusive or dilatory, a WG member may appeal to the WG leadership.

**C. Expert Contributors**
The WG has flexibility/discretion to invite participation of the expert contributors in specific fields as it deems necessary.

Expert contributors are not expected to participate in any consensus designation process, but provide perspective/expertise/knowledge to the PDP WG.

Based on the WG's determination, the Council may be able to use an independent evaluation process (e.g., GNSO Council Standing Selection Committee) to confirm whether those individuals have demonstrated the expertise/knowledge/perspective.

## Leadership Structure:

**One (1) Chair + One (1) Vice Chair**

The GNSO Council will appoint one (1) qualified, independent Chair (neutral, not counted as from the WG membership) for the WG.

The WG, once formed, may select one (1) Vice Chair to assist the Chair. The Vice Chair can be selected among the WG's Members. However, if a Member is selected as the Vice Chair, his/her appointing organization may appoint a new Member as a replacement.

Should at any point a Vice Chair need to step into the role of Chair, the same expectations with regards to fulfilling the role of Chair as outlined in this charter will apply.

## Leadership Criteria:

**Expectations for the WG Leadership (Chair + Vice Chair):**
The WG leadership is expected to carry out the role and responsibilities and meet the qualification as detailed in the Expectations for Working Group Leaders & Skills Checklist.

In short, the WG leadership is expected to:

- Lead with neutrality and impartiality;
- Encourage representational balance;
- Ensure WG documents represent the diversity of views;
- Balance working group openness with effectiveness;
- Make time commitment;
- Contribute ideas and knowledge to working group discussions;
- Oversee project management of the WG deliberations;
- Build consensus;
- Make consensus designation on working group recommendations;
- Enforce compliance with Statement of Participation;
- Enforce compliance with ICANN's Expected Standards of Behavior;
- Ensure compliance with Community Anti-Harassment Policy;
- Be versed in GNSO Operating Procedures; and
- Handle working group complaint process.

**Expectation for the WG Chair:**
As outlined in the GNSO Working Group Guidelines, the purpose of a Chair is to call meetings, preside over working group deliberations, manage the process so that all members have the opportunity to contribute, and report the results of the Working Group to the Chartering Organization. These tasks require a dedicated time commitment as each week calls have to be prepared, the agenda concretized, and relevant material reviewed. The Chair shall be neutral. While the Chair may be a member of any group which also has representation on the Working Group, the Chair shall not act in a manner which favors such group. The Chair shall not be a member of the Working Group for purposes of consensus calls.

In addition, it is expected – that interested candidates shall have considerable experience in chairing working groups, and direct experience with at least one GNSO Policy Development Process throughout its lifecycle. Familiarity with the functioning of a Working Group is important to understand the various leadership skills that are necessary to employ during a WG's lifecycle. For example, a Chair has to ensure that debates are conducted in an open and transparent manner and that all interests are equally and adequately represented within the Group's discussions. During the later stages of a WG when recommendations are drafted, a Chair will benefit from understanding the viewpoints of various members to ensure that an acceptable and effective outcome – ideally in the form of consensus – can be achieved.

The WG Chair is specifically expected to carry out the following responsibilities, including but not limited to:

- Attend all PDP Working Group meetings to assure continuity and familiarity with the subject matter and the ongoing discussions;
- Prepare meetings by reading all circulated materials;

- Be familiar with the subject matter and actively encourage participation during the calls;
- Be active on the PDP mailing list and invite PDP WG members and liaisons to share their viewpoints;
- Drive the progress forward and assure that discussions remain on point;
- Work actively towards achieving policy recommendations that ideally receive full consensus;
- Ensure that particular outreach efforts are made when community reviews are done of the group's output;
- Underscore the importance of achieving overall representational balance on any sub-teams that are formed;
- Enforce Statement of Participation, ICANN’s Standards of Behavior, and Community Anti-Harassment Policy;
- Coordinate with staff and ensure that the WG is supported as effectively as possible; and
- Conduct consistent, adequate, and timely reporting to the GNSO Council on the progress of the PDP.

The WG Chair is expected to meet most of the following qualifications:

- Direct experience in consensus building processes and preferably direct experience in GNSO PDPs;
- Knowledge of and preferably direct experience in IDN related work at ICANN;
- Knowledge of ICANN policies and procedures as they relate to the relevant issue;
- Project management skills: including facilitating goal-oriented Working Group meetings, agenda setting and adherence, time management, encouraging collaboration, driving the completion of action items and achieving milestones in accordance with the WG timeline and work plan, keeping the Working Group’s actions, discussions and meetings focused on serving its ultimate goals and deliverables;
- Ability to enforce compliance with the Statement of Participation, ICANN’s Expected Standards of Behavior, and Community Anti-harassment Policy;
- Ability to determine when outreach is necessary and to undertake it;
- Ability to identify the diversity of views within the Working Group, if applicable;
- Knowledge of and ability to designate consensus on Working Group recommendations based on the level of agreement;
- Ability to help Working Group members understand that a consensus is a decision that is collaboratively reached and that the Working Group members can “live with”; accordingly, it may not be a perfect or unanimous decision;
- Commitment to review the Consensus Playbook and attend potential training related to the Playbook, facilitate consensus building by employing the tools and techniques as detailed in the playbook;
- Ability to refrain from promoting a specific agenda and ensuring fair, objective treatment of all opinions within the Working Group;
- Ability to distinguish between Working Group members offering genuine dissent and those raising irrelevant or already closed issues merely to block the Working Group’s progress toward its goal;
- Ability to halt disruption and, in extreme cases, exclude a Working Group member from a discussion per Section 3.5 of the GNSO Working Group Guidelines on Rules of Engagement;

- Ability to ensure that closed Working Group decisions are not revisited, unless there is a consensus to do so (usually in light of new information brought to the Working Group's attention);
- Ability to commit the time required to perform the WG Chair's responsibilities;
- Knowledge of topics in other policy efforts that have relations to or dependencies with the PDP working group topics;
- Ability to create factual, relevant and easily understandable messages, and able to clearly deliver them to the Working Group
- Ability to deliver a point clearly, concisely, and in a friendly way
- Exhibit agility and confidence in evolving situations and is able to swiftly transition from topic to topic
- Highly effective oral, written, and interpersonal communication skills (in simple, comprehensible English);
- Excellent research skills with the ability to discern factual, factually relevant, and persuasive details and sources;
- Commitment to manage a diverse workload, while collaborating with a Working Group of individuals with different background and interests in driving objectives; and
- Able to effectively build a course of action, analyze trade-offs, and make recommendations even in ambiguous situations; and
- Knowledge of and ability to participate in the Working Group complaint process, commitment to review the Clarification to Complaint Process in GNSO Working Group Guidelines Section 3.7.

**Expressions of Interest for the WG Chair:**
Staff is expected to publish a request for Expressions of Interest for the role of Chair. The GNSO Council leadership and Standing Selection Committee leadership will jointly review the responses and will propose a Chair to the GNSO Council which will then either affirm the selection or reject the selection and send the process back to the GNSO Council leadership and Standing Selection Committee leadership.

The Expression of Interest should address the following issues, including but not limited to:

- What is the applicant's interest in this position?
- What particular skills and attributes does the applicant have that will assist him/her in chairing the WG and facilitating consensus building?
- What is the applicant's knowledge of and/or experience in Latin script diacritics related work at ICANN, if any?
- What is the applicant's knowledge of ICANN policies and procedures?
- What is the applicant's experience with the GNSO Policy Development Process?
- What is the applicant's experience with consensus building involving various stakeholders, as well as familiarity with the Consensus Playbook?
- Is the applicant able to commit the time required and necessary work needed to chair the PDP?
- Does the applicant have any affiliation with or involvement in any organization or entity with any financial or non-financial interest in the subject matter of this PDP?
- Also expected to be included:
    - A link to an up-to-date Statement of Interest (SOI) - https://community.icann.org/x/c4Lg
    - A statement confirming commitment and ability to act neutrally.

**Expectations for the Vice Chair:**
Finally, as also pointed out in the GNSO Working Group Guidelines, the Vice Chair may facilitate the work of the Chair by ensuring continuity in case of absence, sharing of workload, and allowing the Chair to become engaged in a particular debate. As a result, similar responsibilities and qualifications are expected from the Vice Chair, although the overall workload may be reduced as a result of being able to share this with the Chair.

**Leadership Review:**

The review of WG leadership provides a regular opportunity for the GNSO Council to check in with WG leadership and Council Liaison to identify resources or input that Council may need to provide, as well as opportunities for the leadership team to improve. The review also enables the GNSO Council to work with the WG leadership and Council Liaison to develop and execute a plan to address possible issues/opportunities identified.

The GNSO Council leadership and/or the Council Liaison may initiate the WG leadership review in response to circumstances indicating that a review is necessary.

The WG leadership shall review the full text of Regular Review of Working Group Leadership document to understand the regular review of WG leadership performance by the GNSO Council, as well as the member survey that feeds into the review. This leadership review may be conducted alongside the WG self-assessment, or be integrated as part of the WG self-assessment based on the GNSO Council's further improvement of the review mechanism.

**GNSO Council Liaison**

The GNSO Council shall appoint one (1) Liaison who is accountable to the GNSO. The Liaison must be a member of the Council, and the Council recommends that the Liaison should be a Council member and be able to serve during the life of this WG.

The complete description of role & responsibilities for GNSO Council Liaison is described in the GNSO Council Liaison Supplemental Guidance. In short, the GNSO Council Liaison is expected to:

- Fulfill liaison role in a neutral manner
    - Importantly, the liaison is expected to fulfil his/her role in a neutral manner. This means that everything the liaison does during his/her tenure, including but not limited to participating in WG calls, reporting status, conveying information, and escalating issues, should be done in that neutral manner.
- Serve as an interim WG Chair until a Chair is named
- Be a regular participant of WG meetings
- Participate in regular meetings with WG Chair
- Report to Council on the WG progress
- Convey to Council on WG communications, questions, concerns
- Inform WG Chair about Council activities impacting the WG
- Refer to Council questions related to WG Charter
- Assist or engage when WG faces challenges
- Assist in case of abuse of ICANN's Expected Standards of Behavior and Community Anti-Harassment Policy
- Assist with knowledge of WG processes and practices
- Facilitate when there is disagreement regarding consensus designation
- Facilitate when a Section 3.7 Complaint Process is invoked
- Initiate the WG leadership review in response to circumstances indicating that a review is necessary

The liaison shall complete the following actions for onboarding purposes:

- Review the GNSO Council liaison to the WGs - Role Description;
- Review the New Liaison Briefing and Liaison Handover document to understand the actions the liaison needs to take for onboarding purposes.
- Consult the supplemental guidance developed to provide more precision in their responsibilities and the frequency in which they must be carried out;
- Familiarize with the provisions of the GNSO Operating Procedures relevant to liaisons;
- Subscribe to the PDP mailing lists and relevant sub teams;
- Subscribe to the PDP Leadership mailing list(s), if applicable. In addition, add o the PDP Leadership Skype chat (or other communication channel) if applicable;
- Consider requesting a catch up call with the relevant GNSO policy support staff. This call should clarify the role of the liaison in terms of PDP conference call attendance, expected responsibilities and an update as to the current status of the PDP if already in operation (milestones and anticipated hurdles);
- Review links to the wiki workspaces and mailing list archives via email;
- (If the PDP is already in operation) Consider requesting that PDP Leadership and the outgoing liaison(s) share relevant briefing documents specific to the PDP, to highlight

the scope of the PDP charter, current status, timeline, milestones, problem areas/challenges, anticipated hurdles, etc;
- (If the PDP is already operational) Participate in an onboarding conference call with the incoming and outgoing liaisons as well as PDP Leadership; GNSO policy support staff will also be present on the call.

**Support Staff:**

The ICANN Staff assigned to the WG will fully support the work of the Working Group as requested by the Chair including meeting support, document drafting, editing and distribution and other substantive contributions when deemed appropriate.

Staff assignments to the Working Group:
- ICANN policy staff members
- GNSO Secretariat

In addition, regular participation of and consultation with other ICANN Org departments such as the GDS is anticipated to ensure timely input on issues that may require ICANN org input such as implementation-related queries. As such, the ICANN Org GDS is expected to appoint at least one (1) Liaison to the WG, as specified in the “Membership Structure” section above.

Furthermore, additional policy staff resources are available to assist the WG leadership for consensus building purposes.

## Section V: Rules of Engagement

**Statements of Interest (SOI) Guidelines:**

Each member of the WG is required to submit an SOI in accordance with Section 5 of the GNSO Operating Procedures.

**Statement of Participation:**

Each Member and Participant of the WG must acknowledge and accept the Statement of Participation (as provided below), including ICANN's Expected Standards of Behavior, before he/she can participate in the WG.

## Statement of Participation

As a Member or Participant of the Policy Development Process on Latin Script Diacritics Working Group:

- I agree to genuinely cooperate with fellow Members of the Working Group to deliberate the issues outlined in the Charter. Where there are areas of disagreement, I will commit to work with others to reach a compromise position to the extent that I am able to do so;
- I acknowledge the remit of the GNSO to develop consensus policies for generic top level domains. As such, I will abide by the recommended working methods and rules of engagement as outlined in the Charter, particularly as it relates to rules in GNSO Working Group Guidelines;
- I will treat all Members of the Working Group with civility both face-to-face and online, and I will be respectful of their time and commitment to this effort. I will act in a reasonable, objective, and informed manner during my participation in this Working Group and will not disrupt the work of the Working Group in bad faith;
- I will make best efforts to regularly attend all scheduled meetings and send apologies in advance when I am unable to attend. I will take assignments allocated to me during the course of the Working Group seriously and complete these within the requested timeframe.
- I agree to act in accordance with ICANN Expected Standards of Behavior, particularly as they relate to:
- Acting in accordance with, and in the spirit of, ICANN's mission and core values as provided in ICANN's Bylaws;
- Listening to the views of all stakeholders and working to build consensus; and
- Promoting ethical and responsible behavior;
- I agree to adhere to any applicable conflict of interest policies and the Statement of Interest (SOI) Policy within the GNSO Operating Procedures, especially as it relates to the completeness, accuracy, and timeliness of the initial completion and maintenance of my SOI; and
- I agree to adhere to the ICANN Community Anti-Harassment Policy and Terms of Participation and Complaint Procedures.

As a Member of the PDP on Latin Script Diacritics Working Group:

- I understand reaching consensus does not mean that I am unable to fully represent the views of myself or the organization I represent. I will abide by the recommended working methods and rules of engagement as outlined in the Charter, particularly as it relates to designating consensus in GNSO Working Group Guidelines.

I acknowledge and accept that this Statement of Participation, including ICANN's Expected Standards of Behavior, is enforceable and any individual serving in a Chair role (such as Chair, Co-Chair, or Acting Chair or Acting Co-Chair) of the Working Group and GNSO Council Leadership Team have the authority to restrict my participation in the Working Group in the event of non-compliance with any of the above.

| |
|---|
| **Problem/Issue Escalation & Resolution Process:** |
| The problem/issue escalation & resolution process within the WG is provided in Sections 3.4 and 3.5 of the Working Group Guidelines. WG members should also reference the Guidelines Concerning ICANN Org Resources for Conflict Resolution and Mediation. |
| **Formal Complaint Process:** |
| The formal complaint process within the WG is provided in Section 3.7 of the Working Group Guidelines. Further details regarding the formal complaint process are included in the Clarification to Complaint Process in GNSO Working Group Guidelines document.<br>The formal complaint process may be modified by the GNSO Council at its discretion. |
| **Section VI: Decision Making Methodologies** |
| **Consensus Designation Process:** |

Section 3.6 of the GNSO Working Group Guidelines, as included below, provides the standard consensus-based methodology for decision making in GNSO WGs.

For consensus building purposes, the WG Leadership, WG Members, and GNSO Council Liaison are expected to review the Consensus Playbook which provides practical tools and best practices to bridge differences, break deadlocks, and find common ground within ICANN processes; potential training related to the Consensus Playbook may be provided for WG Leadership, Members, and GNSO Council Liaison.

### 3.6 Standard Methodology for Making Decisions

The Chair will be responsible for designating each position as having one of the following designations:

- **Full consensus** - when no one in the group speaks against the recommendation in its last readings. This is also sometimes referred to as **Unanimous Consensus.**
- **Consensus** - a position where only a small minority disagrees, but most agree. *[Note: For those that are unfamiliar with ICANN usage, you may associate the definition of 'Consensus' with other definitions and terms of art such as rough consensus or near consensus. It should be noted, however, that in the case of a GNSO PDP originated Working Group, all reports, especially Final Reports, must restrict themselves to the term 'Consensus' as this may have legal implications.]*
- **Strong support but significant opposition** - a position where, while most of the group supports a recommendation, there are a significant number of those who do not support it.
- **Divergence** (also referred to as **No Consensus**) - a position where there isn't strong support for any particular position, but many different points of view. Sometimes this is due to irreconcilable differences of opinion and sometimes it is due to the fact that no one has a particularly strong or convincing viewpoint, but the members of the group agree that it is worth listing the issue in the report nonetheless.
- **Minority View** - refers to a proposal where a small number of people support the recommendation. This can happen in response to a **Consensus**, **Strong support but significant opposition**, and **No Consensus;** or, it can happen in cases where there is neither support nor opposition to a suggestion made by a small number of individuals.

In cases of **Consensus**, **Strong support but significant opposition**, and **No Consensus**, an effort should be made to document that variance in viewpoint and to present any **Minority View** recommendations that may have been made. Documentation of **Minority View** recommendations normally depends on text offered by the proponent(s). In all cases of **Divergence,** the WG Chair should encourage the submission of minority viewpoint(s).

The recommended method for discovering the consensus level designation on recommendations should work as follows:

i. After the group has discussed an issue long enough for all issues to have been raised, understood and discussed, the Chair, or Co-Chairs, make an evaluation of the designation and publish it for the group to review.
ii. After the group has discussed the Chair's estimation of designation, the Chair, or Co-Chairs, should reevaluate and publish an updated evaluation.
iii. Steps (i) and (ii) should continue until the Chair/Co-Chairs make an evaluation that is accepted by the group.
iv. In rare case, a Chair may decide that the use of polls is reasonable. Some of the reasons for this might be:
    - A decision needs to be made within a time frame that does not allow for the natural process of iteration and settling on a designation to occur.
    - It becomes obvious after several iterations that it is impossible to arrive at a designation. This will happen most often when trying to discriminate

between **Consensus** and **Strong support but Significant Opposition** or between **Strong support but Significant Opposition** and **Divergence.**

Care should be taken in using polls that they do not become votes. A liability with the use of polls is that, in situations where there is **Divergence** or **Strong Opposition**, there are often disagreements about the meanings of the poll questions or of the poll results.

Based upon the WG's needs, the Chair may direct that WG Members do not have to have their name explicitly associated with any Full Consensus or Consensus view/position. However, in all other cases and in those cases where a group member represents the minority viewpoint, their name must be explicitly linked, especially in those cases where polls where taken.

Consensus calls should always involve the entire Working Group and, for this reason, should take place on the designated mailing list to ensure that all Working Group members have the opportunity to fully participate in the consensus process. It is the role of the Chair to designate which level of consensus is reached and announce this designation to the Working Group. Member(s) of the Working Group should be able to challenge the designation of the Chair as part of the Working Group discussion. However, if disagreement persists, members of the WG may use the process set forth below to challenge the designation.

If several Members in a WG disagree with the designation given to a position by the Chair or any other consensus call, they may follow these steps sequentially:

1. Send email to the Chair, copying the WG explaining why the decision is believed to be in error.
2. If the Chair still disagrees with the complainants, the Chair will forward the appeal to the CO liaison(s). The Chair must explain his or her reasoning in the response to the complainants and in the submission to the liaison. If the liaison(s) supports the Chair's position, the liaison(s) will provide their response to the complainants. The liaison(s) must explain their reasoning in the response. If the CO liaison disagrees with the Chair, the liaison will forward the appeal to the CO. Should the complainants disagree with the liaison support of the Chair’s determination, the complainants may appeal to the Chair of the CO or their designated representative. If the CO agrees with the complainants’ position, the CO should recommend remedial action to the Chair.
3. In the event of any appeal, the CO will attach a statement of the appeal to the WG and/or Board report. This statement should include all of the documentation from all steps in the appeals process and should include a statement from the CO.

**Who Can Participate in Consensus Designation:**

Consensus calls or decisions are limited to Members who may consult as appropriate with their respective appointing organizations. However, for the purpose of assessing consensus, groups that do not fulfil their maximum membership allowance should not be disadvantaged.

The WG Chair shall ensure that all perspectives are appropriately taken into account in assessing Consensus designations on the final recommendations.

Unless otherwise specified in this Charter, the GNSO Working Group Guidelines apply in full and Consensus designations are therefore the responsibility of the Work Group Chair and are to be made in accordance with the consensus levels described in Section 3.6 of the Working Group Guidelines.

**Termination or Closure of Working Group:**

Typically, the WG will close upon the delivery of its last Final Report, unless assigned additional tasks or follow-up by the GNSO Council.

The GNSO Council may terminate or suspend the WG prior to the publication of its last Final Report for significant cause such as changing or lack of community volunteers, the planned outcome for the project can no longer be realized, or when it is clear that no consensus can be achieved.

The WG Chair, in collaboration with the WG support staff and the GNSO Council Liaison, shall use an escalation procedure, which helps define the health of the WG and informs the GNSO Council's decision on whether the WG should be terminated or suspended.

## Section VII: Change History

## Section VIII: Charter Document History

| Version | Date | Description |
|---|---|---|
| 1.0 | TBD | |
| | | |

| | | | |
|---|---|---|---|
| **Staff Contact:** | TBD | **Email:** | TBD |

**Translations: If translations will be provided please indicate the languages below:**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |