Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Comments on ICANN/GNSO Initial Report on the DNS Abuse Mitigation Policy Development Process 1

About M³AAWG

The Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) is the largest global industry organization focused on addressing online abuse across messaging, mobile, and infrastructure ecosystems. M³AAWG was founded in 2004 and brings together more than 200 member organizations spanning internet service providers, telecommunications carriers, cloud service providers, security vendors, and technology companies. Collectively, M³AAWG members handle the majority of the world's email, messaging, and voice traffic.

Domain names and the infrastructure that supports them are important components of the online abuse ecosystem and are increasing areas of focus for M³AAWG and its members. M³AAWG develops and promotes industry best practices for identifying, mitigating, and preventing domain name abuse, drawing on the operational experience of stakeholders across the domain name, hosting, security, and broader internet infrastructure communities. M³AAWG therefore views the ICANN ADC PDP as important and directly relevant to its work, particularly where its outcomes may affect the security and abuse implications of domain name registration and management.

M³AAWG submits this intervention from technical, privacy, and public policy perspectives.

Executive Summary

M³AAWG generally supports the DNSAM PDP 1 Working Group's preliminary recommendations[1] on Associated Domain Checks (ADCs), while suggesting some improvements. Requiring registrars to proactively investigate domains linked to confirmed DNS abuse actors addresses a long-standing operational gap that threat intelligence practitioners, abuse reporters, and infrastructure operators have

[1] Initial Report at: https://gnso.icann.org/sites/default/files/policy/2026/draft/dnsam-pdp-initial-report-18aug26-en.pdf

confronted for years: the one-domain-at-a-time approach that allows coordinated campaigns to persist while abuse reports are processed individually.

The eight preliminary recommendations and five implementation guidance items constitute a reasonable, well-balanced framework. The Working Group has threaded a difficult needle between establishing meaningful baseline obligations and preserving operational flexibility for a diverse registrar ecosystem. M[3]AAWG's comments focus on areas where the recommendations can be strengthened without expanding scope, where ambiguity risks undermining enforcement, and where the policy's interaction with real-world abuse reporting workflows deserves additional attention.

Our priority concerns are:

(1) the absence of any requirement for a registrar to conduct ADCs across the accreditations ("Affiliated Registrars") it owns, and
(2) the "promptly" standard for ADC timelines, which, without supplementary guidance such as worked examples or advisory scenarios, risks inconsistent application,
(3) the need for the policy effectiveness review (Recommendation 7) to incorporate reporter-side data and outcomes, not only registrar compliance data, and
(4) the importance of ensuring that the compromised-domain exclusion does not become a default justification for declining to conduct ADCs.

We offer these comments to strengthen the policy within its current scope and to flag matters that should inform future work.

Priority Responses to Recommendations

Preliminary Recommendation 1: ADC Trigger

M[3]AAWG agrees that tying the ADC trigger to the existing Section 3.18.2 standard of "actionable evidence" is sound. This avoids creating a separate evidentiary threshold while grounding the obligation in language already familiar to registrars and ICANN Compliance.

We support Implementation Guidance 1.1's clarification that "is being used for DNS Abuse" covers current, recent, intermittent, and recurring abuse, including cases where abusive activity has ceased. This is operationally critical. Threat actors routinely rotate domains in and out of active use, and campaigns often exhibit intermittent patterns designed to evade detection. A policy that applied only to abuse observable at the exact moment of review would be easy to circumvent and would miss the majority of real-world cases.

The exclusion of compromised domains from the ADC trigger is appropriate in principle: a compromised website should not cause every other domain under the same registrant's account to be investigated. However, M[3]AAWG notes that the distinction between "registered for the purpose of conducting DNS Abuse" and "compromised" can be ambiguous in practice, particularly early in an investigation. Registrars may not always be adept at determining whether a domain was registered with malicious intent or whether it is compromised. Some domains are registered legitimately, parked, and then sold or transferred to abusive actors. Others are registered through bulk-purchase accounts where some domains are used legitimately, and others are not. The WG should consider additional implementation guidance or worked examples that illustrate how registrars should approach borderline cases in order to prevent the compromised-domain exclusion from being used as a default reason to decline performing an ADC.

Preliminary Recommendations 2-4: ADC Investigation, Reasonable Investigation, and Determining Association

M[3]AAWG generally agrees with the framework across these three recommendations. The approach is practical: registrars investigate using information reasonably accessible to them. However, M[3]AAWG suggests that registrars ***must*** take into account and investigate credible information provided in complaints. The flexible, non-exhaustive set of association criteria (account identifiers, naming patterns, shared infrastructure, campaign characteristics) reflects how abuse investigations work.

We agree with the WG's rationale that no single data point should be determinative and that the policy should not prescribe a fixed investigation sequence. Registrars differ significantly in their technical capabilities, business models, and data environments. A prescriptive approach would either set the floor too low (rendering the obligation meaningless for sophisticated registrars) or too high (creating unachievable requirements for smaller operators) and may not account for changes in how risks present themselves.

Two points warrant emphasis. First, the draft states, "This policy only requires ADC within a registrar portfolio and does not require cross-registrar checks/coordination." This is a policy shortcoming when a company owns two or more registrar accreditations. M[3]AAWG recommends that a registrar ***must***[2]

[2] This is a ***must*** in the sense of RFC 2119. https://www.rfc-editor.org/info/rfc2119/

reasonably examine registrations at its "Affiliated Registrars"[3] and under their operational control when an ADC is triggered at one of those registrars.

Second, the role of external abuse reports deserves more attention. Recommendation 3 lists "abuse reports" as a category of reasonably accessible information, and the Rationale for Recommendation 1 confirms that external reporters can provide valid sources of actionable evidence. M[3]AAWG members are among the reporters of DNS Abuse to registrars. They observe significant variation in how registrars ingest, process, and act on these reports. The quality of an ADC is only as good as the information the registrar is willing to consider. The implementation guidance should affirm that a reasonable investigation includes giving genuine consideration to relevant external reports, including those that describe campaign-level patterns and identify potential associated domains.

Preliminary Recommendation 5: Safeguards for ADC Investigations

M[3]AAWG supports the principle that ADCs must comply with applicable data privacy laws and contractual requirements. We agree with the WG that privacy concerns in the ADC context primarily relate to personal data, not to technical checks such as reviewing nameserver configurations or DNS records. However, we are not aware of privacy laws that would prevent a registrar from checking its own registrant data to discover fraud or abuse. For example, GDPR specifically states that registrars have a lawful basis and legitimate interest for using registrant data for fraud prevention and checking compliance with contractual terms of service.[4] Checking whether multiple domains under the same account share nameservers, use similar hosting infrastructure, or exhibit coordinated registration patterns does not require accessing personal data. The implementation guidance should be clear that registrars should **not** use spurious claims of privacy protection to avoid performing relevant and useful ADC checks.

Preliminary Recommendation 6: Timeline for ADC

M[3]AAWG understands the WG's rationale for adopting a "promptly" standard rather than a fixed deadline. DNS abuse incidents vary in urgency, complexity, and evidentiary requirements, and a single universal deadline would be poorly calibrated for many cases.

---

[3] See paragraphs 1.3 and 1.4 of the ICANN Registrar Accreditation Agreement: 1.3 "Affiliate" is defined as "a person or entity that, directly or indirectly, through one or more intermediaries, Controls, is controlled by, or is under common control with, the person or entity specified." 1.4 "Affiliated Registrar" is "another Accredited registrar that is an Affiliate of Registrar."
https://itp.cdn.icann.org/en/files/accredited-registrars/registrar-accreditation-agreement-21jan24-en.pdf

[4] See for example GDPR Recital 47. https://gdpr-info.eu/recitals/no-47/

That said, "promptly" without additional interpretive guidance creates a compliance standard that is difficult to enforce and easy to satisfy nominally. The WG should develop supplementary implementation guidance, whether through worked examples, advisory scenarios, or tiered expectations linked to abuse severity, that gives both registrars and ICANN Contractual Compliance a shared understanding of what "prompt" looks like in common case types. Without this, the timeline requirement risks remaining encouraging rather than becoming operational.

When new DNS abuse amendments were added to ICANN's Registrar Accreditation Agreement in 2024, ICANN org itself created an Advisory that provided guidance to registrars and registry operators about how ICANN org and its Contractual Compliance department would interpret the new obligations.[5] It expanded on what ICANN org thinks is "prompt," what evidentiary standards ICANN org considers actionable, and included example scenarios. M^{3}AAWG recommends that the WG review that Advisory and develop additional Preliminary Implementation Guidance for recommendations, particularly where existing guidance lacks sufficient interpretive detail or illustrative scenarios, so that new requirements are defined in sufficient and additional detail, and so that ICANN org has clear guidance. While some interpretation will always be necessary on the part of ICANN org and its Contractual Compliance department, sufficiently detailed guidance should be provided via the policy-making process.

M^{3}AAWG also notes that the ADC timeline should not delay action on the triggering domain itself. The report already addresses this by clarifying that an ADC can be performed before, during, or after mitigation action on the triggering domain, but this point deserves emphasis in the Final Report.

Preliminary Recommendation 7: Measuring ADC Policy Effectiveness

M^{3}AAWG supports a review after one year, not two years. M^{3}AAWG echoes the WG's caution against relying solely on aggregate abuse-volume statistics to assess effectiveness. Direct causation between a single policy and overall abuse levels is difficult to establish, and the review should focus on operational indicators: whether ADCs are being conducted, whether they are effectively surfacing associated domains in the expected way, and whether those findings lead to proportionate action.

M^{3}AAWG believes that the data should not be limited to "information available to ICANN Contractual Compliance, ICANN's Office of the CTO (OCTO), and a limited set of aggregated

[5] "Advisory: Compliance With DNS Abuse Obligations in the Registrar Accreditation Agreement and the Registry Agreement" at https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en

information maintained by registrars in the ordinary course of business." We recommend that the review methodology ***must***[6] include reporter-side data in addition to registrar-side compliance data. We also recommend that the review include a public comment period. Organizations that submit abuse reports can provide valuable perspective on whether ADCs are producing observable changes in campaign disruption outcomes, whether report quality expectations have changed, and whether registrar responsiveness to campaign-level reports has improved. M^{3}AAWG and its members would be willing to contribute aggregated, privacy-preserving data to such a review.

We note ALAC's objection that the review should also assess unintended impacts on legitimate registrants, including erroneous associations and false positives. M^{3}AAWG agrees that tracking these outcomes is important and supports the inclusion of this dimension, provided it does not require new case-level reporting obligations on registrars.

Preliminary Recommendation 8: Demonstrating Compliance

We believe that the compliance demonstration framework is practical. Requiring registrars to maintain an internal process description and to document ADC triggers, investigations, findings, and actions, using records generated in the ordinary course of business, strikes an appropriate balance between auditability and operational burden.

M^{3}AAWG supports the requirement that internal ADC process descriptions be made available to ICANN upon request. This is an essential accountability mechanism. Without it, ICANN Contractual Compliance would have no practical way to assess whether a registrar's ADC process is reasonable or whether it was actually followed.

M^{3}AAWG also encourages ICANN to enhance transparency around the deployment of ADC and other DNS abuse mitigation measures. For example, where a set of domains is taken down as the result of an ADC, it may be valuable for the community to have visibility into the fact that an ADC formed the basis for the action and, where appropriate, to be able to determine which domains were considered associated.

[6] This is a **must** in the sense of RFC 2119. https://www.rfc-editor.org/info/rfc2119/

Cross-Cutting Observations

Report Quality and Reporter Responsibilities

The Initial Report places appropriate expectations on abuse reporters: reports should include sufficient information to support the alleged DNS Abuse, and where abuse is intermittent or recurring, the report should demonstrate the pattern. M[3]AAWG agrees with these expectations. High-quality, evidence-based reporting is essential for the ADC framework to function effectively. Reporters that submit unsubstantiated reports should not expect to trigger ADC obligations.

M[3]AAWG has published best practices on abuse reporting that align with the standards described in the Initial Report. We encourage the IRT, during the implementation phase, to consider developing or endorsing shared guidance on what constitutes a well-evidenced report for ADC purposes. This would benefit both registrars (by reducing the volume of reports that do not meet the actionable-evidence threshold) and reporters (by providing clarity on what information to include).

The Reseller Model

Implementation Guidance 3.1's treatment of resellers is important. Many abusive registrations occur through reseller channels, and registrars may have limited direct visibility into end-customer activity. The guidance correctly states that registrars may rely on resellers to conduct ADC investigation steps, while remaining fully responsible for all RAA obligations. The accountability of the registrar is critical and should not be diluted in the Final Report.

Conclusion

M[3]AAWG appreciates the opportunity to comment on the DNSAM PDP 1 Initial Report and acknowledges the considerable effort the Working Group has invested in producing a balanced, well-reasoned set of recommendations. The WG has moved quickly, from charter adoption in January 2026 to an Initial Report in August, while maintaining broad participation and achieving full or near-full consensus on every recommendation.

The core thread running through M[3]AAWG recommendations is this: the ADC framework represents a meaningful step forward, and its value depends on the specificity and enforceability of its implementation. Recommendations that are flexible enough to accommodate diverse registrar environments are also, by definition, flexible enough to satisfy without materially changing behavior. The implementation phase, including the work of the IRT and the development of supplementary

guidance, will determine whether the ADC obligation produces real operational change or becomes a compliance formality.

M[3]AAWG is committed to supporting work in this area and is prepared to provide technical expertise, member perspectives, and supplemental comments on any of the issues raised in this comments submission.

We appreciate the opportunity to submit feedback and welcome further engagement as needed to answer any questions during this process. Please address any inquiries to M[3]AAWG Executive Director Amy Cadagin at comments@m3aawg.org.

Sincerely,
Amy Cadagin
Executive Director

Messaging, Malware and Mobile Anti-Abuse Working Group (M[3]AAWG)
P.O. Box 9125, Brea, CA 92822, USA
www.m3aawg.org

Submitted: September 21, 2026