

The ICANN GNSO “Business Constituency”



ICANN Business Constituency (BC) Comment on [DNS Abuse Mitigation PDP 1 Initial Report](#) 28-Sep-2026

Preliminary Recommendation 1

Selection: [Support Recommendation as written](#)

Response: – The BC supports Preliminary Recommendation 1 as written. The actionable-evidence trigger, tied to Section 3.18.1 of the RAA, is the correct threshold: it avoids speculative or unsupported reports and 'weaponized' complaints, while ensuring that credible evidence initiates a broader investigation. This is consistent with the BC's Early Input of 20 March 2026, which recommended that the trigger be a registrar determination grounded in actionable evidence rather than the mere receipt of an abuse report.

Preliminary Implementation Guidance 1.1

Selection: [Support Implementation Guidance as written](#)

Response: –

Rationale on Preliminary Recommendation 1 and Preliminary Implementation Guidance 1.1

Selection: [Open-ended rationale comment](#)

Response:

The BC supports the rationale's focus on actionable evidence and its recognition that valid evidence may come from the registrar's own analysis or from external reporters. The rationale usefully confirms that an ADC can proceed before, in parallel with, or after mitigation of the triggering domain, and that the ADC trigger should not delay prompt mitigation under existing obligations. Together, these points serve the purpose the BC identified in its Early Input: closing the one-domain-at-a-time gap so that whole campaigns, not just individual domains, can be curtailed.

Preliminary Recommendation 2

Selection: [Support Recommendation as written](#)

Response: –

Preliminary Recommendation 3

Selection: [Support Recommendation as written](#)

Response: – The BC supports Preliminary Recommendation 3 as written. Anchoring a reasonable investigation to information reasonably accessible to the registrar in the normal course of its operations - through contractual obligations, technical systems, and abuse reports - establishes a workable baseline while respecting differences in registrar capabilities, systems, and business models. The BC particularly appreciates that the recommendation does not require registrars to generate new data or access information they do not lawfully or practically possess, consistent with the data-minimization principles in the BC's Early Input.

The BC also notes, consistent with its Early Input (Sections 2.4 and 9.2), that defining the investigation at the level of information categories rather than published detection thresholds or methods avoids handing malicious actors a blueprint for evasion, while remaining auditable under Preliminary Recommendation 8.

Preliminary Implementation Guidance 3.1

Selection: [Support Implementation Guidance as written](#)

Response: –

Preliminary Recommendation 4

Selection: [Support Recommendation as written](#)

Response: –

Preliminary Implementation Guidance 4.1

Selection: [Support Implementation Guidance as written](#)

Response: – The BC supports Implementation Guidance 4.1 as written. The non-exhaustive indicator list - common accounts and connection points, coordinated-activity patterns such as naming conventions and shared infrastructure, and information derived from internal analysis or external reports - covers the association signals that matter in modern campaigns while leaving room for evolving techniques. Treating the list as illustrative rather than exhaustive also avoids publishing a fixed detection blueprint that malicious actors could engineer around.

Rationale on Preliminary Recommendations

Selection: [Open-ended rationale comment](#)

Response:

The BC agrees with the rationale's approach: evidence-driven, proportionate ADCs; no prescribed exhaustive sequence of steps; no portfolio-wide reviews as a matter of course; and room for a broader review where the evidence indicates a larger coordinated campaign. The express statement that no single data point is determinative, together with proportionality tailored to the nature, scope, and severity of the reported abuse, protects legitimate portfolio registrants - corporate domain management, brand protection, marketing portfolios, and defensive registrations - a concern the BC emphasized in its Early Input (Section 5.3).

The BC notes the rationale's confirmation that this policy requires ADCs only within a registrar's portfolio. The BC offers a forward-looking observation on cross-registrar campaigns under Other Comments, without qualifying its support for the recommendations.

Preliminary Recommendation 5

Selection: [Support Recommendation as written](#)

Response: –

Preliminary Implementation Guidance 5.1

Selection: [Support Implementation Guidance as written](#)

Response: –

Rationale on Preliminary Recommendation 5 and Preliminary Implementation Guidance 5.1

Selection: [Open-ended rationale comment](#)

Response:

The BC agrees with the rationale that existing registrar contracts and applicable laws provide the core safeguards, and that the policy should not create a separate retention regime beyond existing legal and contractual requirements. The BC also finds helpful the clarification that privacy concerns relate to personal data rather than technical checks such as nameserver review: many ADC steps rely on non-personal or low-risk technical indicators, and the policy rightly does not discourage them. Privacy proportionality operates here as a balancing exercise - preventing unnecessary processing while permitting lawful, targeted use of information needed to stop or disrupt DNS Abuse.

Preliminary Recommendation 6

Selection: [Other](#)

Response:

The BC supports Preliminary Recommendation 6 as written and records one reservation for the Working Group's awareness.

The BC's reservation is this: in its Early Input (Sections 3 and 8), the BC recommended objective, time-bound expectations for initiating ADCs, because timeliness will largely determine whether the policy disrupts campaigns in practice rather than documenting them after the fact. The BC accepts the WG's consensus judgment on 'promptly' and does not propose a wording change. The BC's support rests on the expectation that: (1) registrars will document the timing of trigger, initiation, and completion in the ordinary course under Preliminary Recommendation 8; (2) the IRT will consider developing illustrative, non-binding guidance or examples supporting consistent interpretation of 'prompt' action across urgent, ordinary, and complex scenarios, as the rationale itself contemplates; and (3) initiation and completion timeliness will be among the matters examined in the two-year review under Preliminary Recommendation 7.

The BC stands ready to work with registrars, ICANN org, and the broader ICANN community, including through the Implementation Review Team and the two-year review, to monitor and strengthen the effectiveness of the ADC policy over time.

Preliminary Implementation Guidance 6.1

Selection: [Support Implementation Guidance as written](#)

Response: –

Rationale on Preliminary Recommendation 6 and Preliminary Implementation Guidance 6.1

Selection: [Open-ended rationale comment](#)

Response:

The BC offers the following neutral observations on the timing rationale. There are legitimate considerations on both sides of the fixed-deadline question. In favor of fixed deadlines: DNS Abuse campaigns often cause harm within hours; objective expectations are easier to assess and enforce; and clear timelines give reporters and affected businesses predictability. In favor of the contextual standard the WG adopted: incident variability is real; alignment with the existing RAA 'promptly' standard avoids inconsistent obligations across Section 3.18 duties; a deadline calibrated for simple cases could force premature conclusions in complex ones, increasing false-positive and collateral-impact risk; and a deadline calibrated for complex cases could normalize delay in urgent ones.

The WG weighed these considerations and most of the group converged on aligning with current RAA obligations rather than creating ADC-specific timeline rules. The BC accepts that judgment. The rationale's reference to possible implementation guidance, examples, advisories, or best practices to support consistent interpretation of 'prompt' action is, in the BC's view, the appropriate channel for further work, and the BC encourages the IRT to pursue it. The two-year review provides the community with an evidence-based opportunity to revisit timing if experience shows that the contextual standard is not producing timely campaign disruption. The BC is committed to contributing constructively to that work alongside registrars and other community stakeholders.

Preliminary Recommendation 7

Selection: [Support Recommendation as written](#)

Response: –

Rationale on Preliminary Recommendation 7

Selection: [Open-ended rationale comment](#)

Response:

The BC supports Preliminary Recommendation 7 as written. A two-year effectiveness review, measured against the policy's stated purposes - a consistent minimum baseline across registrars, enforceability by ICANN

Contractual Compliance, and contribution to the timely identification and disruption of DNS Abuse campaigns - is essential to ensure the policy delivers practical outcomes and not only process standardization.

The BC welcomes the direction in which ICANN org should work with the IRT to identify a limited set of aggregated data points, derived to the extent feasible from information already available to ICANN Contractual Compliance, OCTO, and registrars in the ordinary course of business. When the IRT takes up that work, the BC would find value in indicators covering, in aggregated and privacy-preserving form, both effectiveness (for example, time from trigger to initiation and completion, associated domains identified and mitigated, and evidence of campaign disruption) and fairness (for example, erroneous associations identified and corrected), consistent with the metrics the BC outlined in its Early Input (Section 10).

The BC stands ready to work with registrars, ICANN org, and the broader ICANN community on this effort, including by contributing business and abuse-reporter perspectives to the IRT's identification of data points, the establishment of baseline data, and the two-year review itself. Monitoring and strengthening the effectiveness of the ADC policy is a shared interest of the entire community, and the BC is committed to constructive participation throughout.

Preliminary Recommendation 8

Selection: [Support Recommendation as written](#)

Response: –

Rationale on Preliminary Recommendation 8

Selection: [Open-ended rationale comment](#)

Response:

The BC agrees with the rationale's balance: documentation sufficient for verification and audit, generated in the ordinary course of business, without unnecessary operational burdens or unnecessary collection of Registered Name Holder data. The connection drawn between Recommendations 5 and 8 - avoiding new data creation solely for ADC purposes while still enabling registrars to demonstrate compliance - is sound, and the documentation framework will also supply much of the aggregated information needed for the two-year effectiveness review under Recommendation 7.

Comments on Comprehensive Impact Assessments

Selection: [Open-ended impact-assessment comment](#)

Response:

The BC agrees with the conclusions of the comprehensive impact assessments: the recommendations can be implemented consistently with human rights, data protection principles, the global public interest, and existing ICANN Consensus Policies. The actionable-evidence trigger, the limitation to reasonably accessible information, and the emphasis on proportionality are important protections, and they mirror the necessity, proportionality, and legitimacy principles in the BC's Early Input (Section 12).

The BC also observes that effective, timely ADCs are themselves protective of rights and the global public interest: under-enforcement or delayed action allows phishing losses, malware distribution, botnet activity,

impersonation, and consumer deception to continue harming users and legitimate businesses. The BC appreciates that the assessments and the recommendations, read together, balance both sides of that ledger.

Other Comments on the Initial Report

Selection: [Open-ended other comment](#)

Response:

The BC supports the Initial Report as written and offers the following constructive, forward-looking suggestions for the Working Group, the IRT, and future community work.

1. Partnership on effectiveness. The BC reiterates its willingness to work with registrars, ICANN org, and the broader ICANN community - through implementation, the IRT, and the two-year review - to monitor and strengthen the effectiveness of the ADC policy. The BC and its members can contribute business, brand-protection, and abuse-reporter perspectives, and practical experience of how campaigns affect businesses and consumers.
2. Registrant recourse (Charter Question 5). As implementation proceeds, the BC encourages the community to consider guidance on how legitimate Registered Name Holders adversely affected by an erroneous association can seek review and restoration in a timely, good-faith manner, consistent with the BC's Early Input (Section 7). Many registrars already operate such channels; sharing good practices through the IRT or community best-practice work would reinforce the proportionality safeguards in Implementation Guidance 5.1 without adding new policy obligations.
3. Future work on cross-registrar intelligence. PDP 1 is appropriately limited to checks within a registrar's portfolio, but DNS Abuse campaigns often span multiple registrars, registries, resellers, hosting providers, and infrastructure services. The BC encourages the community to identify, as future work, trusted, proportionate, and legally compliant mechanisms for sharing campaign indicators across relevant actors.
4. Abuse reporting mechanisms. As a practical matter, online abuse reporting mechanisms that allow submission of multiple related domains and supporting indicators in a single report would support the campaign-level purpose of ADCs and improve the quality of the actionable evidence available to registrars.
5. Standardized reporting formats. The BC further suggests that standardized, machine-readable reporting formats — for both abuse reports submitted to registrars and the documentation registrars maintain under Recommendation 8 — would materially assist automated validation of, and adherence to, the ADC policy. The BC encourages the IRT to consider developing such formats as part of its implementation work, in consultation with registrars and reporters.
6. Implementation timeline and compliance verification. The BC notes that the Initial Report does not specify a timeline for registrars to implement the ADC policy following its adoption, nor a cadence for ICANN Contractual Compliance to verify that implementation. This is a distinct question from the per-incident "promptly" standard addressed in Preliminary Recommendation 6, where the BC accepted the WG's rationale for a contextual rather than fixed standard given incident-level variability. Rollout of the ADC capability itself, however, is a one-time organizational undertaking better suited to an objective timeframe. The BC encourages the IRT, as part of its implementation work under Recommendations 7 and 8, to consider: (1) a defined implementation window (for illustration, on the order of four months) following the policy's entry into force; and (2) a risk-based verification cadence — for example, an initial compliance check within the first year post-implementation, with subsequent checks roughly annually, adjusted more or less frequently according to a registrar's demonstrated

compliance history. The BC believes such an approach would complement, rather than duplicate, the aggregated data points and effectiveness metrics the BC has already encouraged the IRT to develop under Recommendation 7, and would give ICANN Contractual Compliance an objective basis for enforcement consistent with the purposes of that Recommendation.

Summary of Submission

Selection: [Required summary - 2,000 character maximum](#)

Response:

The Business Constituency supports the DNS Abuse Mitigation PDP 1 Initial Report and its eight Preliminary Recommendations and five Implementation Guidances as written. The BC provided Early Input on 20 March 2026 and has participated actively in the Working Group; it is pleased that the preliminary recommendations reflect the core positions the BC advanced, including an actionable-evidence trigger, an evidence-based exclusion for compromised domains, a reasonable and proportionate investigation standard, flexible but meaningful association criteria, privacy safeguards balanced against effective mitigation, auditable documentation, and a two-year effectiveness review. Moving beyond one-domain-at-a-time response is necessary to identify and disrupt coordinated DNS Abuse campaigns, and this policy is a meaningful step in that direction.

On Preliminary Recommendation 6, the BC supports the use of the contextual "promptly" standard, with a reservation. The BC's Early Input favored objective, time-bound expectations for initiating ADCs, and the BC continues to believe that timeliness will largely determine whether the policy disrupts campaigns in practice. The BC accepts the WG's judgment that a single universal deadline would be over- or under-inclusive and that alignment with existing RAA obligations avoids dual timing standards. The BC's support rests on the expectation that timing will be documented under Recommendation 8, that the IRT will consider illustrative guidance for urgent, ordinary, and complex cases, and that initiation and completion timeliness will be examined in the two-year review.

The BC stands ready to work with registrars, ICANN org, and the broader community through implementation and review to monitor and strengthen the effectiveness of the ADC policy, and offers constructive suggestions for future work in its comments.