ICANN | GNSO

Generic Names Supporting Organization

DRAFT Initial Report on the DNS Abuse Mitigation Policy Development Process 1

Status of This Document

This is the Initial Recommendations Report of the GNSO DNS Abuse Mitigation Policy Development Process 1 (here after DNSAM PDP1) Working Group (WG) WILL BE posted for public comment.

Preamble

The objective of this Initial Recommendations Report is to document the Working Group's deliberations on charter questions and on its eight (8) preliminary recommendations to consider before the group issues its Final Report after review of public comments received on this report. The Final Report will be delivered to the GNSO Council for its consideration.

Table of Contents

Table of Contents

1. Executive Summary

The GNSO Council requested an Issue Report on DNS Abuse in August 2025 and in doing so, suggested three (3) priority topics that should be included in the Policy Development Process (PDP) on DNS Abuse that is expected to follow the completion of the Final Issue Report. The DNS Abuse Small Team, in alignment with community support, recommended narrowly scoped PDPs on three issues. The Final Issue Report 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 on:

1. **Associated Domain Checks:** A framework requiring registrars to proactively pivot to investigate domains linked to malicious actors, particularly in cases of high-volume domain registrations used for DNS Abuse campaigns.

Threat actors register large portfolios of malicious domains which enables them to launch coordinated phishing or malware campaigns at scale. The Registrar Accreditation Agreement (RAA) currently requires registrars to evaluate individual domain names upon receipt of a DNS Abuse report. 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. Without this requirement, an attacker might only lose one domain at a time, continuing to use the rest until each is individually reported. 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. If registrars proactively pivot on the information, it could potentially curtail whole campaigns.

On 11 December 2025 the GNSO Council voted to initiate two policy development processes (PDPs) on DNS Abuse Mitigation: PDP 1 on Associated Domain Checks to convene its working group immediately and PDP 2 on safeguards for unrestricted API access to convene when the GNSO Council decides it is an appropriate time, taking into consideration the progress and resources needed for DNS Abuse Mitigation PDP 1. Following the convening of a charter drafting team, the GNSO Council adopted the DNS Abuse Mitigation PDP 1 charter on 15 January 2026. The DNSAM PDP1 WG had its kick-off meeting during ICANN86.

The DNSAM PDP1 WG has developed eight (8) preliminary recommendations aiming to address the issue above. The list of recommendations includes:

- Preliminary Recommendation 1: Associated Domain Check (ADC) Trigger
- Preliminary Recommendation 2: ADC Investigation
- Preliminary Recommendation 3: Reasonable Investigation
- Preliminary Recommendation 4: Determining Association

- Preliminary Recommendation 5: Safeguards for ADC Investigations
- Preliminary Recommendation 6: Timeline for ADC
- Preliminary Recommendation 7: Measuring ADC Policy Effectiveness
- Preliminary Recommendation 8: Demonstrating Compliance

The following section will provide in detail the WG`s recommendation text and rationale.

2. Preliminary Recommendations

The WG was chartered to provide the GNSO Council with "policy recommendations regarding the issues identified in the DNS Abuse Mitigation Final Issue Report. Following its analysis of each of the questions outlined in its Charter related to this task, the WG has arrived at a set of preliminary conclusions and recommendations. The WG believes that when it formulates its final recommendations, if approved by the GNSO Council and the ICANN Board, there will be substantial improvement to the current environment. The objective of this PDP is to establish a more consistent framework for the initiation and conduct of ADCs in connection with DNS Abuse investigations. While some registrars may already conduct ADCs voluntarily or pursuant to their own operational practices, the WG discussed that existing approaches may vary significantly across registrars in terms of methodology, thresholds, safeguards, timing, and accountability mechanisms. In this context, the PDP seeks to develop more consistent baseline requirements and expectations across registrars, including with respect to proportionality, evidentiary standards, safeguards, operational considerations, and efforts to minimize false positives and collateral impacts on legitimate registrants.

The WG was chartered by the GNSO Council to create an obligation for registrars to investigate other domains associated with a customer account or registrant where at least one domain is found to be engaged in DNS Abuse, as defined in the RAA. Following its analysis of each of the questions outlined in its Charter related to this task, the WG has arrived at a set of preliminary recommendations and conclusions.

The WG has now completed its consideration of Charter Questions 1 to 9. In many cases, the responses led to preliminary policy recommendations, including related rationale and/or implementation guidance. Throughout this work, the WG recognized that several Charter Questions address interconnected issues/aspects and therefore resulted in overlapping themes or complementary approaches. To keep the recommendations clear, coherent, concise, and easier to implement, the WG sought to avoid repeating substantially similar recommendations across multiple sections. Where overlap existed, the intent was to consolidate related concepts where appropriate, while ensuring that each recommendation remains distinct.

Types of DNS Abuse Mitigation PDP1 Working Group outputs

Recommendation:
The Working Group expects that the GNSO Council and ultimately the ICANN Board will approve and implement all recommendations set forth in this Final Report, and ICANN Org will work closely with an Implementation Review Team (IRT) to ensure that implementation takes place in

line with the Working Group's intent. Recommendations often address what the Working Group recommends takes place, as opposed to how it should take place. Recommendations typically use the term "must," indicating that the recommended action is required to take place and/or necessary.

Implementation Guidance:
The Working Group strongly recommends the stated action, with a strong presumption that it will be implemented, but recognizes that there may exist valid reasons in particular circumstances to not take the recommended action exactly as described. However, the party to whom the action is directed must make all efforts to achieve the purpose behind the recommended action (as expressed in the rationale and the recommendation to which the implementation guidance is linked, if applicable) even if done through a different course. In all cases, the full implications must be understood and carefully weighed before choosing a different course. Implementation guidance commonly refers to how a recommendation should be implemented.

2.1. Proposed Recommendation 1: Associated Domain Check (ADC) Trigger

Preliminary Recommendation 1
When a registrar has actionable evidence that a Registered Name is being used for DNS Abuse pursuant to Section 3.18.2 of the Registrar Accreditation Agreement (RAA), the registrar MUST perform an Associated Domain Check (ADC). For the avoidance of doubt, this requirement MUST not extend to compromised domains.

Preliminary Implementation Guidance
When reviewing actionable evidence for the purpose of ADC, the phrase "is being used for DNS Abuse" is not limited to DNS Abuse that is active at the time of review. Registrars may rely on actionable evidence of current, recent, intermittent, recurring, or otherwise well-evidenced DNS Abuse, including where the domain is no longer active or the abusive activity has ceased. Abuse reports submitted to a registrar should include sufficient information and evidence to support the reported allegation of DNS Abuse. Where the reported abuse is intermittent, recurring, or otherwise not continuously observable, the report should include evidence clearly demonstrating the pattern of abusive activity.

Preliminary Rationale
The WG considered that the trigger for an ADC should remain tied to Section 3.18.2 of the RAA and to the registrar having actionable evidence of DNS Abuse. The trigger avoids potentially onerous demands on registrars, which could arise from an overly broad or speculative trigger, such as relying on an unsubstantiated report of DNS Abuse or a prediction of future abuse behavior. The requirements under section 3.18.2 of the RAA do not establish limitations on where the actionable evidence is acquired. What this means, in a practical sense, is that the registrar can identify the actionable evidence through its own analysis or the registrar can be informed by a report from any external reporter – e.g., law enforcement, cybersecurity professionals, ICANN org, IP rights holders and agents, etc. – both may constitute valid sources of actionable evidence under the RAA. The WG further considered, as noted in the Charter, that

an ADC is most appropriately required where the registrar has sufficient indicators to reasonably determine that the domain name has been registered for the sole purpose of conducting DNS Abuse, rather than where a legitimate domain has been compromised by a third party. Compromised Domain means a domain name that was registered for legitimate purposes but is subsequently exploited, or controlled by an unauthorized party to conduct DNS Abuse without the knowledge, authorization, or participation of the registrant and/or when an otherwise legitimate or benign domain name is used as a vector for DNS Abuse without the knowledge or consent of the registrant.

Actionable evidence as defined in the ICANN Advisory on Compliance With DNS Abuse Obligations means that the information that is readily available to the registrar must be sufficient to enable the registrar to make a reasonable determination as to whether the Registered Name is being used for one or more forms of DNS Abuse. Registrars are encouraged to proactively monitor the Registered Names that they sponsor to identify potential DNS Abuse. A registrar's assessment of actionable evidence will vary depending on the circumstances of each case. Abuse reports submitted to a registrar should include sufficient information and evidence to support the reported allegation of DNS Abuse. Where the reported abuse is intermittent, recurring, or otherwise not continuously observable, the report should include evidence reasonably demonstrating the pattern of abusive activity.

The WG discussed whether the obligation to perform an ADC should be conditioned on the registrar having completed mitigation action in respect of the domain name that triggered the ADC. However, the WG concluded that an ADC is part of a proactive mitigation action to identify whether one or more associated domains have been registered for the sole purpose of conducting DNS Abuse. Hence, relative to the triggering domain name, an ADC can be performed prior to taking mitigation action; in parallel with mitigation action; or where the registrar has already taken or is in the process of taking appropriate mitigation action. The WG discussed that the trigger for ADC should not substantially delay prompt mitigation action on already existing obligations.

2.2. Proposed Recommendation 2: ADC Investigation

Preliminary Recommendation 2
A registrar MUST perform a reasonable investigation in order to determine whether or not associated domains are used for DNS Abuse per 3.18.2 of the RAA.

2.3. Proposed Recommendations 3: Reasonable Investigation

Preliminary Recommendation 3
A reasonable investigation by a registrar MUST consist of reviewing information reasonably accessible to the registrar in the normal course of its operations to determine whether associated domain names are being used for DNS Abuse, per 3.18.2 of the RAA. A reasonable investigation MUST be practical and proportionate based on the circumstances and consistent with Section 3.18.2. A reasonable investigation MUST NOT require registrars to access or

generate data that is not reasonably available to them, recognizing that registrar capabilities, technical systems, and available data may differ across and within registrars.

Registrars MAY conduct an ADC by using a flexible, non-exhaustive set of criteria that allows registrars to identify domains that are reasonably linked to the same abusive activity, account, or actor.

Preliminary Implementation Guidance:
For the purposes of this policy, "reasonably accessible data" includes:

- Data required to be collected or maintained under applicable ICANN agreements;
- Data otherwise held by the registrar and accessible through its technical systems; and
- Information received by the registrar in connection with an abuse report or investigation.

Where a registrar operates through a reseller or similar business model:

- A registrar may rely on a reseller to conduct ADC investigation steps using data reasonably available to the reseller.
- Registrars will remain responsible for all relevant contractual obligations, as required by 3.12 of the RAA. This means the registrar is fully responsible for complying with all RAA requirements (including 3.18) even when it uses a reseller.

2.4. Proposed Recommendation 4: Determining "Association"

Preliminary Recommendation 4
To determine whether "association" exists, a registrar MUST take into consideration potential indicators such as the Registered Name Holder or account-related information and/or technical or coordinated activity/behavioral indicators, that are reasonably accessible to the registrar and most likely to yield useful and actionable information. When determining "association," registrars MUST take into account what is reasonably access to the registrar; the specific elements considered in any given ADC, even within a single registrar, may vary depending upon the particular circumstances.

Preliminary Implementation Guidance
Such association MAY include, but is not limited to, the following factors as applicable and as available:

- domains within the same account, customer, registrant, end customer, or other potential common connection point;.
- domains exhibiting common patterns or indicators of coordinated activity, including naming conventions, shared infrastructure (e.g., nameservers), and/or campaign characteristics identified through internal analysis or external reporting; or
- domains linked through information reasonably available to the registrar during its operations, including information derived from internal analysis and/or external reports that provide indicators of what to look for in a campaign.

Preliminary Rationale on Preliminary Recommendation 2-4
The WG recommends that registrars may use a range of technical, operational, or abuse intelligence signals, recognizing that different indicators (e.g., email addresses, account identifiers, infrastructure patterns, or behavioral signals) may be relevant depending on the

circumstances, and that no single data point will be determinative in all cases. The policy should not prescribe a fixed or exhaustive sequence of investigation steps, but should allow registrars to apply a range of indicators and pattern recognition signals appropriate to the circumstances. This policy only requires ADC within a registrar portfolio and does not require cross-registrar checks/coordination. A reasonable investigation should remain distinct from enforcement, meaning registrars should assess available evidence first and determine proportionate next steps based on that assessment. The WG intends that ADCs remain evidence-driven and proportionate. The recommendation is not intended to require registrars to conduct portfolio-wide reviews as a matter of course. At the same time, the WG recognises that the facts and circumstances of a particular case may justify a broader review. Accordingly, the recommendation neither mandates nor prohibits a more comprehensive investigation where such action is reasonable and proportionate under the circumstances. For the avoidance of doubt, a proportionate investigation is one that is reasonably tailored to the available evidence and the nature, scope, and severity of the reported DNS Abuse. The WG understands that proportionality may support reviewing a limited number of associated domains in some cases, while in other cases a broader review may be justified where the evidence indicates a larger coordinated abuse campaign, multiple related domains, or other factors suggesting that abuse extends beyond the reported domain name.

2.5. Proposed Recommendation 5: Safeguards for ADC investigations

Preliminary Recommendation 5
ADC MUST be conducted in compliance with applicable law(s) (including data privacy laws) and contractual requirements. A registrar MUST NOT be required to collect or generate new data solely for the purpose of ADC and/or demonstrating compliance. Furthermore, nothing in this policy should be understood to prohibit a registrar from using data, tools, or services that it may lawfully use in the normal course of its operations to investigate DNS Abuse and conduct ADC.

However, registrars MUST apply “association” criteria for ADC in a reasonable and proportionate manner taking into consideration the following (non-exhaustive):

- the risk of over-association, including scenarios where domains may be linked through reseller models, privacy/proxy services, or shared data that does not reflect common control;
- avoid reliance on assumptions that all domains sharing attributes are by default controlled by the same bad actor;
- the importance of ensuring that association is based on indicators that are meaningful and actionable, rather than speculative;
- the importance of accessing data only when deemed necessary to perform the ADC;
- usage of minimum information reasonably available and necessary to determine whether domain names are associated and avoid collecting or processing additional data not needed for that purpose; and,
- the potential impact on domain name registrants.

Preliminary Implementation Guidance

The WG recommends that a registrar conducting an ADC SHOULD limit access to and correlation of data to what is reasonably appropriate for the investigation, taking into account the purpose of the check, the nature of the evidence, and the need to protect registrants and registrars. The policy SHOULD avoid creating an overly prescriptive or obligation-heavy privacy framework and instead rely on high-level safeguards that can operate across different jurisdictions, business models, and technical environments. The policy SHOULD NOT require incident-level sharing of precise information unless otherwise required by applicable law or contract, and any approach to retention of investigation results SHOULD be consistent with applicable law and existing contractual obligations, rather than creating a separate, retention regime under this policy. However, proportionate and lawful sharing of relevant information SHOULD be permitted where necessary for effective abuse mitigation or compliance with applicable law or contractual obligations.

Preliminary Rationale
WG members agreed that existing registrar contracts and laws already provide core safeguards. Furthermore, WG members said that ADCs must account for registrar agreements, GDPR, and country-specific laws. They proposed registrars should access only data reasonably appropriate for DNS Abuse investigations and only for the investigation period. Some WG members said applicable law alone is insufficient because some jurisdictions lack strong privacy protections. Additionally, they clarified privacy concerns related to personal data, not technical checks like nameservers. WG members noted the policy should not discourage proactive investigations and recommend against adding new retention regimes beyond existing legal or contract requirements.

2.6. Proposed Recommendation 6: Timeline for ADC

Preliminary Recommendation 6
A Registrar MUST initiate and conduct an ADC promptly following the trigger as defined in Preliminary Recommendation 1, taking into account the specific circumstances of each case. For the avoidance of doubt, this requirement does not extend to compromised domains.

Preliminary Implementation Guidance
In determining what constitutes “prompt” initiation and completion of an ADC, relevant considerations MAY include:

- the severity and immediacy of the DNS Abuse;
- the scale and complexity of the abuse activity under review;
- the need to minimize collateral impact on legitimate registrants; and
- operational realities and information available.

Preliminary Rationale
The WG discussed a potential timeline for conducting and initiating ADC and noted that retaining a contextual and flexible “promptly” standard aligned with existing RAA obligations. Hence, the WG recommends “Promptly” should be understood to be aligned with the ICANN Advisory: Compliance with DNS Abuse Obligations. The WG further noted that DNS Abuse incidents may vary significantly in urgency, complexity, evidentiary requirements, operational impact, and risk of collateral harm. The WG discussed the consideration of the development of implementation guidance, examples, advisories, or best practices to support consistent interpretation of

"prompt" action under varying operational and abuse scenarios. Some participants preferred a precise timeline over promptly, but most of the WG converged on aligning with the current RAA obligations rather than creating ADC-specific timeline rules.

2.7. Proposed Recommendation 7: Measuring ADC Policy Effectiveness

Preliminary Recommendation 7

Following implementation of the ADC policy, ICANN org should conduct a review of the policy's effectiveness after two years. The review should assess whether the policy is achieving its intended purpose and what, if anything, could be improved.
The review could consider both quantitative and qualitative indicators, including but not limited to:

- Whether registrars are conducting ADCs when the obligation is triggered.
- Whether ICANN Compliance can assess compliance with the ADC obligation.
- Whether associated domains identified through ADCs are being addressed consistently with existing DNS Abuse mitigation obligations.
- Whether the policy has improved consistency of registrar ADC practices across the industry.
- Whether the policy or related implementation guidance should be updated in light of changes in DNS Abuse patterns, methodologies, or operational practices.

Preliminary Rationale

The WG discussed and noted that the review should recognise that DNS Abuse is dynamic and that direct causation between this policy and overall abuse levels may be difficult to establish. The review should therefore avoid relying solely on aggregate abuse-volume statistics and should instead assess the policy's practical effectiveness in improving ADC performance and compliance. The WG expects the IRT to work on the identification of the relevant data points to assess the indicators noted above, as well as the establishment of baseline data for future measurement. IRT to consider whether and how metrics on ADC metrics can be included in the regular DNS Abuse mitigation metrics already produced by ICANN.

2.8. Proposed Recommendation 8: Demonstrating Compliance

Preliminary Recommendation 8

Registrars MUST be able to demonstrate compliance with the ADC requirements when the obligation is triggered by actionable evidence of DNS Abuse. A registrar MUST be able to demonstrate, through records and documentation maintained in the ordinary course of business:

- The trigger and time of trigger of the ADC.
- Whether and when an ADC was conducted.
- What information was reviewed that was reasonably accessible directly to the registrar

or through its reseller at the time.
- Whether, and how many, associated domains were identified.
- What resulting action, if any, was taken in relation to associated domains.
- That the ADC process followed was reasonable and proportionate under the circumstances.

The policy MUST not prescribe a format for documentation. Registrars may maintain evidence in forms provided the evidence is sufficient to demonstrate compliance with the ADC requirements.

A registrar MUST develop and maintain an internal process description for conducting ADCs. This internal process should describe the steps the registrar uses when an ADC is conducted and should take into account any applicable ADC advisory or implementation guidance. The internal process MUST be made available to ICANN upon request.

Preliminary Rationale
The WG intends for this recommendation to be demonstrable and auditable without requiring registrars to create extensive new recordkeeping systems solely for ADC purposes. The purpose of the recommendation is to enable verification that an ADC was conducted and that resulting decisions were supported by a reasonable investigation. The WG expectation is that registrars maintain sufficient records, generated in the ordinary course of business, to demonstrate compliance with the policy requirements.

2.9. Conclusions and Next Steps

This Initial Report will be posted for public comment for 40 Days. After the WG's review of public comments received on this report, it will complete this section documenting any conclusions based on the overall findings of the report.

3. Expected impact of recommendations

As per the PDP Manual, the Initial Report is expected to include "A statement on the WG discussion concerning impact of the proposed recommendations, which could consider areas such as economic, competition, operations, privacy and other rights, scalability and feasibility". This section is also expected to address the expected impact, if any, on human rights.

(PLACEHOLDER TO BE UPDATED WITH FINAL WG IMPACT ASSESSMENT)

4. Glossary

The definitions included in this glossary are intended to support a shared understanding of key terms used by the Working Group and to provide context for the rationale and intent underlying its discussions and outputs. The definitions are specific to this Working Group,are provided for explanatory purposes only, and are not intended to create, modify, or serve as legally binding

definitions. Terms listed here, that are not already contractually defined, should be read as interpretative aids to facilitate clarity and consistency, while allowing sufficient flexibility for implementation.

Actionable Evidence as defined in the ICANN Advisory on Compliance With DNS Abuse Obligations means that the information that is readily available to the registrar must be sufficient to enable the registrar to make a reasonable determination as to whether the Registered Name is being used for one or more forms of DNS Abuse. Registrars are encouraged to proactively monitor the Registered Names that they sponsor to identify potential DNS Abuse. A registrar's assessment of actionable evidence will vary depending on the circumstances of each case. Abuse reports submitted to a registrar should include sufficient information and evidence to support the reported allegation of DNS Abuse. Where the reported abuse is intermittent, recurring, or otherwise not continuously observable, the report should include evidence reasonably demonstrating the pattern of abusive activity.

Compromised Domain means a domain name that was registered for legitimate purposes but is subsequently exploited, or controlled by an unauthorized party to conduct DNS Abuse without the knowledge, authorization, or participation of the registrant and/or when an otherwise legitimate or benign domain name is used as a vector for DNS Abuse without the knowledge or consent of the registrant.

Customer is the target of the ADC which may include a Registered Name Holder, Account Holder, Reseller, and/or Privacy/Proxy Customer as defined in the RAA. A customer is an individual or entity that has entered into an agreement with a service provider, such as a registrar or registry, to receive specific services. This definition extends beyond a simple financial transaction to include any party that holds a registered interest or account, establishing a formal relationship governed by terms of service and ICANN policies.

DNS Abuse: For the purposes of the RAA, the RA, and the ICANN Advisory on Compliance With DNS Abuse Obligations, *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).

End Customer: refers to the final individual or entity that actually uses a service or resource, such as a domain name, for their own purposes rather than for resale or further distribution.

Registered Name: "Registered Name" as defined in the RAA refers to a domain name within the domain of a TLD, whether consisting of two (2) or more (e.g., john.smith.name) levels, about which a TLD Registry Operator (or an affiliate engaged in providing Registry Services) maintains data in a Registry Database, arranges for such maintenance, or derives revenue from such maintenance. A name in a Registry Database may be a Registered Name even though it does not appear in a zone file (e.g., a registered but inactive name).

Registered Name Holder: As defined in the RAA, a “Registered Name Holder” means the holder of a Registered Name.

Reseller: As defined in the RAA, a “Reseller” is a person or entity that participates in Registrar’s distribution channel for domain name registrations (a) pursuant to an agreement, arrangement

or understanding with Registrar or (b) with Registrar's actual knowledge, provides some or all Registrar Services, including collecting registration data about Registered Name Holders, submitting that data to Registrar, or facilitating the entry of the registration agreement between Registrar and the Registered Name Holder.

4.1. Other Relevant Sections of this Report

For a complete review of the issues and relevant interactions of this WG, the following sections are made available in the later pages of this document to satisfy portability needs.

- Background of the issue documenting how it was discovered and eventually approved for further exploration by the GNSO Council
- Documentation of who participated in the WG's deliberations, attendance records, and links to Statements of Interest as applicable.
- An annex that includes the WG's mandate as defined in the Charter adopted by the GNSO Council.
- Documentation on the solicitation of community input through formal SO/AC and SG/C channels, including responses.

5. Deliberations of the Working Group

This Section provides an overview of the deliberations of the WG. The points outlined below are meant to provide the reader with relevant background information on the WG's deliberations and processes, and should not be read as either final recommendations or as representing the entirety of the deliberations of the WG. The WG will not finalize its recommendations to the GNSO Council until it has conducted a thorough review of the comments received during the public comment period on this Initial Report.

5.1. Initial Fact-Finding and Research

Per its Charter, the WG was tasked to review a list of topics and questions, as part of its work to develop policy recommendations relating to DNS Abuse Mitigation focusing on developing requirements for Registrars to conduct Associated Domain Checks on well evidenced DNS Abuse. These topics and questions were derived in large part from the prior work done by staff with the Issue Report and the Drafting Team that developed the WG's Charter. Furthermore, the WG had a consensus building exercise during its kick-off at ICANN86 and received Subject Matter Expertise on current ADC practices before starting their deliberations on the Charter Questions.

The WG grouped all its Charter questions into specific categories (i) Initiating Associated Domain Check(s) (ii) Demonstrating Compliance (iii) Impact Assessments.

5.2. Community Input

According to the GNSO's PDP Manual, a PDP WG should formally solicit statements from each GNSO Stakeholder Group and Constituency at an early stage of its deliberations. A PDP WG is also encouraged to seek the opinion of other ICANN Supporting Organizations and Advisory Committees who may have expertise, experience or an interest in the issue. As a result, the WG reached out to all ICANN Supporting Organizations and Advisory Committees as well as GNSO Stakeholder Groups and Constituencies with a request for input at the start of its deliberations. In response, statements were requested and received from:

- RrSG – Registrar Stakeholder Group
- RySG – Registry Stakeholder Group
- BC– Business Users Constituency
- IPC – Intellectual Property Constituency
- ISPCP – Internet Service and Connection Providers Constituency
- NCSG – Non-Commercial Stakeholder Group
- NCUC – Non-Commercial Users Constituency
- NPOC – Not-for-Profit Organizations Constituency
- ccNSO – Country Code Names Supporting Organization
- ALAC – At-Large Advisory Committee
- GAC – Governmental Advisory Committee
- SSAC – Security and Stability Advisory Committee
- RSSAC – Root Server System Advisory Committee

All responses received were reviewed by the WG and incorporated into the DNSAM PDP1 WG review document and wiki for each of its Charter questions. All of the statements received were

added to the template for each Charter question (where applicable) and reviewed by the WG as part of its deliberations on that particular topic.

5.3. ICANN Org and ICANN Board Interaction

To help support a smooth transition from policy development to eventual implementation of GNSO Council-adopted and ICANN Board-approved recommendations, the WG has been supported by early and ongoing engagement with ICANN org subject matter experts. Liaisons from ICANN org's Global Domains and Strategy (GDS), ICANN Compliance, and ICANN OCTO attended WG calls, providing input and responding to questions where it was possible to do so in real time. The liaisons were available for WG questions to ICANN org that required additional research or input. In addition, the ICANN Board appointed two liaisons to the WG who also regularly attended the WG calls to act as a conduit between the Board and the DNSAM PDP1 WG.

5.4. ICANN Org and ICANN Board Interaction

The WG reported its progress to the GNSO Council through a monthly update to the "Project List" – a compilation of GNSO's active projects, standing committees, and other work organized by the flow of the PDP – in which the DNSAM PDP1 WG's updates were included and refreshed each month. An archive of these lists is available on the wiki. The GNSO Council liaison to the WG served as an additional point of connection between the Council and the WG. Moreover, the leadership team of the DNSAM PDP1 has been invited to speak to the GNSO Council through GNSO Council Webinars prior to ICANN Public Meetings and/or when it was timely to share important information or key milestones

5.5. Deliberations Regarding Initiating Associated Domain Check(s)

The following Charter questions were grouped into this category as already provided by the Charter.

1. What triggers the requirement to investigate associated domain names?
2. What criteria should be used to define "association" between domains? What elements can be considered to establish such "association"?
3. Defining "investigation": What constitutes a "reasonable investigation" by a registrar? What investigation steps are required or recommended? Are the criteria for investigation proportionate and necessary? What is the impact of this investigation on domain name registrants?
4. What data access and privacy safeguards are necessary to protect both registrants and registrars during associated domain checks?
5. If the associated domain checks have an adverse impact on domain name registrants, are there corresponding remedies?
6. What are appropriate timelines and thresholds for initiating and concluding the associated domain check?

The WG deliberated on all these questions above and used the collaboration document to capture its key takeaways and straw proposal language. Further review took place in the WG's preliminary recommendation review document.

5.6. Deliberations Regarding Demonstrating Compliance

The following Charter questions were grouped into this category as already provided by the Charter.

1. 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?
2. What metrics will be used to evaluate the policy's effectiveness?
3. How can registrars demonstrate their compliance with the obligations to ICANN and what types of evidence and information can registrars submit?

The WG deliberated on all these questions above and used the collaboration document to capture its key takeaways and straw proposal language. Further review took place in the WG's preliminary recommendation review document.

5.7. Deliberations Regarding Impact Assessments

The following impact assessments were grouped into this category as already provided by the Charter.

- Human Rights Impact Assessment
- Data Protection Considerations
- Global Public Interest Checklist
- Potential Impact on Consensus Policies

The WG conducted a scoped impact assessment during its deliberations as an opportunity to raise material risks and obvious conflicts through WG input. The scoped assessment was intended to help document and stabilize the current preliminary recommendation language and is not intended to replace the final comprehensive impact assessments. The WG completed its scoped impact assessment as captured in this document: Scoped Impact Assessment DNSAM PDP1.

(PLACEHOLDER FOR FINAL IMPACT ASSESSMENTS)

6. Conclusions and Next Steps

6.1. Preliminary Consensus Designations

Below is the DNSAM PDP1 Chair's designation as to the level of consensus on each recommendation in this Initial Report. These designations were made following the process as outlined in the message to the DNSAM PDP1 WG mailing list on TBC and in accordance with Section 3.6 - Standard Methodology for Making Decisions of the GNSO Working Group Guidelines.[1] By TBC, yes/no objections were received for recommendation.[2]

Recommendation #	Leadership Team's Proposed Designation
DNSAM PDP1	
Recommendation 1: Associated Domain Check (ADC) Trigger	
Recommendation 2: ADC Investigation	
Recommendation 3: Reasonable Investigation	
Recommendation 4: Determining Association	
Recommendation 5: Safeguards for ADC	
Recommendation 6: Timeline for ADC	
Recommendation 7: Measuring ADC Policy Effectiveness	
Recommendation 8: Demonstrating Compliance	

[1] ANNEX 1: GNSO Working Group Guidelines: https://gnso.icann.org/sites/default/files/filefield_23493/annex-1-gnso-wg-guidelines-07apr11-en.pdf

[2] Comments received if any TBC

6.2. Next Steps

The WG will complete the next phase of its work and develop its recommendations in a Final Report to be sent to the GNSO Council for review following its analysis of public comments received on this Initial Report.

7. Approach Taken by the Working Group

7.1 Working Methodology

The DNSAM PDP1 WG began its deliberations on 08 March 2026. It continued its work primarily through weekly conference calls lasting for 90min, in addition to email exchanges on its mailing list, with further discussions taking place at ICANN Public Meetings when scheduled. All the WG's meetings are documented on its wiki workspace including its mailing list, draft documents, background materials and input received from ICANN's SO/ACs and the GNSO's Stakeholder Groups and Constituencies.

The WG also prepared a Work Plan, which was reviewed on a regular basis. In order to facilitate its work, the WG decided to use a template to tabulate all input received in response to its request for Constituency and Stakeholder Group statements (see Annex B).

The WG scheduled community sessions at each ICANN Public Meeting that took place after its formation, at which it presented its preliminary findings and/or conclusions to the broader ICANN community for discussion and feedback. During ICANN85 and ICANN86 the WG had four (4) working sessions per meeting. In addition, the WG organized an ICANN86 prep-week webinar on 21 May 2026.

The WG deliberated its Charter questions and used the collaboration document to capture its key takeaways and straw proposal language. Further review took place in the WG's preliminary recommendation review document.

7.2. WG Membership and Attendance

The members of the DNSAM PDP1 WG are:

Group / Name	Affiliation	Meetings Attended*
RrSG:		
Name 1	RrSG Member	00
Name 2	RrSG Member	00
Name 3	RrSG Member	00
Name 4	RrSG Member	00
Name 5	RrSG Participant	00
Name 6	RrSG Alternate	00

Group / Name	Affiliation	Meetings Attended*
RySG:		
Name 1	RySG Member	00
Name 2	RySG Member	00
Name 3	RySG Participant	00
Name 4	RySG Alternate	00
RrSG:		
Name 1	Registrar Co. Name	00
Name 2	Registrar Co. Name	00
Name 3	Registrar Co. Name	00
BC		
Name 1	BC Member	00
Name 2	BC Member	00
Name 3	BC Participant	00
Name 4	BC Alternate	
ISPCP:		
Name 1	ISPCP Member	00
Name 2	ISPCP Member	00
Name 3	ISPCP Participant	00
Name 4	ISPCP Alternate	00
IPC:		
Name 1	IPC Member	00
Name 2	IPC Member	00
Name 3	IPC Participant	00
Name 4	IPC Alternate	00
NCSG:		

Group / Name	Affiliation	Meetings Attended*
Name 1	NCSG Member	00
Name 2	NCSG Member	00
Name 3	NCSG Participant	00
Name 4	NCSG Alternate	00
NPOC:		
Name 1	NPOC Member	00
Name 2	NPOC Member	00
Name 3	NPOC Participant	00
Name 4	NPOC Alternate	00
NCUC:		
Name 1	NCUC Member	00
Name 2	NCUC Member	00
Name 3	NCUC Participant	00
Name 4	NCUC Alternate	00
ccNSO:		
Name 1	ccNSO Member	00
Name 2	ccNSO Member	00
Name 3	ccNSO Participant	00
Name 4	ccNSO Alternate	00
ALAC:		
Name 1	ALAC Member	00
Name 2	ALAC Member	00
Name 3	ALAC Participant	00
Name 4	ALAC Alternate	00
GAC:		

Group / Name	Affiliation	Meetings Attended*
Name 1	GAC Member	00
Name 2	GAC Member	00
Name 3	GAC Participant	00
Name 4	GAC Alternate	00
SSAC:		
Name 1	SSAC Member	00
Name 2	SSAC Member	00
Name 3	SSAC Participant	00
Name 4	SSAC Alternate	00
RSSAC:		
Name 1	RSSAC Member	00
Name 2	RRSAC Member	00
Name 3	RRSAC Participant	00
Name 4	RRSAC Alternate	00

The Statements of Interest of the WG members can be found at HERE.

The attendance records can be found at [INSERT LINK]. The email archives can be found at HERE.

* The following are the ICANN SO/ACs and GNSO Stakeholder Groups and Constituencies for which WG members provided affiliations:

RrSG – Registrar Stakeholder Group
RySG – Registry Stakeholder Group
BC– Business Users Constituency
IPC – Intellectual Property Constituency
ISPCP – Internet Service and Connection Providers Constituency
NCSG – Non-Commercial Stakeholder Group
NCUC – Non-Commercial Users Constituency
NPOC – Not-for-Profit Organizations Constituency
ccNSO – Country Code Names Supporting Organization
ALAC – At-Large Advisory Committee
GAC – Governmental Advisory Committee
SSAC – Security and Stability Advisory Committee

RSSAC – Root Server System Advisory Committee

** This list was accurate as of the publication of this report. Note that some members joined the WG only after it began meeting, and WG members that have since left are indicated with ++ against their names.

Annex A – Workplan

Annex B – Membership and Attendance