ICANN | GNSO

Generic Names Supporting Organization

Final Report on the DNS Abuse Mitigation Policy Development Process 1

Status of This Document

This is the Final Report of the GNSO DNS Abuse Mitigation Policy Development Process 1 (hereafter DNSAM PDP 1) Working Group (WG) that will be submitted to the GNSO Council.

Preamble

The objective of this Final Report is to document the WG's deliberations on the DNSAM PDP 1's charter questions, the WG's eight (8) Recommendations and six (6) Implementation Guidance, in addition to its treatment of feedback received during Public Comment. The Final Report will be delivered to the GNSO Council for its consideration.

This Final Report may be translated into different languages; please note that only the English version is authoritative.

Table of Contents

1. Executive Summary **3**
2. Final Recommendations **5**
3. Expected Impact of Recommendations **18**
4. Glossary **20**
5. Deliberations of the Working Group **22**
6. Conclusions and Next Steps **27**
7. Approach Taken by the Working Group **28**

1. Executive Summary

The DNSAM PDP 1 WG was tasked with developing policy recommendations on Associated Domain Checks (ADCs). Following its deliberations on the Charter Questions, the WG has completed its work and is submitting **eight (8) Recommendations and six (6) Implementation Guidance** to the GNSO Council for consideration.

The recommendations establish a framework for when and how registrars should conduct ADCs in response to actionable evidence of DNS Abuse. Taken together, they address:

- when an ADC is triggered;
- what constitutes a reasonable investigation and how association between domains may be determined;
- safeguards and proportionality considerations for ADC investigations;
- the timing of ADCs;
- how the outcomes of the resulting policy should be reviewed and measured; and
- how registrars can demonstrate compliance with the resulting requirements.

At a high level, the proposed framework is intended to create a policy requirement for all registrars to conduct an ADC when triggered. In addition, the framework aims to develop a consistent baseline across registrars while maintaining an evidence-based and proportionate approach. The recommendations do not prescribe a single investigative methodology. Instead, they recognize differences in registrar systems, available information, operational circumstances and the nature of individual DNS Abuse cases.

The WG's deliberations were conducted through a sustained process of weekly meetings, leadership discussions, ICANN Public Meeting sessions and community input. The WG also used the Public Comment period to test and refine its Initial Report. Public Comment feedback was considered in the context of the WG's prior deliberations, with related comments clustered where appropriate so that the underlying issues could be considered together. The review was dependent on WG members' deep preparation for, and participation in, four sessions at ICANN87. In addition to the items flagged by the leadership team (LT), each WG member was asked to flag any public comments which they believed warranted further discussion by the WG. At the end of each session, the Chair invited WG members to raise any concerns not already raised. The WG review at ICANN87 resulted in a combination of drafting changes, clarifications, additional Implementation Guidance and strengthened rationale, while retaining approaches where the WG determined that the underlying issue had already been considered or that a proposed change was not warranted.

The WG thanks the community members and organizations that took the time to submit Public Comments on the Initial Report and WG members for doing their "homework" in advance of the working sessions at ICANN87. The feedback identified a number of areas where the Initial Report could benefit from greater clarity, by addressing inconsistencies, ambiguities and areas where the intended application of the recommendations could be better explained. This input provided a valuable basis for further discussion and consideration by the WG, including during the four working sessions held at ICANN87. The preparatory work by the WG allowed efficient and fulsome consideration of the Public Comments within the deliberately expeditious timeline of this PDP.

The resulting Final Report therefore represents the WG's final policy recommendations following its consideration of the Charter Questions, community input, Public Comment and implementation-related considerations. The recommendations are accompanied by rationales and supporting Implementation Guidance intended to explain their purpose and support consistent implementation.

The Final Report is submitted to the GNSO Council for consideration, with the proposed recommendations subject to the applicable GNSO policy-development process and subsequent consideration by the ICANN Board.

Background and PDP Context

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 was 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 suggested 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 PDP, the Council initiated a PDP on:

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

Threat actors might register portfolios of malicious domains to enable 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 name 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 domain names operated by the same actor, even when those domain names 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 (ADCs) to convene its Working Group (WG) immediately and PDP 2 on safeguards for unrestricted Application Programming Interface (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 PDP 1 WG had its kick-off meeting during ICANN85 in Mumbai.

The DNSAM PDP 1 WG has developed eight (8) recommendations aiming to address the issue above. The list of recommendations includes:

- Recommendation 1: Associated Domain Check (ADC) Trigger
- Recommendation 2: ADC Investigation
- Recommendation 3: Reasonable Investigation
- Recommendation 4: Determining Association
- Recommendation 5: Safeguards for ADC Investigations
- Recommendation 6: Timeline for ADC
- Recommendation 7: Review of ADC Policy Outcomes and Enforceability
- Recommendation 8: Demonstrating Compliance

The following section will provide in detail the WG's recommendation text, implementation guidance, and rationale.

2. Final 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 final conclusions and recommendations. The WG believes that these recommendations, if approved by the GNSO Council and the ICANN Board, will substantially improve the current DNS Abuse environment. The objective of this PDP is to establish a more consistent framework for initiating and conducting 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 such 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 the obligation to check associated domain names. At the same time, the PDP seeks to ensure that in interpreting the requirements to conduct a reasonable ADC, ICANN org cannot impose obligations on registrars that would violate applicable law or globally recognized data protection principles, such as proportionality and data minimization. The Policy that follows should be interpreted with this tenet in mind.

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 final recommendations and conclusions.

The WG has now completed its consideration of Charter Questions 1 to 9. In many cases, the responses led to final policy recommendations, including related and/or implementation guidance. Throughout this work, the WG recognized that several Charter Questions address

interconnected issues/aspects resulting 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. Thus, the final recommendations and implementation guidance should be understood holistically as a set, rather than their constitutive parts.

Types of DNS Abuse Mitigation PDP 1 Working Group Outputs

Recommendation:
The WG 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 WG's intent. Recommendations often address what the WG 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 WG 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.

The glossary section 4 of this report contains definitions of the terms used in the Recommendations and Implementation Guidance.

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

Recommendation 1
When a registrar has actionable evidence that a Registered Name is being used for DNS Abuse as defined in 3.18.1 of the Registrar Accreditation Agreement (RAA), the registrar MUST perform an Associated Domain Check (ADC). For the avoidance of doubt, this requirement does not extend to Compromised Domain Names.

Implementation Guidance 1.1
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 occurring 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 Registered Name is no longer active or the abusive activity has ceased. Actionable evidence may be identified through the registrar's own analysis or received

from an external source, consistent with existing contractual obligations. Abuse reports submitted to a registrar should include sufficient information and evidence to support the reported allegation of DNS Abuse pertaining to the same abuse scheme and/or abusive actor, where relevant. Where the reported DNS Abuse is intermittent, recurring, or otherwise not continuously observable, the information provided should be sufficient to support a reasonable determination of the alleged abusive activity, consistent with the applicable actionable evidence standard.

A Compromised Domain Name means a domain name that is used as a vector for DNS Abuse without the knowledge or consent of the Registered Name Holder or beneficial user. The registrar shall reasonably determine, based on the information accessible to it and the circumstances applicable to the case, if the Registered Name is a Compromised Domain Name.

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, both may constitute valid sources of actionable evidence under the RAA.

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 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.

At ICANN87 during its Public Comment Review, the WG recognized that the current Compromised Domain Name definition could benefit from greater precision as noted in various Public Comments. The discussion indicated support for exploring a simpler definition based on

use of a domain by an unauthorized party as a vector for DNS Abuse. This would preserve the intended exclusion while potentially avoiding subjective determinations about whether a domain is legitimate or benign. The WG also emphasized that excluding compromised domains from the ADC trigger does not remove existing contractual DNS Abuse Mitigation obligations.

The WG considered comments requesting clarification of the sources of actionable evidence and the information relevant to reports of intermittent or recurring DNS Abuse. The WG's intent was not to restrict actionable evidence to external reports or to impose additional reporting obligations beyond the applicable actionable-evidence standard.

The proposed clarification recognizes that actionable evidence may originate from a registrar's own analysis or external sources. For intermittent or recurring abuse, the information should be sufficient to support a reasonable determination of the alleged activity, without imposing an additional or separate evidentiary threshold.

2.2. Final Recommendation 2: ADC Investigation

Recommendation 2
A registrar MUST perform a reasonable investigation in order to determine whether or not Registered Names associated with the trigger domain name are also being used for DNS Abuse as defined in 3.18.1 of the RAA, consistent with Recommendation 1 as well as Recommendations 3-8.

2.3. Final Recommendation 3: Reasonable Investigation

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 as defined in 3.18.1 of the RAA. For the purposes of this Recommendation, information reasonably accessible to the registrar includes, but is not limited to, information ordinarily accessible to the registrar through its contractual obligations, technical systems, and abuse reports.

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 accessible 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.

Implementation Guidance 3.1

The categories of reasonably accessible information identified in Recommendation 3 establish

the minimum baseline for a reasonable investigation. A reasonable investigation does not require consideration of every category in every case but should address those categories that are reasonably relevant under the circumstances. The Recommendation does not prescribe how registrars should review, prioritize, or weigh that information, recognizing that registrar capabilities, technical systems, business models, and the facts and circumstances of individual cases may differ.

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 accessible 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. Final Recommendation 4: Determining "Association"

Recommendation 4
To determine whether "association" exists, a registrar MUST take into consideration reasonably accessible indicators that are relevant under the circumstances and likely to yield useful information. Such indicators MAY include, as applicable, Registered Name Holder or account-related information, technical indicators, and indicators of coordinated activity or registration patterns. When determining "association," the specific elements considered in any given ADC, even within a single registrar, may vary depending upon the particular circumstances.

Implementation Guidance 4.1
When determining whether association exists, the indicators taken into consideration by the registrar MAY include, but are not limited to, the following factors as applicable and as available:

- domains within the same account, customer, Registered Name Holder, end customer, or other potential common connection points, including under differing registrar accreditations within the same registrar family operating on a common platform;
- 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.

These indicators are illustrative and non-exhaustive; their evidentiary weight may vary depending on the circumstances. No single weak or commonly shared infrastructure indicator necessarily establishes association or common control. In some circumstances, one specific indicator may support a reasonable determination of association; in other circumstances, multiple indicators may need to be considered together.[1]

[1] See: "SAC135: SSAC Comments on the Initial Report of the GNSO DNS Abuse Mitigation Policy Development Process 1," 28 September 2026. Available at: https://itp.cdn.icann.org/en/files/publications/sac-135-28-09-2026-en.pdf

Rationale on Recommendations 2-4

The WG recommends that registrars may use a range of technical, operational, or abuse intelligence signals, recognizing that different association indicators (e.g., account identifiers, infrastructure patterns, or registration activity 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 reasonable 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 mitigation, 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 recognizes 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.

On Recommendation 2, the WG considered a minor drafting clarification to align Recommendation 2 with Recommendation 1 and Recommendations 3 – 8. No objections were raised to this adjustment.

The discussion also addressed Public Comment requests to extend ADCs across affiliated registrars operating under common ownership or control. While the WG had previously determined that cross-registrar ADCs were not covered by the Charter, commenters highlighted situations where multiple registrar accreditations operate through shared technical systems or a common abuse desk. Members acknowledged the distinction between shared operational systems and affiliated registrars operating independently. The discussion identified the existing concept of "reasonably accessible" information as potentially relevant where information is already accessible through common systems, without creating a new blanket obligation for cross-registrar investigations. Some members nevertheless questioned whether this would be sufficiently clear or enforceable.

On Recommendation 3, the WG carefully reconsidered comments seeking to specify the categories of information a registrar must consider during a reasonable investigation, including information collected under contractual obligations, technical systems, reseller-held information and abuse reports.

---

and ICANN OCTO “Associated Domain Analysis Using Public Data,” 18 September 2026. Available at: https://www.icann.org/en/system/files/files/octo-044-18sep26-en.pdf

The WG acknowledged ICANN org's explanation that the proposed changes were intended to improve clarity and facilitate implementation, rather than change the underlying standard. However, members expressed concern that the revised wording could materially alter the previously negotiated compromise by implying that information a registrar is contractually required to maintain must necessarily be reviewed, regardless of whether it is reasonably accessible in the normal course of operations.

The WG reaffirmed that the standard of reasonable accessibility is central to ensuring that ADC obligations remain operationally feasible and proportionate. The fact that information is retained under a contractual obligation does not necessarily mean it is readily accessible for an ADC. The WG also recognized differences in registrar systems, business models and applicable data-access restrictions.

On Recommendation 4, the WG considered comments seeking greater specificity concerning the indicators used to determine association, including requests for additional indicators or mandatory consideration of particular categories.

The WG reaffirmed that association must be assessed using indicators reasonably accessible and relevant to the circumstances. The WG deliberately avoided establishing a fixed or exhaustive set of indicators because their relevance and evidentiary value may differ across investigations. Requiring identical indicators or investigative methods in all cases could produce inappropriate associations or fail to accommodate different patterns of DNS Abuse.

The proposed clarification maintains the existing categories of registered-name-holder or account-related information, technical indicators, and coordinated activity or registration patterns, while emphasizing their contextual relevance. The WG considered comments seeking to expand the illustrative list of indicators and explain how individual indicators should be assessed. Members broadly supported clarifying that the list is non-exhaustive and that indicators carry different evidentiary weight depending on the circumstances.

The discussion distinguished weak or commonly shared infrastructure indicators, which may not independently establish association, from more specific indicators that could support a reasonable determination in a particular case. The WG recognized that some investigations may reasonably rely on one indicator, while others may require several indicators considered together.

2.5. Final Recommendation 5: Safeguards for ADC Investigations

Recommendation 5
ADC MUST be conducted in compliance with contractual requirements including but not limited to section 3.7.2[2] of the RAA. 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.

[2] Section 3.7.2 of the RAA: Registrar shall abide by applicable laws and governmental regulations.

Implementation Guidance 5.1

Registrars SHOULD apply "association" criteria for the ADC in a reasonable and proportionate manner. The following are important, non-exhaustive considerations intended to inform a reasonable and proportionate implementation of an ADC. They do not establish separate requirements that must each independently be satisfied or against which compliance is independently assessed:

- 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;
- avoiding reliance on assumptions that all domains sharing only certain attributes are by default controlled by the same malicious 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;
- limiting access to and processing of information reasonably accessible under Recommendation 3 to what is reasonably necessary for the purpose of the ADC, and avoiding collection or processing of additional data not needed for that purpose;
- the risk of false positives or erroneous associations and the potential impact on Registered Name Holders or beneficial users.

In implementing this recommendation, registrars will not be required or expected to take any action in contravention of applicable law, including internationally recognized privacy principles, as appropriate. Implementation of this Policy should not be interpreted as requiring registrars to process more personal data than is reasonably necessary to perform an ADC, or otherwise to act in a manner that disproportionately impacts the fundamental rights of Registered Name Holders. The WG recommends that a registrar conducting an ADC SHOULD limit access to and correlation of data to what is reasonably accessible for the investigation, taking into account the purpose of the check and the nature of the evidence, and the need to protect Registered Name Holders and registrars. The policy SHOULD avoid creating an overly prescriptive framework and instead rely on high-level safeguards (as noted above) that can operate across different jurisdictions, business models, and technical environments. 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.

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 that 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 recommended against adding new retention regimes beyond existing legal or contract requirements.

The WG considered comments seeking to distinguish between ICANN-enforceable contractual obligations and compliance with applicable law, including data privacy laws. ICANN Contractual Compliance explained that the original formulation could create uncertainty about whether ICANN org would be expected to assess compliance with national laws, which falls outside its contractual enforcement role. The WG clarified that they understand it is not for ICANN org to enforce applicable law (including data privacy laws) or the considerations noted in IG 5.1.

The WG did not establish sufficient agreement on the proposed replacement wording. The Chair therefore concluded that the original Recommendation 5 language should be retained and the slightly revised version is meant to tie contractual requirements with the concept of compliance with laws that already exists within the RAA rather than creating a new, freestanding obligation to comply with laws that is either redundant with the RAA or, worse, would have some meaning that it does not already have within the RAA that remains undefined but enshrined in new Policy. This preserves the requirement to conduct ADCs in accordance with applicable law without the intention to establish any new requirement for ICANN to enforce these laws. The WG understands these are outside of scope for ICANN org.

The WG considered comments seeking greater clarity that the safeguards listed in IG 5.1 are important considerations for reasonable and proportionate ADCs, rather than separate contractual compliance tests.

ICANN Contractual Compliance explained that assessing each consideration independently could create expectations beyond the WG's intended policy obligation. The WG supported clarifying that the list is non-exhaustive and does not establish separate requirements that must each independently be satisfied or assessed for compliance.

The WG also supported refinements concerning data minimization, false positives, erroneous associations and potential impacts on Registered Name Holders or beneficial users. These clarifications reinforce the importance of proportionate implementation without prescribing a uniform investigative method.

2.6. Final Recommendation 6: Timeline for ADC

Recommendation 6
A registrar MUST conduct an ADC promptly following the trigger as defined in final Recommendation 1, taking into account the specific circumstances of each case.

Implementation Guidance 6.1
In determining what constitutes “prompt” initiation and completion of an ADC, relevant considerations MAY include:

- the severity and immediacy of the DNS Abuse and risk of imminent harm;
- the scale and complexity of the abuse activity under review;
- the need to minimize collateral impact on Registered Name Holders; and
- operational realities and information available.

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. For the purpose of this PDP and as noted in the ICANN Advisory, promptly means within a reasonable time under the circumstances and without unreasonable delay. There is no fixed deadline for what constitutes prompt, as the appropriate time frame depends on the specifics of each case. A single universal deadline would inevitably be too long in some situations and too short in others.

The WG considered comments seeking clarification that the promptness requirement applies to the conduct of an ADC and not merely its initiation.

Members acknowledged the importance of ensuring that registrars undertake and progress an ADC without undue delay. However, several members cautioned that expressly requiring prompt completion could inadvertently encourage premature closure of investigations, particularly where additional associated domains are discovered or a DNS Abuse campaign remains active.

The WG agreed that the term "conduct" better captures the intended obligation without artificially separating initiation, investigation and completion. The WG also reaffirmed that promptness is assessed in light of the specific circumstances of each case, rather than against a uniform deadline. ICANN Contractual Compliance confirmed that the reasonableness of the time taken is assessed contextually and that a rushed investigation may not satisfy the applicable reasonable-investigation obligation.

The WG considered comments requesting explicit reference to the speed of abusive campaigns and the risk of imminent harm. Members supported recognizing imminent harm as a relevant consideration but questioned the clarity and usefulness of the term "velocity." The WG concluded that the latter could introduce unnecessary ambiguity and that the relevant considerations could be adequately expressed through severity, immediacy and risk of imminent harm.

2.7. Final Recommendation 7: Review of ADC Policy Outcomes and Enforceability

Recommendation 7

Following implementation of the ADC policy, ICANN org should conduct a review after two years from the effective date of the resulting Consensus Policy. The review should assess whether the policy is achieving its intended purpose and what, if anything, could be improved. The review should be informed by relevant quantitative and qualitative information. In interpreting that

information, the review should recognize that changes in overall levels or patterns of DNS Abuse may be influenced by factors other than the ADC policy and may not be directly attributable to the policy alone.

The policy's intended purpose is to:

- establish a consistent minimum baseline across registrars for conducting ADCs when the policy obligation is triggered;
- ensure that compliance with the ADC obligations can be effectively assessed and enforced by ICANN Contractual Compliance and, where appropriate, can act when obligations are not met; and
- contribute to the timely identification and disruption of DNS Abuse campaigns, through the application of ADCs, recognizing that the policy is one of several measures intended to mitigate DNS Abuse.

To support the review, ICANN org should work with the IRT during implementation to refine the set of data, metrics, and other relevant information that can support analysis of the policy's implementation, enforceability, effects, and trends over time. Any baseline information necessary for meaningful comparison should be identified sufficiently early to allow for its collection before the review is conducted. Such data points should, to the extent feasible, be derived from information available to ICANN Contractual Compliance, ICANN's Office of the CTO (OCTO), and a limited set of aggregated information maintained by registrars in the ordinary course of business.

Implementation Guidance 7.1

Information supporting the policy outcome review conducted by ICANN org MAY include, but is not limited to, as appropriate and available, information accessible to ICANN org through existing mechanisms. The following are non-exhaustive examples of potential information sources:

- Reputation data at the domain-level from evidence-based blocklists, including information identifying domain names reported as engaging in DNS Abuse, such as reputation blocklists;
- Bulk Registry Data available pursuant to Specification 4, Section 3 of the Registry Agreement, recognizing that this information does not include registrant-level information such as email addresses, payment information, or other account-level data, but may contain other relevant information such as registrar IANA ID and registration creation date;
- gTLD zone file data available through the Centralized Zone Data Service (CZDS), including delegated domain names and associated nameserver information;
- Passive DNS data, which may provide information regarding DNS query responses and patterns of use;
- ICANN Contractual Compliance data, including information reported through the DNS Abuse Mitigation Enforcement dashboard and its associated open-data reporting;
- relevant findings from ICANN Contractual Compliance audits; and
- metrics and data relating to the enforcement of ADC requirements and related outcomes, as incorporated, where appropriate, into ICANN Contractual Compliance's regular reporting following implementation of the policy.

These sources provide different and complementary forms of information and should be

interpreted in context. For example, ICANN Contractual Compliance data reflects matters that come to Contractual Compliance's attention, including through complaints, investigations and audits, and does not represent a complete record of all registrar DNS Abuse mitigation activity. Accordingly, no individual data source should, on its own, be used to draw broad conclusions about the practices or performance of the registrar population as a whole.

The IRT may further define the relevant metrics, format, methodology and other implementation details within the scope of the information ICANN org is entitled to obtain under applicable contractual requirements. To the extent feasible, ICANN org should publish aggregated ADC data to the extent it lawfully can, so that associated-domain reporting and registrar response can be studied independently and systematically as suggested in SAC135.[3]

The review should be conducted through the established ICANN post-implementation assessment process, including the Policy Status Report process.

Rationale
The WG discussed and noted that the review should recognize 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 should consider whether and how ADC metrics can be included in the regular DNS Abuse mitigation metrics already produced by ICANN.

In considering Public Comment, the WG reviewed concerns that Recommendation 7 did not sufficiently clarify the objective of the effectiveness review, the timing of the review, the data needed to assess outcomes, or the extent to which changes in DNS Abuse could be attributed to the ADC policy. The WG considered proposed revisions intended to address these concerns and agreed to clarify that the review should assess whether the policy is achieving its intended purpose, specify that the two-year period begins on the effective date of the resulting Consensus Policy, and recognize that broader DNS Abuse trends may be influenced by factors beyond the policy. The WG emphasized that the existing description of the policy's intended purpose should remain unchanged, as it provides the basis for evaluating the policy's outcomes.
The WG also considered whether to remove the reference to a limited set of aggregated information maintained by registrars in the ordinary course of business. Members raised concerns that removing this language would reopen a previously negotiated compromise. Although ICANN org highlighted that information held by registrars is not necessarily information it is contractually entitled to obtain, the WG did not reach agreement to remove the reference, and it was retained.

In response to Public Comment on the data needed to support the review, the WG also

[3] **SAC135:** The Security and Stability Advisory Committee (SSAC) submitted SAC135, *SSAC Comments on the Initial Report of the GNSO DNS Abuse Mitigation Policy Development Process 1*, as part of the Public Comment process on 28 September 2026. The Working Group appreciates the SSAC's detailed technical input and consideration, including its observations and recommendations relating to Associated Domain Checks, compliance records and measurement of policy outcomes. The contribution provided useful input for the Working Group's consideration during its review of Public Comment.

considered new Implementation Guidance identifying potential information sources and explaining their limitations. Members emphasized that the list should be non-exhaustive, that data quality and the appropriate unit of measurement must be considered, and that Compliance data do not represent a complete record of registrar DNS Abuse handling activity. The guidance should support a meaningful review without creating new data-access or reporting obligations for Contracted Parties. These changes are intended to clarify how the review may be conducted while preserving the previously agreed policy framework.

2.8. Final Recommendation 8: Demonstrating Compliance

Recommendation 8
Registrars MUST be able to demonstrate compliance with the ADC requirements, through records and documentation maintained in the ordinary course of business, when the obligation is triggered by actionable evidence of DNS Abuse. Some of the data points that MAY be sufficient to show compliance include:

- 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 various 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.

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's expectation is that registrars maintain sufficient records, generated in the ordinary course of business, to demonstrate compliance with the policy requirements. Recommendation 3 is intended to avoid creating a requirement for registrars to collect or generate new data solely for the purpose of conducting an ADC. Recommendation 8 recognizes that registrars MUST be able to demonstrate compliance with the policy through reasonable documentation, internal procedures, and records maintained in the ordinary course of business or developed as part of implementing these requirements. The intent is to ensure that compliance can be demonstrated without creating unnecessary operational burdens for registrars, or resulting in unnecessary collection or processing of data

relating to Registered Name Holders. Recommendation 5 and 8 recognize that registrars may need to establish internal procedures, workflows, and, where necessary, compliance records to demonstrate that ADC obligations have been met.

The WG considered Public Comment seeking clarification of the records and documentation registrars may need to demonstrate compliance with the ADC requirements, including whether registrars that do not currently conduct ADCs, or do not retain records of those activities, may need to establish additional documentation. Commenters also sought clarification that the listed data points are non-exhaustive and may demonstrate compliance individually or in combination, as appropriate.

In response, leadership presented proposed language intended to clarify these points and support effective implementation and enforcement. ICANN Contractual Compliance explained that registrars must be able to demonstrate that an ADC was conducted and that the resulting decisions were supported by a reasonable investigation. Without sufficient evidence, it may be difficult to assess compliance. The proposed wording was intended to clarify this existing requirement, rather than introduce a new obligation.

The WG discussed whether to incorporate the proposed language. While IPC and GAC representatives supported greater clarity, some members, including representatives of the Registrar Stakeholder Group, cautioned that explicitly addressing the creation of new records could reopen a previously negotiated compromise. Members emphasized that the existing recommendation already requires registrars to be able to demonstrate compliance through records and documentation maintained in the ordinary course of business. The Chair concluded that the WG had not reached sufficient agreement to revise the recommendation and retained the original wording.

2.9. Conclusions and Next Steps

The DNSAM PDP 1 Final Report will be considered by the GNSO Council to determine the next course of action. The Initial Report was posted for Public Comment for forty (40) days. The WG reviewed the Public Comments received on this Initial Report and considered whether any changes needed to be made to its final recommendations. The WG's treatment of Public Comment has been noted in the rationale. The WG finalized all recommendations in this Final Report to be sent to the GNSO Council for review. If adopted by the GNSO Council, the Final Report would then be sent to the ICANN Board for its consideration and, potentially, adoption as an ICANN Consensus Policy.

3. Expected Impact of Recommendations

As per the PDP Manual, the Final 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.

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 final recommendation language and was 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 PDP 1.

Once the WG's final Recommendations became more stable, the WG conducted its comprehensive impact assessments as summarized below and accessible here including updates made based on Public Comment received.

HRIA Analysis for DNSAM PDP 1

The worksheet presents a detailed Human Rights Impact Assessment (HRIA) of the final recommendations. It assesses potential effects on relevant human rights (primarily privacy, due process, freedom of expression, freedom of association) and concludes that the final Recommendations are expected to have limited adverse impacts because ADCs are restricted to investigations based on actionable evidence that a Registered Name is being used for DNS Abuse, must comply with applicable law and contractual requirements, and emphasize proportionality. Overall, the assessment finds that the recommendations appropriately balance DNS Abuse mitigation with protection of registrant rights. In this context, the WG worked 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 Registered Name Holders.

GPI Checklist

The worksheet assesses the final Recommendations against the Global Public Interest (GPI) framework. It considers whether the final Recommendations advance objectives such as DNS security and stability, benefit to the Internet community, and ICANN's technical coordination. The analysis concludes that the final Recommendations generally align with the GPI principles by strengthening DNS Abuse mitigation while preserving operational flexibility for registrars and incorporating safeguards to avoid unnecessary burdens or overreach that could impact Registered Name Holders.

Consideration of Data Privacy Issues

The worksheet evaluates the final Recommendations from a data privacy policy perspective rather than providing a legal opinion. It examines whether ADCs require processing of personal data, whether such processing is necessary and proportionate, any potential associated privacy risks, and the safeguards available and discussed to mitigate those risks. The assessment concludes that privacy risks are low because the recommendations limit investigations to reasonably accessible information, discourage creation of new data solely for ADCs, and require compliance with applicable laws.

Consensus Policies

The worksheet reviews existing ICANN Consensus Policies to determine whether and how the DNSAM PDP 1 final Recommendations would affect them. It catalogues current policies across areas such as registration data, transfers, expiration, registry services, and rights protection, and

assesses the expected impact of the proposed recommendations. The overall conclusion is that the recommendations would have minimal to no impact on existing Consensus Policies, as they are expected to establish a new consensus policy governing ADCs rather than substantially modifying existing policy obligations.

4. Glossary

The definitions included in this glossary are intended to support a shared understanding of key terms used by the WG and to provide context for the rationale and intent underlying its discussions and outputs. The definitions are specific to this WG, 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. 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 Name: A Compromised Domain Name means a domain name that is used as a vector for DNS Abuse without the knowledge or consent of the Registered Name Holder or beneficial user. The registrar shall reasonably determine, based on the information accessible to it and the circumstances applicable to the case, if the Registered Name is a Compromised Domain Name.

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: As defined in 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: As defined in the RAA, a "Registered Name" 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 Documents

For a complete review of the issues and relevant interactions of this WG, the following sections are made available in the WG wiki space.

- Background of the issue documenting how it was discovered and eventually approved for further exploration by the GNSO Council: https://icann-community.atlassian.net/wiki/x/AQCtLQ
- Documentation of who participated in the WG's deliberations, attendance records, and links to Statements of Interest as applicable: https://icann-community.atlassian.net/wiki/x/CQCsLQ
- The WG's mandate as defined in the Charter adopted by the GNSO Council: https://icann-community.atlassian.net/wiki/x/AQCsLQ
- Documentation on the solicitation of community input through formal SO/AC and SG/C channels, including responses: https://icann-community.atlassian.net/wiki/x/DgCeOg

5. Deliberations of the Working Group

This Section provides an overview of the deliberations of the WG.

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 ICANN85 and received Subject Matter Expertise on current ADC practices before starting its 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. The following document was shared with instructions for sharing input to all SO/AC SG/C leaders and chairs:

- RrSG – Registrar Stakeholder Group
- RySG – Registry Stakeholder Group
- BC– Business Users Constituency
- IPC – Intellectual Property Constituency
- ISPCP – Internet Service Providers and Connectivity 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

Submissions were received from the following groups:

- Business Users Constituency (BC)
- Governmental Advisory Committee (GAC)
- Intellectual Property Constituency (IPC)
- Internet Service Providers and Connectivity Providers Constituency (ISPCP)

- Non-Commercial Stakeholder Group (NCSG)
- Registrar Stakeholder Group (RrSG)

All responses received were reviewed by the WG and incorporated into the DNSAM PDP 1 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.

5.2.1. Public Comment Review

The DNS Abuse Mitigation PDP 1 WG used the Public Comment period to test its Initial Report, identify areas requiring clarification or improvement, and determine whether the feedback warranted changes before developing the Final Report. The review was designed to build on the WG's prior deliberations, rather than automatically reopen every issue or treat every proposed wording change as a new substantive concern.

How comments were reviewed: To make the review manageable while allowing time for substantive discussion, PDP 1 Leadership grouped comments raising similar or related issues into clusters. This enabled the WG to consider the underlying concern and possible responses together, rather than reviewing each submission individually in sequence. The approach did not exclude individual comments from consideration: WG members were asked to read all submissions in advance and were given opportunities throughout the ICANN87 sessions to raise comments, evidence or concerns they believed had been overlooked or warranted further discussion.

How feedback was assessed: Most comments supported the overall intent of the recommendations while suggesting alternative wording, greater specificity or additional clarification, and a smaller number of comments asked for more substantive review or clarification. The WG considered whether such feedback warranted a change to the recommendation or Implementation Guidance, a stronger explanation of the existing approach in the rationale, or no amendment where the issue had already been considered and the proposed change was not justified.

Documentation: The review approach was communicated to the WG in advance (during the 8 September and 5 October prep week webinars) and reiterated at the start of the ICANN87 sessions. The review tool documenting WG members' considerations was shared with the group in advance. Members were reminded of their responsibility to review the submissions and to raise any concerns not captured in leadership's initial assessment. The WG's discussions and resulting decisions are intended to be reflected in the relevant Public Comment review records and the Final Report rationale, explaining how feedback was considered and why particular changes were or were not made.

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 PDP 1 WG.

5.4. GNSO Council 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 PDP 1 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 PDP 1 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 final 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 final 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 final 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 PDP 1.

Once the WG's final Recommendations became more stable, the WG conducted its full impact assessments as summarized below and accessible here.

HRIA Analysis for DNSAM PDP 1

The worksheet presents a detailed Human Rights Impact Assessment (HRIA) of the final recommendations. It assesses potential effects on relevant human rights (primarily privacy, due process, freedom of expression, freedom of association) and concludes that the final Recommendations are expected to have limited adverse impacts because Associated Domain Checks are restricted to investigations based on actionable evidence that a Registered Name is being used for DNS Abuse, must comply with applicable law and contractual requirements, and emphasize proportionality. Overall, the assessment finds that the recommendations appropriately balance DNS Abuse mitigation with protection of registrant rights. The WG worked 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 Registered Name Holders.

GPI Checklist

The worksheet assesses the final Recommendations against the Global Public Interest (GPI) framework. It considers whether the final Recommendations advance objectives such as DNS

security and stability, benefit to the Internet community, and ICANN's technical coordination. The analysis concludes that the final Recommendations generally align with the GPI principles by strengthening DNS abuse mitigation while preserving operational flexibility for registrars and incorporating safeguards to avoid unnecessary burdens or overreach that could impact Registered Name Holders.

Data Privacy Considerations

The worksheet evaluates the final Recommendations from a data privacy perspective rather than providing a legal opinion. It examines whether Associated Domain Checks require processing of personal data, whether such processing is necessary and proportionate, any potential associated privacy risks, and the safeguards available and discussed to mitigate those risks. The assessment concludes that privacy risks are low because the recommendations limit investigations to reasonably accessible information, discourage creation of new data solely for ADC, and require compliance with applicable laws.

Consensus Policies

The worksheet reviews existing ICANN Consensus Policies to determine whether and how the DNS Abuse Mitigation PDP 1 final Recommendations would affect them. It catalogues current policies across areas such as registration data, transfers, expiration, registry services, and rights protection, and assesses the expected impact of the proposed recommendations. The overall conclusion is that the recommendations would have minimal to no impact on existing Consensus Policies, as they are expected to establish a new consensus policy governing Associated Domain Checks rather than substantially modifying existing policy obligations.

6. Conclusions and Next Steps

6.1. Consensus Designations

Below is the DNSAM PDP 1 Leadership Team's designation as to the level of consensus on each recommendation in this Final Report. These designations were made following the process as outlined in the message to the DNSAM PDP 1 WG mailing list on 13 November 2026, and in accordance with Section 3.6 – Standard Methodology for Making Decisions of the GNSO Working Group Guidelines. The consensus call closed on 23 November 2026, and an objection was received to Full Consensus by NCSG on Recommendation 7 and Implementation Guidance 7.1.[4] Furthermore, SSAC, ALAC and IPC shared comments and considerations for the record, while supporting the originally proposed designations of full consensus.[5] The full record of the comments received during the Consensus Call can be found here.

Final Recommendation # **Final Implementation Guidance #**	**Leadership Team's Designation**
DNSAM PDP 1	
Final Recommendation 1: Associated Domain Check (ADC) Trigger	Full Consensus
Final Implementation Guidance 1.1: ADC Trigger	Full Consensus
Final Recommendation 2: ADC Investigation	Full Consensus
Final Recommendation 3: Reasonable Investigation	Full Consensus
Final Implementation Guidance 3.1: Reasonable Investigation	Full Consensus
Final Recommendation 4: Determining Association	Full Consensus
Final Implementation Guidance 4.1: Determining Association	Full Consensus
Final Recommendation 5: Safeguards for ADC	Full Consensus
Final Implementation Guidance 5.1: Safeguards for ADC	Full Consensus
Final Recommendation 6: Timeline for ADC	Full Consensus
Final Implementation Guidance 6.1: Timeline for ADC	Full Consensus
Final Recommendation 7: Review of ADC Policy Outcomes and Enforceability	Consensus

[4] See the email list opening, closing and Working Group feedback of the consensus call here: https://lists.icann.org/hyperkitty/list/gnso-dnsabuse-pdp@icann.org/thread/64OCDQ44JXSII54HBF2X2DHB2VJUQXRZ/

[5] Ibid.

Final Implementation Guidance 7.1: Review of ADC Policy Outcomes and Enforceability	Consensus
Final Recommendation 8: Demonstrating Compliance	Full Consensus

6.2. Next Steps

The DNSAM PDP 1 Final Report will be considered by the GNSO Council to determine the next course of action. If the Final Report is approved by the GNSO Council, it will be forwarded to the ICANN Board of Directors for consideration and potential action in accordance with the ICANN Bylaws.

7. Approach Taken by the Working Group

7.1. Working Methodology

The DNSAM PDP 1 WG began its deliberations on 08 March 2026. It continued its work primarily through weekly conference calls lasting for 90 minutes, 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 final findings and/or conclusions to the broader ICANN community for discussion and feedback. During ICANN85, ICANN86, and ICANN87 the WG had four (4) working sessions per meeting. In addition, the WG organized ICANN86 and ICANN87 prep-week webinars. An Initial Report webinar was also hosted on 8 September 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 recommendation review document.

7.2. WG Membership and Attendance

The members and attendance of the DNSAM PDP 1 WG can be found below or on the wiki along with links to Statements of Interest (SOI). Individual meeting attendance records can also be found for each meeting, and the email archives can be found here. Below is a summary of the regular meetings held for the DNSAM PDP 1 WG:

Plenary Meetings

- 20 Plenary calls scheduled (9 were cancelled due to early delivery of report) for a total of 31 actual meeting hours

Leadership Meetings

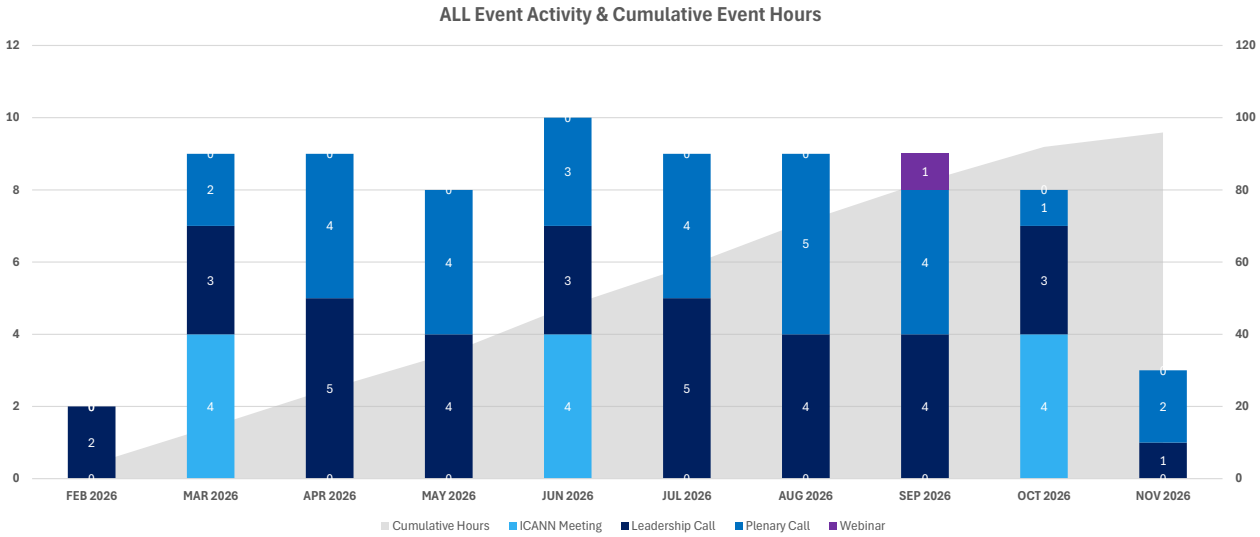
- 26 Leadership calls scheduled (8 were cancelled) for a total of 25.4 actual meeting hours

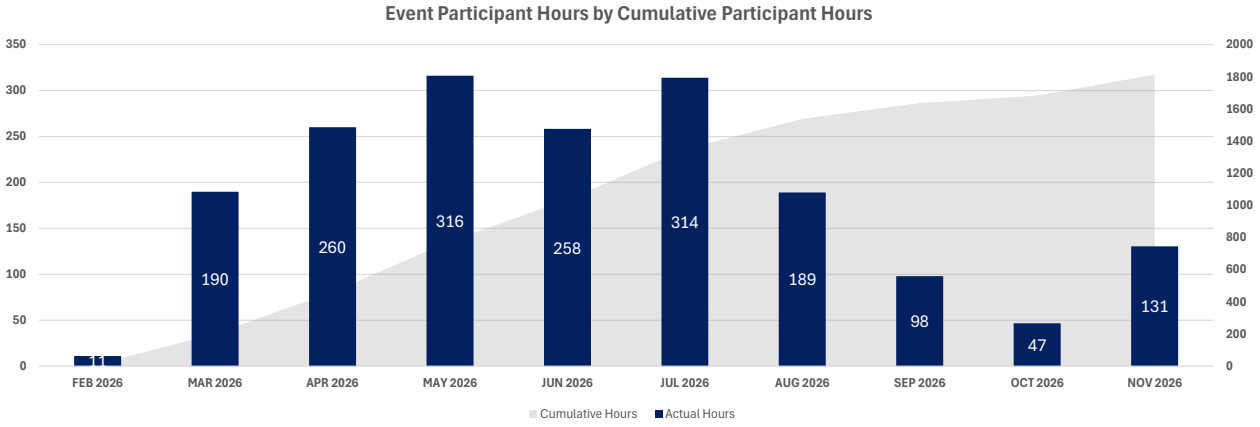
Overall Meeting Activities

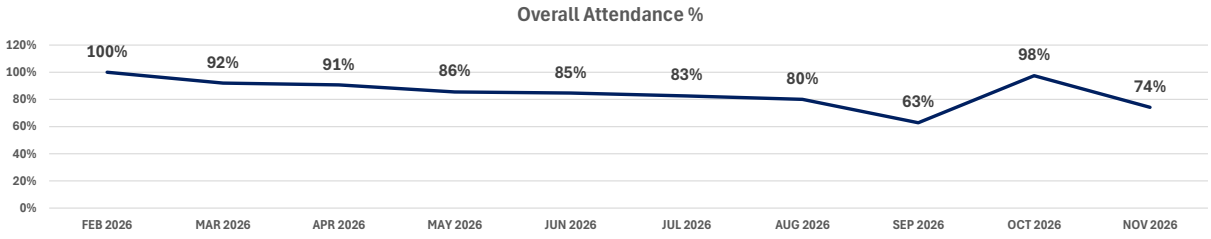
- 46 total virtual meetings scheduled (17 total were cancelled) for a total of 56.4 actual meeting hours and 1,715 participant meeting hours
- 85.0% attendance rate of all participants of the 46 plenary and leadership meetings
- 12 total face-to-face sessions for a total of 15 actual meeting hours across three ICANN Public Meetings (ICANN 85-87); attendance only taken of leadership and staff at ICANN

Meetings

- 1 Initial Report webinar with 156 registered and 98 actual attendees







Participant and Type	Registered	Attended	Percent	Role	SOI	Start Date	Depart Date
Member	**754**	**657**	**87%**				
At-Large Advisory Committee (ALAC)	**40**	**31**	**78%**				
Eunice Alejandra Perez Coello	2	2	100%		SOI	20.10.2026	
Kathleen Scoggin	18	13	72%		SOI	09.02.2026	20.10.2026
Steinar Grøtterød	20	16	80%		SOI	06.02.2026	
Commercial Business Users Constituency (BC)	**40**	**34**	**85%**				
Ching Chiao	20	17	85%		SOI	06.02.2026	
Luke Wood	20	17	85%		SOI	06.02.2026	
Country Code Names Supporting Organization (CCNSO)	**84**	**81**	**96%**				
Diego Luna	15	15	100%		SOI	27.04.2026	
Eberhard Lisse	20	19	95%		SOI	15.02.2026	
Nick Wenban-Smith	49	47	96%	Vice-Chair	SOI	17.02.2026	
GNSO Council	**114**	**106**	**93%**				
Jennifer Chung	57	53	93%	Liaison	SOI	10.02.2026	
Paul McGrady	57	53	93%	Chair	SOI	17.02.2026	
Governmental Advisory Committee (GAC)	**40**	**36**	**90%**				
Gabriel Andrews	20	18	90%		SOI	04.02.2026	
Martina Barbero	20	18	90%		SOI	28.01.2026	
ICANN Board	**18**	**14**	**78%**				
James Galvin	18	14	78%	Liaison	SOI	06.04.2026	
Intellectual Property Constituency (IPC)	**40**	**37**	**93%**				
Marc Trachtenberg	20	19	95%		SOI	10.02.2026	
Mary Penn	20	18	90%		SOI	07.02.2026	
Internet Corporation for Assigned Names & Numbers (ICANN)	**57**	**44**	**77%**				
Dennis Chang	17	14	82%	Liaison		08.04.2026	
Mukesh Chulani	20	14	70%	Liaison		07.03.2026	
Peter Eakin	20	16	80%	Liaison		07.03.2026	
Internet Service Providers and Connectivity Providers Constituency (ISPCP)	**40**	**34**	**85%**				
NITIN WALIA	20	18	90%		SOI	10.02.2026	
Thomas Rickert	20	16	80%		SOI	17.03.2026	
Non-Commercial Stakeholder Group (NCSG)	**40**	**32**	**80%**				
Farzaneh Badii	20	17	85%		SOI	11.02.2026	
Michaela Shapiro	20	15	75%		SOI	09.02.2026	
Non-Commercial Users Constituency (NCUC)	**40**	**34**	**85%**				
Bruna Martins dos Santos	20	14	70%		SOI	09.02.2026	
Juliana Harsianti	20	20	100%		SOI	09.02.2026	
Not-for-Profit Organizations Constituency (NPOC)	**41**	**35**	**85%**				
Farell Folly	21	17	81%		SOI	12.02.2026	
Yao Amevi A. Sossou	20	18	90%		SOI	09.02.2026	
Registrar Stakeholder Group (RrSG)	**80**	**71**	**89%**				
Carlos Becerra	20	20	100%		SOI	09.02.2026	
Eric Rokobauer	20	18	90%		SOI	09.02.2026	
Natalie Howatson	20	19	95%		SOI	09.02.2026	
Volker Greimann	20	14	70%		SOI	10.02.2026	
Registry Stakeholder Group (RySG)	**40**	**35**	**88%**				
Brian Cimbolic	20	18	90%		SOI	28.01.2026	
Dennis Tan	20	17	85%		SOI	28.01.2026	
Security and Stability Advisory Committee (SSAC)	**40**	**33**	**83%**				
Matthew Thomas	20	13	65%		SOI	09.02.2026	
Rod Rasmussen	20	20	100%		SOI	10.02.2026	
Grand Total	**754**	**657**	**87%**				

Participant and Type	Registered	Attended	Percent	Role	SOI	Start Date	Depart Date
Participant	**261**	**167**	**64%**				
At-Large Advisory Committee (ALAC)	**20**	**11**	**55%**				
Claire C. Craig	20	11	55%		SOI	06.02.2026	
Commercial Business Users Constituency (BC)	**21**	**16**	**76%**				
Lawrence OlaWale-Roberts	21	16	76%		SOI	06.02.2026	
Country Code Names Supporting Organization (CCNSO)	**20**	**14**	**70%**				
Diego Luna	5	5	100%		SOI	14.02.2026	27.04.2026
Mira Fajriyah	15	9	60%		SOI	30.04.2026	
Governmental Advisory Committee (GAC)	**20**	**10**	**50%**				
Emanuele Iovini	8	4	50%		SOI	06.07.2026	
Wolfgang Holzapfel	12	6	50%		SOI	17.02.2026	06.07.2026
Intellectual Property Constituency (IPC)	**20**	**12**	**60%**				
Hector Manoff	20	12	60%		SOI	10.02.2026	
Internet Service Providers and Connectivity Providers Constituency (ISPCP)	**20**	**14**	**70%**				
Anil Kumar Jain	20	14	70%		SOI	09.02.2026	
Non-Commercial Stakeholder Group (NCSG)	**20**	**17**	**85%**				
Benjamin Akinmoyeje	20	17	85%		SOI	09.02.2026	
Non-Commercial Users Constituency (NCUC)	**20**	**2**	**10%**				
John Gbadamosi	20	2	10%		SOI	10.02.2026	
Not-for-Profit Organizations Constituency (NPOC)	**20**	**16**	**80%**				
Godsway Kubi	20	16	80%		SOI	03.02.2026	
Registrar Stakeholder Group (RrSG)	**20**	**19**	**95%**				
Reg Levy	20	19	95%		SOI	09.02.2026	
Registry Stakeholder Group (RySG)	**20**	**7**	**35%**				
Neha Nair	20	7	35%		SOI	04.02.2026	
Root Server System Advisory Committee (RSSAC)	**20**	**14**	**70%**				
Erum Welling	20	14	70%		SOI	20.02.2026	
Security and Stability Advisory Committee (SSAC)	**20**	**15**	**75%**				
Jothan Frakes	20	15	75%		SOI	09.02.2026	
Grand Total	**261**	**167**	**64%**				

Participant and Type	Registered	Attended	Percent	Role	SOI	Start Date	Depart Date
Alternate	**137**	**134**	**98%**				
At-Large Advisory Committee (ALAC)	**19**	**18**	**95%**				
Eunice Alejandra Perez Coello	18	18	100%		SOI	07.02.2026	20.10.2026
Kathleen Scoggin	1	0	0%		SOI	20.10.2026	
Commercial Business Users Constituency (BC)	**10**	**10**	**100%**				
Vivek Goyal	10	10	100%		SOI	06.02.2026	
Country Code Names Supporting Organization (CCNSO)	**4**	**3**	**75%**				
Bruce Tonkin	4	3	75%		SOI	14.02.2026	
Governmental Advisory Committee (GAC)	**12**	**12**	**100%**				
Emanuele Iovini	1	1	100%		SOI	27.02.2026	06.07.2026
Janos Drienyovszki	4	4	100%		SOI	09.07.2026	
Naoum Mengoudis	7	7	100%		SOI	29.01.2026	26.06.2026
ICANN Board	**11**	**11**	**100%**				
Chris Buckridge	11	11	100%	Liaison	SOI	06.04.2026	
Intellectual Property Constituency (IPC)	**12**	**12**	**100%**				
David Hughes	12	12	100%		SOI	12.02.2026	
Internet Service Providers and Connectivity Providers Constituency (ISPCP)	**2**	**2**	**100%**				
Santanu Acharya	2	2	100%		SOI	07.02.2026	
Non-Commercial Stakeholder Group (NCSG)	**12**	**12**	**100%**				
EDMUND BRAHENE	12	12	100%		SOI	09.02.2026	
Non-Commercial Users Constituency (NCUC)	**3**	**3**	**100%**				
Emmanuel Elolo Agbenonwossi	3	3	100%		SOI	14.03.2026	
Not-for-Profit Organizations Constituency (NPOC)	**14**	**14**	**100%**				
Christabel Mebaghandu	14	14	100%		SOI	09.02.2026	
Registrar Stakeholder Group (RrSG)	**17**	**17**	**100%**				
Theo Geurts	17	17	100%		SOI	09.02.2026	
Registry Stakeholder Group (RySG)	**17**	**17**	**100%**				
Chris Disspain	17	17	100%		SOI	23.02.2026	
Security and Stability Advisory Committee (SSAC)	**4**	**3**	**75%**				
Gautam Akiwate	4	3	75%		SOI	09.02.2026	
Grand Total	**137**	**134**	**98%**				

Participant and Type	Registered	Attended	Percent	Role	SOI	Start Date	Depart Date
Staff - Assigned	**220**	**211**	**96%**				
Internet Corporation for Assigned Names & Numbers (ICANN)	**220**	**211**	**96%**				
Feodora Hamza	58	54	93%			16.01.2026	
John Emery	57	54	95%			16.01.2026	
Julia Bisland	19	19	100%			16.01.2026	
Steve Chan	56	54	96%			16.01.2026	
Terri Agnew	30	30	100%			16.01.2026	
Grand Total	**220**	**211**	**96%**				