10 November 2026

DNSAM PDP1 – Final Recommendations and Implementation Guidance as seen in the Final Report

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current, recent, intermittent, recurring, or otherwise well-evidenced DNS Abuse, including where the Registered Name is no longer active or the abusive activity has ceased.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 sup-port 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.

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]

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.

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.

---

[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
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

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

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.

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.

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.

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.

[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.