NETBEACON INSTITUTE

White Paper: Proposal for PDPs on DNS Abuse

May 2025

Introduction

This white paper from the NetBeacon Institute sets forth a series of narrowly scoped potential Policy Development Processes (PDPs) focused on specific, actionable aspects of DNS Abuse mitigation and prevention. Our goal in developing this white paper is to foster ICANN Community discussion by providing a set of practical, achievable, and impactful approaches to reducing DNS Abuse. The NetBeacon Institute has a unique vantage point, and from this perspective we believe now is the time to make meaningful, forward-looking progress through Community-driven policy development.

This work is meant to aid and inform—not preempt—existing Community dialogues, offering a possible foundation for exploring the next generation of policy approaches. Each proposed PDP would be designed to be:

- **Narrowly scoped**, with clear, outcome-oriented objectives. This narrow scoping will help ensure the impact of the PDP results in an improved approach to DNS Abuse.
- **Actionable**, grounded in operational realities and informed by Community input.
- **Complementary**, building toward a more complete and enforceable DNS Abuse policy landscape.

Through our NetBeacon Measurement and Analytics Platform (MAP) and NetBeacon Reporter initiatives, we have visibility into how abuse is carried out, how contracted parties are responding, and where policy gaps might lie. As an initiative of Public Interest Registry, and led by a previous chair of the Registrar Stakeholder Group, we also have an operational understanding of industry practices and what improvements could be effective and feasible.

This proposed approach seeks to build directly on Community work such as the recommendations of the GNSO Small Team on DNS Abuse.[1] This team emphasized that, as it relates to policy development on DNS Abuse, "a one-size-fits-all" solution is unlikely to be effective, and instead encouraged the use of practical, tightly scoped efforts where appropriate.[2] Considerable Community efforts have put us in a position to commence these PDPs. In addition to the GNSO Small Team, we want to highlight the Security and Stability

[1] GNSO DNS Abuse Small Team, "Report to GNSO Council," 7 October 2022, https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf.
[2] *Id.* at 8.

Advisory Committee's publication SAC115[3] (and other SSAC work), the Second Security and Stability Review Final Report,[4] the Competition, Consumer Trust, and Consumer Choice Review Team Final Report,[5] work from the At-Large Advisory Committee,[6] numerous communiques from the Government Advisory Committee,[7] as well as ICANN's most recent study Inferential Analysis of Maliciously Registered Domains (INFERMAL).[8]

We were pleased to see the re-formation of the GNSO Small Team on DNS Abuse. Its original work helped sharpen Community focus on the most pressing DNS Abuse issues and was instrumental in building the momentum that led to the recently adopted DNS Abuse amendments to the gTLD Registry Agreement and Registrar Accreditation Agreement.[9] We hope that this work is helpful to that team.

We believe a series of sequential, streamlined, and tightly focused PDPs, each targeting specific abuse-related issues will provide both attainable and meaningful results. While each effort is deliberately narrow in scope, the collective impact could be significant in establishing new standards and obligations to address persistent gaps in abuse mitigation. This approach

---

[3] Internet Corporation for Assigned Names and Numbers (ICANN) Security and Stability Advisory Committee, "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.

[4] Second Security, Stability, and Resiliency (SSR2) Review Team, "SSR2 Review Team Final Report," 25 January 2021, https://www.icann.org/en/public-comment/proceeding/second-security-stability-and-resiliency-ssr2-review-team-final-report-28-01-2021.

[5] Competition, Consumer Trust, and Consumer Choice Review Team, "Final Report," 8 September 2018, https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

[6] At-Large Advisory Committee, "Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations," 8 June 2023, https://www.icann.org/zh/public-comment/proceeding/amendments-base-gtld-ra-raa-modify-dns-abuse-contract-obligations-29-05-2023/submissions/policy-staff-in-support-of-the-at-large-community-at-large-advisory-committee-alac-19-07-2023.

[7] Government Advisory Committee (GAC), "GAC Communique - Istanbul, Türkiye," 18 November 2024, https://gac.icann.org/advice/communiques/ICANN81%20Istanbul%20Communique.pdf; GAC, "GAC Communique - Seattle, United States of America," 17 March 2025, https://gac.icann.org/advice/communiques/ICANN82_Seattle_Communique_.pdf.; *see also* NetBeacon Institute, "GAC Communiques and Community Activity on DNS Abuse," February 2024, https://netbeacon.org/wp-content/uploads/2024/05/Report_2024-01-Community-Activity-on-DNS-Abuse.pdf.

[8] ICANN, "Inferential Analysis of Maliciously Registered Domains (INFERMAL)," 11 November 2024, https://infermal.korlabs.io/static/documents/infermal.pdf. *See also* https://infermal.korlabs.io/.

[9] ICANN organization (org), "Public Comment Summary Report: Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations," 31 August 2023, https://www.icann.org/en/public-comment/proceeding/amendments-base-gtld-ra-raa-modify-dns-abuse-contract-obligations-29-05-2023.

aligns with the GNSO Small Team's 2022 recommendation supporting "tightly scoped policy development" regarding malicious registrations.[10]

The GNSO Small Team further emphasized that such an approach should yield results that are "short, simple, [and] easy to implement requirements."[11] The proposed PDPs are designed to meet those standards.

This document introduces five potential PDP topics for the Community's discussion and consideration, each addressing what we believe to be a specific gap in DNS Abuse policy:

- **Associated Domain Check**: A reactive approach requiring registrars to investigate domains linked to malicious actors, particularly in cases of bulk domain registrations used for DNS Abuse campaigns.
- **Friction in Bulk Registrations for New Customers**: A proactive approach that seeks to introduce friction for new customer accounts, prior to gaining access to high volume registration tools (i.e., API access for new customers), until trust is established.
- **Subdomain DNS Abuse**: A proposal to help address the growing abuse of subdomain services by codifying the responsibilities of registrants who offer them, via requirements in registrar and registry terms of service.
- **Registrant Recourse Mechanisms**: A measure that ensures registrants have a path to challenge enforcement actions of registrars or registries when taken in error.
- **Centralized Coordination on DGA Malware and Botnets**: A proposal to have ICANN serve as a coordination hub for law enforcement and national CERTs in cases involving DGA-based malware and botnets, enabling more efficient, synchronized mitigation.

Two of the proposed PDPs help address an issue gaining increased attention from the Community: malicious registrations associated with "bulk" registrations via unrestricted access to Application Programming Interfaces (API).[12] The INFERMAL report examined factors

[10] GNSO DNS Abuse Small Team, "Report to GNSO Council," 7 October 2022, at 10, https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf.

[11] *Id.* at 11.

[12] The ICANN Community has identified abuse associated with bulk registrations as a priority. For example, the GNSO Small Team on DNS Abuse recommended that "the GNSO Council requests the Registrar Stakeholder Group and others (for example, ICANN org, the RySG and the [NetBeacon Institute]) to further explore the role that bulk registrations play in DNS Abuse . . . ." *Id.* at 4. The GAC has also shown interest in exploring bulk registrations as a contributor to abuse, noting that "it [is] important to look further into the topic of bulk registrations of domain names as one of the most correlated drivers to DNS Abuse, according to the INFERMAL report." GAC, "GAC Communique - Seattle, United States of America," 17 March 2025, at 12, https://gac.icann.org/advice/communiques/ICANN82_Seattle_Communique_.pdf.

making malicious DNS Abuse registrations more likely and determined that "registrars providing API access for domain registration or account creation experience a staggering 401% rise in malicious domains."[13] This concern for bulk registrations via exploitation of an ungated API is reflected in other community work and dialogue, such as in the most recent GAC Communique.[14] Our approach does not seek to waste cycles by defining what number constitutes "bulk," as that effort would be not only unproductive, but counterproductive, as bad actors would likely work around a set threshold. Instead, we try to address issues of access to the tools that enable bulk registrations, making it more difficult to carry out those criminal campaigns.

We believe that with narrow scope, focused engagement, and good-faith collaboration these PDPs can be completed within ten or less meetings of the respective PDP teams.

We recognize that not all of these proposals may ultimately become the subject of policy development, so we offer our thoughts and analysis on these issues to support the GNSO as well as the wider Community in determining what could be potential PDPs.

Executive Summaries: Proposed DNS Abuse PDP Topics

PDP 1: Associated Domain Check

The Problem: Malicious domains are often part of broader campaigns involving dozens or hundreds of related domains. Currently, there is no requirement that registrars investigate other domains associated with those confirmed as malicious, allowing large swaths of malicious infrastructure to persist.

Proposed Solution: This PDP would examine whether registrars, upon receiving a valid abuse report, should be required to review other associated domains, for example by investigating domains in the same user account, or linked to the same registrant. This "pivot" approach would help identify and mitigate related DNS Abuse more effectively, particularly in organized campaigns (including those registered in bulk to conduct such campaigns).

[13] ICANN, "Inferential Analysis of Maliciously Registered Domains (INFERMAL)," 11 November 2024, at 1, https://infermal.korlabs.io/static/documents/infermal.pdf.
[14] GAC, "GAC Communique - Seattle, United States of America," 17 March 2025, at 12, https://gac.icann.org/advice/communiques/ICANN82_Seattle_Communique_.pdf.

PDP 2: Friction Requirements for Accessing Registration APIs for New Customers

The Problem: Malicious actors use ungated APIs to exploit the ability to register large volumes of abusive domains in bulk.

Proposed Solution: This PDP would 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. For example, API access might only be granted to a new customer once some set number of domains remained registered past the Add Grace Period without being identified as abusive. This approach balances the need to prevent abuse with the legitimate use of bulk registration by trusted entities.

PDP 3: Subdomain DNS Abuse Requirements

The Problem: A substantial share of DNS Abuse occurs at the subdomain level, often through third-party services outside of ICANN's direct reach.[15] Suspending a second-level domain due to subdomain abuse risks widespread collateral damage. Registries and registrars lack tools to ensure that services making subdomains available to third parties have responsible practices in place.

Proposed Solution: This PDP would seek to require registrants operating services that generate subdomains for use by third parties to implement basic abuse prevention and response mechanisms, such as maintaining an abuse contact and committing to investigate third-level (or beyond) DNS Abuse. These obligations would flow from registry and registrar terms of service or acceptable use policies. Recent data shows an increase in subdomain-based phishing, so this policy aims to create accountability without unnecessary collateral damage.

PDP 4: Registrant Recourse for DNS Abuse Suspensions

The Problem: Registrants currently lack a consistent and transparent process to contest a domain suspension due to suspected DNS Abuse, even if a legitimate domain is suspended due to a website compromise. Without a clear recourse mechanism, legitimate registrants may suffer reputational or operational harm from mistaken or disputed suspensions.

---

[15] Interisle, "Phishing Landscape 2024: An Annual Study of the Scope and Distribution of Phishing," July 2023, at 4, https://interisle.net/insights/phishing-landscape-2024-an-annual-study-of-the-scope-and-distribution-of-phishing.

Proposed Solution: This PDP would seek to establish a baseline requirement for registrars and registries to provide a publicly available process—such as a webform or email—for registrants seeking to lift a suspension to submit evidence to a registry or registrar for review. While the PDP would not mandate reinstatement of the domain, it would seek to ensure that registrants have a meaningful opportunity to be heard, improving fairness and accountability without weakening DNS Abuse obligations.

PDP 5: Establishing a Centralized ICANN Coordination Role for DGA-Related Malware and Botnet Mitigation

In addition, we note one possible additional track of work for Community discussion. It may be that this work does not necessitate a PDP if ICANN Org instead developed a program along these lines.

The Problem: Today, law enforcement must contact each implicated registry individually when trying to mitigate malware or botnets that use Domain Generation Algorithms (DGAs) at scale, which can result in fragmented, delayed, and inconsistent responses. These are low frequency but high impact events and streamlining their administration would make it easier and faster for law enforcement to deal with large-scale criminal abuse campaigns.

The Solution: This work would seek to establish a role for ICANN as a trusted clearinghouse for DGA-related reports from vetted law enforcement and national CERTs, giving them the option to engage centrally rather than via individual registry operators. ICANN would coordinate with all implicated registries, significantly reducing takedown latency and ensuring a more uniform, timely, and efficient response across the DNS ecosystem.

We also provide potential charter questions for each of the above proposed PDPs for consideration, in case they are helpful in assessing the respective PDP.

Detailed Discussion: Recommended Policy Development Process Work

This section provides a more detailed look into the problem statement and rationale for each proposed PDP.

Associated Domain Check

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 Problem

Criminals often register large portfolios of malicious domains which enables them to launch coordinated phishing or malware campaigns at scale. The Registrar Accreditation Agreement (RAA) currently only requires registrars to evaluate individual domain names upon receipt of an abuse report.[16] 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.

Background and Rationale

Malicious actors routinely register hundreds or even thousands of domains for a single abuse campaign. Recent research from ICANN's Security, Stability, and Resilience Research team indicated that approximately 43% of phishing domains that were flagged as abusive by reputation block lists appear to have been batch registered.[17] Similarly, the 2024 Interisle Phishing Threat Landscape Report found that 27% of the domains used for phishing in their data were registered in bulk.[18]

Yet, when even one of those domains is flagged for abuse, registrars currently have no obligation to check for other related domains—potentially allowing most of the malicious campaign to remain active and undetected. Many responsible registrars already "pivot" and conduct Associated Domain Checks today, but this would require that all registrars act similarly.

---

[16] ICANN, Registrar Accreditation Agreement (RAA), 2013, https://www.icann.org/en/contracted-parties/accredited-registrars/registrar-accreditation-agreement.

[17] ICANN, "Identification and abuse characteristics of batch registered gTLD domains," May 2025, https://ripe90.ripe.net/wp-content/uploads/presentations/65-RIPE_presentation_v1.1.pdf.

[18] Interisle, "Phishing Landscape 2024: An Annual Study of the Scope and Distribution of Phishing," July 2023, at 8, https://interisle.net/insights/phishing-landscape-2024-an-annual-study-of-the-scope-and-distribution-of-phishing.

The Associated Domain Check would solve a major 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. This policy also avoids the complex task of defining exactly how many domains qualify as a bulk registration.

This change, if implemented, could disrupt entire campaigns with a single abuse report. For example, in the well-documented EZ Pass smishing campaigns,[19] one malicious domain report with sufficient evidence could lead to the identification and suspension of hundreds more that share the same account or patterns (e.g. alpha numerical patterns in the domain name string) and for which evidence is available.

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 unfettered access to automated registration tools (like ungated APIs) for high-volume customers would now bear a cost for enabling malicious portfolios. This is why we believe that the Associated Domain Check could have a meaningful preventative impact on the presence of malicious campaigns.

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

This proposed PDP recognizes the balance recommended by the GNSO Small Team:

> Even though there may be evidence of bulk registrations being used for malicious activities, there are also examples in which bulk registrations are used for

[19] Virginia Department of Transportation; EZPass Virginia Service Center, "Active Smishing Scam," https://www.ezpassva.com/news-resources/news/2025/active-smishing-scam.html;
Federal Bureau of Investigation, "Smishing Scam Regarding Debt for Road Toll Services," 12 April 2024, https://www.ic3.gov/PSA/2024/PSA240412.

> legitimate purposes. . . It may be difficult to identify objective factors. . . and there is a risk of impeding bulk registrations for legitimate purposes.[20]

Through this narrowly scoped, evidence-triggered obligation, the ICANN Community could take a substantial step forward in disrupting malicious campaigns, reducing DNS Abuse uptime, and facilitating meaningful reactive steps to mitigate DNS Abuse associated with bulk registrations for criminal campaigns.

Potential Charter Questions

Potential Charter Questions for this PDP could include:

(1) Should 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?
(2) What criteria should be used to define "association" between domains (e.g., customer account ID, registrant email, payment method)?
(3) 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?

Friction Requirements for Accessing Registration APIs for New Customers

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.

The Problem

[20] DNS Abuse Small Team, "Report to GNSO Council," 7 October 2022, at 11-12, https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf.

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 brand new customer account has access to an API where it can create thousands of names at once (i.e., 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.

That practice creates a low-friction, high-reward environment for DNS Abuse, where bad actors can deploy infrastructure faster than defenders can detect or mitigate it. By introducing measured friction—such as withholding API access until a customer demonstrates benign behavior—this PDP seeks to make abuse more expensive, slower, and riskier for attackers.

Background and Rationale

In 2024, ICANN published its INFERMAL report which analyzed the factors that make maliciously registered domains for DNS Abuse more likely. As noted above, it found that "registrars providing API access for domain registration or account creation experience a *staggering 401% rise in malicious domains*,"[21] and that this was the single biggest factor identified for increasing the likelihood of abuse. Frictionless access to APIs allows for campaigns like the EZ Pass Smishing campaign to propagate in a matter of hours.

This PDP proposes that registrars must implement minimum thresholds before granting access to high-speed or high-volume registration methods. Such thresholds could include:

- Requiring that a registrant has held one or more domains through the Add Grace Period without action for DNS Abuse.
- Implementing waiting periods for newly created accounts.
- 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.

These reasonable customer-activity based friction points would not restrict legitimate bulk registrations—such as those by brand owners or researchers that have established accounts with existing registrars—but would ensure that access to these tools is earned, not automatic.

[21] ICANN, "INFERMAL," 11 November 2024, at 1 (emphasis added), https://infermal.korlabs.io/static/documents/infermal.pdf.

We would like to provide two important considerations for this work:

- Effectively all transactions at wholesale registrars are via API. As noted in the Associated Domains Check, this policy would need to differentiate between retail API access, and API access where a signed reseller agreement is in place.
- We suggest 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.[22]

By introducing lightweight but effective friction points, this PDP would shift the balance: making it harder for bad actors to weaponize scale, while preserving legitimate registration use cases through accountable and staged access. We believe this approach creates a meaningful proactive requirement to counter bulk malicious registrations associated with ungated APIs. It also avoids the requirement to set an exact number of "bulk" registrations and instead provides a more future proofed policy based on customer behaviour.

Potential Charter Questions

Potential Charter Questions for this PDP could include:

(1) What minimum safeguards should registrars be required to implement before granting access to high-speed or high-volume domain registration tools (e.g., APIs) to new customer accounts?
(2) How can "trustworthiness" be defined or operationalized in a way that is based on customer behavior rather than identity?
(3) What types of friction (e.g., waiting periods, registration history, and DNS Abuse checks) are both effective and feasible for registrars to implement?
(4) Should 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?

Subdomain DNS Abuse Requirements

This PDP establishes DNS Abuse mitigation obligations for registrants who offer subdomain services to third parties, effectively propagating responsible abuse handling procedures to

[22] Registrars are, of course, free to implement friction based on customer identity, but that friction would be out of scope of this PDP.

the third-level. As a result, registrars and registries would be in a better position to hold registrants accountable for DNS Abuse through enforceable provisions in their terms and conditions.

The Problem

As DNS Abuse mitigation becomes more effective at the second-level, threat actors have shifted to exploiting services that generate subdomains. This change presents serious challenges for the DNS ecosystem. Registrars and registries lack the tools or authority to directly act on abuse occurring at the third level without causing immense collateral damage. 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 connected services or infrastructure. For example, Microsoft 'Office 365 for Business' accounts automatically generate a subdomain of 'example.onmicrosoft.com.' Suspending the 'onmicrosoft.com' domain for the actions of a single malicious user could prevent tens of thousands of businesses from accessing their email and documents.

The 2024 Interisle Phishing Landscape Report[23] shows that 24% of all phishing attacks take place via subdomains—a figure that has more than doubled since 2021. The same report documents 454,948 phishing attacks created on just 750 second-level domains operated by subdomain providers.[24] Meanwhile, a DNS Research Federation analysis found that 36.27% of phishing attacks use subdomain infrastructure belonging to a tiny fraction of domain names[25]—pointing to a concentrated threat vector with limited oversight.

Despite the growing scale of abuse,[26] 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. As a result, malicious actors can operate persistent phishing infrastructure with near impunity.

Background and Rationale

[23] Interisle, "Phishing Landscape 2024: An Annual Study of the Scope and Distribution of Phishing," 23 July 2024, at 4, https://interisle.net/insights/phishing-landscape-2024-an-annual-study-of-the-scope-and-distribution-of-phishing.

[24] *Id.* at 17.

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

[26] *See* Dark Reading: Rob Wright, "Dynamic DNS Emerges as Go-to Cyberattack Facilitator," 16 May 2025, https://www.darkreading.com/threat-intelligence/dynamic-dns-cyberattack-facilitator.

The purpose of this PDP is to create obligations for second-level registrants that operate services generating subdomains used by third parties. The policy would not seek to regulate 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.

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:

1. Maintain a publicly available, monitored abuse reporting mechanism, such as an email address or web form.
2. Prohibit DNS Abuse on any associated subdomains in their own terms of service or similar policy.
3. Review and respond to credible abuse complaints concerning subdomain misuse.
4. Implement internal processes or technical controls to mitigate abuse on third-level domains.

This model provides best practices in proportional enforcement and escalation. As SAC115 further explains:

> The most effective and proportional solution to a particular abuse problem requires understanding the nature of the enabling infrastructure and dealing directly with those providers in the appropriate manner.[27]

Additionally, the GNSO Small Team on DNS Abuse has emphasized the importance of giving registrars and registries practical tools to address new forms of abuse, including those that fall outside existing ICANN contracts. Subdomain abuse is a prime example of that emerging gap—one that is growing rapidly in both volume and severity.

By embedding these new obligations into terms of service, this policy enables registrars and registries to enforce against registrants who host or tolerate DNS Abuse via subdomains—without needing to suspend the entire domain or overreach their technical remit.

---

[27] ICANN SSAC, "SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS," 19 March 2021, at 20, https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-115-en.pdf.

We understand that this PDP is unlikely to result in significant enforcement mechanisms, (aside from ICANN Contractual Compliance requiring that the relevant registry or registrar has the appropriate terms and conditions in place). The focus of this PDP is to create tools for registries and registrars to engage with and require action from services that generate subdomains engaged in DNS Abuse. We also note that having and maintaining an abuse contact is a basic responsibility for any web service engaging with third parties.

Potential Charter Questions

Potential Charter Questions for this PDP could include:

(1) What minimum DNS Abuse mitigation obligations should registrars and registries require of registrants who offer subdomain services to third parties?
(2) Under what conditions should registrars and registries be required to provide notice to the registrant that it is violating the relevant terms of service—for example, when the registrar or registry receives credible reports or other indicators that a registrant is offering subdomain services to third parties and those services are being abused?
(3) What types of abuse reporting mechanisms and internal monitoring processes are appropriate and feasible for subdomain service providers to implement?
(4) Recognizing that suspension of a second-level domain is almost never a proportionate response for abuse on a third-level domain, how should a registry or registrar approach a scenario in which a registrant has not met its obligations under this proposed policy (i.e., provide notice to the registrant of the same)?

Registrant Recourse for DNS Abuse Related Suspensions

The Problem

When a domain name is suspended due to suspected DNS Abuse, registrants currently lack a consistent, transparent process to request that the registrar or registry review its decision.[28] While swift action is often necessary to combat abuse, the 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.

[28] *See* Digital Medusa, "DNS Abuse Mitigation and Human Rights Impact Assessment," 26 March 2025, https://digitalmedusa.org/dns-abuse-mitigation-and-human-rights-impact-assessment/ ("**Access to Remedy**: Individuals affected by takedowns or suspensions must have access to dispute resolution mechanisms.")

Background and Rationale

Suspensions for DNS Abuse are sometimes contested by registrants, particularly when decisions are made based on limited or incomplete information. Yet, 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.

This PDP aims 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. For the avoidance of doubt, this PDP does not intend to create a system in which a registrant has endless bites of the apple; instead it would provide an opportunity for a registrar or registrar (whichever applied the suspension) to review the relevant information.[29]

This PDP proposes a clear, minimum standard requiring that registrars and registries:

1. Maintain a publicly available webform or email address through which registrants can request review.
2. Be willing and able to accept and review evidence submitted by the registrant.
3. Evaluate the submission in good faith, with the discretion to maintain or lift the suspension based on the merits of the evidence.

This approach echoes guidance from the Internet & Jurisdiction Policy Network, which recommends that: "Registrars and Registries should maintain a publicly available process (even an informal one) for allowing a registrant to contest or appeal an action against a domain name for technical abuse," and that the registrant's submission "must include independently verifiable evidence that does not require (or at least minimizes the need for) the DNS Operator to interpret the law, which is generally outside the DNS Operator's expertise."[30]

---

[29] This PDP would not presume reversal or lifting of a suspension. A registry or registrar may certainly determine that the suspension was correctly applied and not reverse. Similarly, this process is not intended to reverse a suspension that is put in place as a result of a court order).

[30] Internet & Jurisdiction Policy Network, Domains & Jurisdiction Program: "Operational Approaches; Norms, Criteria, Mechanisms," April 2019, at 28,

By creating a lightweight and non-adversarial process, this policy improves procedural fairness and accountability in abuse-related suspensions. It does not mandate reversal of any suspension but ensures that registrants have access to a process for recourse—an essential safeguard in a robust and trustworthy DNS Abuse mitigation framework.

Potential Charter Questions

Potential Charter Questions for this PDP could include:

(1) What minimum standards should be required of registrars and registries to provide registrants with a mechanism for requesting review of a domain suspension related to DNS Abuse, particularly including, but not limited to, instances in which a domain is suspended due to a compromise at the website level? Could such a mechanism be a webform, or a dedicated email address for reviewing these submissions?
(2) What elements should be included in a registrant recourse process to ensure it is accessible, fair, and does not unduly burden DNS Abuse mitigation efforts?
(3) Should registrars and registries be required to accept and evaluate reasonable and actionable supporting evidence from registrants contesting a suspension, and what constitutes "reasonable" evidence in this context?
(4) How can the process foster procedural fairness for registrants while preserving the discretion of registrars and registries to maintain suspensions where DNS Abuse is confirmed?

Establishing a Centralized ICANN Coordination Role for DGA-Related Malware and Botnet Mitigation

Note: 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.

The Problem

When law enforcement or national Community Emergency Response Teams (CERTs) detect malware or botnet operations using domain generating algorithms (DGAs), the malicious domains are often spread across multiple registries. Currently, investigators must contact

https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf.

registries individually, which is slow, inconsistent, and fragmented. A time-consuming DNS Abuse practice means malicious activity is able to persist longer than necessary.

Background and Rationale

To address this challenge, this PDP 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 will not only 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.

ICANN would then prepare the necessary Security Response Waivers (SRWs) and liaise with the relevant registries. Registries would still be able to engage with the relevant law enforcement if there are questions. ICANN could also notify any ccTLDs that wish to opt-in to such a program (since ccTLDs would not be bound by any policy outcome). This approach builds on the existing work between the GAC's Public Safety Working Group and the gTLD Registries Stakeholder Group, which collectively published a "Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets"[31] as well as the Internet & Jurisdiction Policy Network's "Framing Brief: Improving the Workflow of Fighting Botnets: Handling Algorithmically Generated Domains (AGDs)."[32]

Registries would still be able to work with identified "abuse warehousing" registrars (i.e., registrars that do not accept retail registrations from the public, but rather warehouse domains previously associated with DNS Abuse for study) to administer or fulfill the terms of the law enforcement initiative(s).

Efficiencies in this process are important given the scale involved with DGAs. As noted in the PSWG and gTLD Registries' publication, 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

[31] GAC's Public Safety Working Group (PSWG) and the gTLD Registries Stakeholder Group (RySG), "Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets," https://www.rysg.info/wp-content/uploads/assets/Framework-on-Domain-Generating-Algorithms-DGAs-Associated-with-Malware-and-Botnets.pdf.

[32] Internet & Jurisdiction Policy Network, Framing Brief: "Improving the Workflow of Fighting Botnets: Handling Algorithmically Generated Domains (AGDs)," 4 October 2022, https://www.internetjurisdiction.net/uploads/pdfs/REF-22-105.Oct.4.2022-1.pdf.

> 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 LE to go before the courts on an annual basis to refresh authority for seizure of the (very large) list of domains expected to be generated by the DGA that year[.] In turn, LE 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.[33]

Proposed Policy Elements:

- Establish ICANN as a trusted escalation and coordination point for DGA-related abuse, receiving reports from law enforcement.
- Define a standardized intake and validation process within ICANN for DGA evidence submissions.
- Enable ICANN to issue SRW waivers or pre-authorized notices to implicated registries to allow prompt action in accordance with contractual obligations.
- Create a notification and coordination protocol for impacted registries to respond simultaneously based on centralized guidance.
- Provide contractual clarity to ensure registries and registrars can rely on ICANN's role in good faith without fear of violating contractual requirements.

Alignment with GNSO Abuse Mitigation Guidance:

This hub-and-spoke coordination model is also consistent with ICANN's remit to support the stability and security of the DNS, and provides a pragmatic alternative to registry-by-registry coordination in time-sensitive, multi-jurisdictional malware and botnet cases.

Potential Charter Questions

Potential Charter Questions for this PDP could include:

(1) Should ICANN serve as a centralized coordination point for receiving, validating, and escalating DGA-related DNS Abuse reports from verified sources such as law enforcement and national CERTS, and provide relevant contractual waivers for gTLD registries in providing notifications?

[33] PSWG and RySG, "Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets," at 3, https://www.rysg.info/wp-content/uploads/assets/Framework-on-Domain-Generating-Algorithms-DGAs-Associated-with-Malware-and-Botnets.pdf.

(2) What minimum process and validation standards should ICANN follow when acting as an intermediary between law enforcement and registries in cases involving DGA-related malware or botnets?
(3) How should registries be expected to respond to centralized abuse reports coordinated by ICANN, and what safeguards are needed to ensure due process and contractual compliance?
(4) What contractual updates or policy clarifications are necessary to support ICANN's role as a trusted intermediary in coordinating timely action on DGA-generated domains for validated law enforcement requests?

Conclusion

We are pleased to offer this white paper for the Community's consideration as it begins to evaluate what should come next in the ongoing work to combat DNS Abuse. In preparing these proposals, we spent significant time reviewing and reflecting on the laudable work of the ICANN Community to date—including efforts by the GNSO Small Team, the GAC, the SSAC, the ALAC, Contracted Parties, and others. We are grateful for the thoughtful analysis and recommendations that have informed this issue so far.

Again, our intent is not to preempt or supersede ongoing community discussions, but rather to provide a resource that can help structure and advance conversations around the next set of possible policy tools.

Each of the proposed PDP topics targets an area where current policy gaps may be impeding progress:

- The **Associated Domain Check** proposal introduces a reactive tool for registrars to investigate other domains linked to a malicious actor, particularly in the context of abuse stemming from malicious domains registered in bulk for malicious campaigns.
- The proposal on introducing **friction into bulk registrations** proposes introduction of friction for new customer accounts prior to gaining access to high-volume registration tools (like APIs) until trust is established.
- The **subdomain DNS Abuse** proposal seeks to help address a growing and underexplored abuse vector by establishing clear obligations for registrants who offer subdomain services via registrar and registry Terms of Service.
- The proposal for light touch **registrant recourse mechanisms** offers the other side of what "acting responsibly" on DNS Abuse means; that registrants should have an

avenue to offer evidence that a registrar or registry may have gotten it wrong and ask for reversal, particularly in cases of website compromise.

- Finally, the proposal to have ICANN to serve as a central coordination hub for law enforcement in high-impact **DGA-related malware and botnet** cases offers meaningful efficiencies—streamlining communications and enabling faster, synchronized mitigation across affected registries.

We look forward to any community discussion and welcome feedback. Comments can be sent to info@netbeacon.org. We remain available and interested in engaging further on these issues as we continue our work in making the Internet safer for everyone.