ICANN Business Constituency (BC) Input on DNS Abuse Mitigation PDP 1

(Associated Domain Checks)

20-Mar-2026

1. Executive Summary

The Business Constituency (BC) supports the initiation of DNS Abuse Mitigation PDP 1 focused on Associated Domain Checks, and appreciates the opportunity to provide the following early inputs.

At the high level, the BC supports the creation of a consensus policy requiring registrars to conduct targeted associated domain checks following confirmation of DNS Abuse on a "seed" domain, provided the policy is:

- narrowly scoped and enforceable,
- mandatory time-bound action,
- adaptable across registrar business models,
- consistent with privacy and data protection frameworks, and
- balanced by procedural safeguards and registrant recourse mechanisms.

2. General Principles and Policy Objectives

The BC recommends that the Working Group align its policy development with the following principles:

2.1 Objective: Disrupt Abuse Campaigns at Scale

The objective of an associated domain check policy should be to reduce DNS Abuse uptime and prevent repeated harm by enabling registrars to identify and mitigate clusters of related abusive domains, not merely individual domains.

2.2 Evidence-Based and Proportionate Action

Associated domain checks must be grounded in actionable evidence and designed to minimize collateral impact on legitimate registrants, including businesses operating legitimate domain portfolios.

2.3 Flexible Implementation; Consistent Minimum Obligations

The BC supports establishing enforceable minimum obligations while allowing flexibility for registrars to implement these obligations in ways that reflect operational realities, differing business models, and evolving threat techniques.

2.4 Avoid Creating a "Blueprint" for Malicious Actors

The BC strongly recommends that policy requirements avoid overly prescriptive technical specifications or published detection thresholds that could be exploited by malicious actors to evade detection.

3. Charter Question 1: What triggers the requirement to investigate associated domain names?

The BC recommends that the trigger for an associated domain check be a confirmed DNS Abuse determination—supported by actionable evidence and a good-faith assessment by the registrar—not merely the receipt of an abuse report. This distinction is essential to ensure the policy is both effective against real campaigns and resilient against false positives, spammy reporting, or malicious "weaponized" complaints. In practice, a raw report can be incomplete, incorrect, or unverifiable; by contrast, a confirmation threshold aligns the obligation with operational reality and reduces the risk of disproportionate impact on legitimate registrants.

The BC further notes that real-world abuse identification often unfolds over time, and policy should support multiple reasonable scenarios for initiating the associated domain check:

- **Scenario A — "Seed first, cluster later" (Time-Bound Pivot):** A registrar receives a DNS abuse report containing actionable evidence (for example, a phishing domain hosting an active credential-harvesting page). Upon confirming that the domain is engaged in DNS abuse as defined in the RAA, the registrar must initiate mitigation action on the abusive domain and begin an associated domain check **within twenty-four (24) hours of receiving the report**.This is the most common operational model: a single confirmed abuse event triggers a broader portfolio review (refer to Section 4) to disrupt the campaign rather than playing "whack-a-mole."
- **Scenario B — "Cluster first, confirmation later" (Time-Bound Cluster Activation):** A registrar identifies a suspicious cluster of domains exhibiting coordinated indicators of abuse (for example, bulk registrations sharing identical registrant handles, repeated infrastructure patterns, or automated string generation behavior). At this stage, suspicion alone does not trigger enforcement action. However, once any single domain within that cluster is confirmed to be engaged in DNS abuse, the confirmation shall activate a time-bound associated domain review obligation.This preserves proportionality: the check becomes mandatory only when suspicion is anchored to verified abuse.
- **Scenario C — "Confirmed abuse emerges after time" (Slow-Burn Campaigns):** A registrant portfolio may appear benign at registration time, but abuse appears days or

weeks later (refer to section 8.3 for further explanation). Under this scenario, once a domain is confirmed abusive, the associated domain check should apply not only to domains registered in the same moment, but also to associated domains registered within an extensive lookback period, recognizing that campaigns may be staggered to evade detection.

- **Scenario D — "Third-party intelligence + registrar confirmation" (Trusted-Signals Action):** In some cases, credible third-party intelligence (e.g., law enforcement referrals, CERT notifications, or high-quality OSINT or commercial datafeeds) may identify a likely campaign and provide strong indicators. Even then, the BC recommends the trigger remain the registrar's confirmation of DNS abuse on at least one domain—after validating the evidence to a reasonable standard—before initiating broader associated domain checks. This approach supports rapid response without outsourcing enforcement decisions to external parties.

3.1 Recommended Trigger Standard

The BC recommends the following policy trigger:

> A registrar shall initiate an associated domain check when it has determined, based on actionable evidence, that a domain name under its sponsorship is engaged in DNS Abuse as defined in the RAA.

This approach ensures the trigger is operationally practical, aligned with the Charter scope, and resistant to misuse through false or malicious reporting.

3.2 Exclusion of Compromised Domains

The BC emphasizes that the trigger must explicitly exclude compromised domains, consistent with the Charter's scope. A compromised domain does not necessarily indicate malicious registration intent or a malicious registrant portfolio.

3.3 Optional Risk-Based Prioritization

Registrars should be permitted (but not required) to apply risk-based prioritization signals in determining urgency and scope of review, such as:

- bulk registration behavior,
- API-enabled registration patterns,
- suspicious payment patterns,
- known repeat abuse patterns.

However, these signals should not replace the core evidentiary threshold required to trigger an associated domain check.

4. Charter Question 2: What criteria should be used to define “association” between domains?

The BC recommends a tiered framework distinguishing between required association criteria and optional supporting correlation signals, ensuring enforceability while avoiding overreach.

4.1 Tier 1 (Required Association Criteria)

The BC recommends that policy require registrars to support association checks based on at least one of the following elements (as applicable):

- customer account identifier (where registrar maintains account-level relationships), and/or
- registrant email address or comparable registrant contact handle (where reseller layers exist), and/or
- transaction/order identifier where relevant and available.
- Same payment method - credit card number, UPI ID, stripe account etc.

Tier 1 elements are generally accessible to registrars and provide a direct link to the registrant or purchasing entity, making them practical for compliance.

4.2 Tier 2 (Permitted Supporting Signals)

Registrars should be permitted to use any and all signals that are available to them to identify likely campaign relationships, such as:

- shared payment instruments,
- shared infrastructure patterns (nameservers, hosting providers, IP ranges),
- shared domain string patterns indicative of automation (DGA, or Domain Generation Algorithm),
- repeat use of known abusive technical configurations,
- account access anomalies.

The BC recommends that Tier 2 signals be treated as supporting evidence to prioritize review, rather than as sole justification for enforcement action.

These are suggestions based on our experience, we believe the registrars should use any and all signals that are at their disposal to make an associate domain check.

5. Charter Question 3: What constitutes a “reasonable investigation” by a registrar?

The BC recommends defining “reasonable investigation” as a proportionate pivot process designed to identify related domains likely involved in the same malicious campaign.

5.1 Minimum Investigation Requirements

A reasonable investigation should include:

1. identification of associated domains using Tier 1 association criteria;
2. screening associated domains for relevant DNS abuse indicators; and
3. escalation for deeper review where indicators suggest coordinated abuse.

5.2 Proportionate and Risk-Based Approach

The BC recommends that the ADC investigation should be proportionate and prioritize domains that exhibit:

- similar abuse characteristics to the seed domain, or
- shared infrastructure signals consistent with campaign behavior.

5.3 Avoiding Harm to Legitimate Portfolio Registrants

The BC emphasizes that bulk domain ownership is common among legitimate registrants, including:

- corporate domain management,
- brand protection,
- marketing portfolios,
- defensive registrations.

The policy must therefore focus on evidence of abusive activity, not merely on the existence of multiple domains.

6. Charter Question 4: What data access and privacy safeguards are necessary?

The BC supports safeguards that ensure associated domain checks remain narrowly targeted and consistent with applicable privacy and data protection principles.

6.1 Data Minimization

Associated domain checks should rely on data already held by the registrar as part of normal business operations. The policy should not require the publication of registrant portfolio data.

6.2 Internal Use and Confidentiality

The BC recommends that associated domain checks be conducted internally, and that any reporting to ICANN Compliance should be structured to avoid unnecessary disclosure of personally identifiable information (PII).

6.3 Targeted Investigation Requirement

The BC recommends that policy explicitly clarify:

> Associated domain checks are triggered only by confirmed DNS abuse and are not intended to create a generalized monitoring or profiling requirement for registrars.

6.4 DPIA and Documentation Considerations

The BC supports considering Data Protection Impact Assessment (DPIA) practices where appropriate, particularly where large-scale portfolio actions are taken, to ensure that privacy impacts are identified and mitigated.

7. Charter Question 5: If associated domain checks have adverse impact on registrants, are remedies needed?

Yes. The BC strongly supports requiring registrars to maintain a registrant recourse mechanism to prevent undue harm from false positives and to support procedural fairness.

7.1 Minimum Recourse Requirements

Registrars should be required to provide:

- a publicly available dispute/recourse mechanism (webform or email channel),
- the ability for registrants to submit evidence, and
- a good-faith review and recovery process.

7.2 Timeliness

The BC recommends that registrars review and recovery requests in a timely manner, especially where domain suspension disrupts legitimate business operations.

7.3 Scope

This recourse mechanism should not be designed as an endless appeal system. It should provide a reasonable opportunity for legitimate registrants to contest actions taken in error or demonstrate that abuse has been mitigated.

8. Charter Question 6: What are appropriate timelines and thresholds?

The BC recommends timelines that are urgent but operationally realistic across registrar environments.

8.1 Initiation

Associated domain checks should be initiated promptly after confirmation of DNS abuse.

8.2 Completion

The BC strongly recommends that the policy incorporates the mandatory 24-hour completion requirements. In some cases, the policy should require completion within a timeframe of 6, 12 hours based on:

- size of associated portfolio,
- nature of the abuse (phishing vs. malware vs. botnet infrastructure),
- availability of evidence,
- urgency of harm.

8.3 Time Dimension

The BC observes that malicious campaigns may involve domain clusters registered in rapid bursts within minutes, or distributed gradually over days, weeks, or months. Accordingly, the BC recommends that the WG ensure that associated domain check obligations are not limited to single-batch registrations, but include a reasonable lookback period and the ability to detect slower campaign patterns. The BC recommends that the policy support a rolling review approach whereby confirmed DNS abuse triggers both an initial pivot investigation and a defined period of heightened scrutiny for additional registrations associated with the same registrant or account.

9. Charter Question 7: What requirements should be mandatory policy vs best practices?

The BC recommends distinguishing between enforceable minimum obligations and discretionary implementation details.

9.1 Mandatory Policy Requirements

The Consensus Policy should require:

1. obligation to initiate associated domain checks following confirmation of DNS abuse;
2. minimum Tier 1 association criteria;
3. minimum investigation steps (pivot + screening);
4. mitigation requirements;
5. maintenance of a registrant recourse mechanism;
6. documentation and recordkeeping obligations.

9.2 Best Practices / Discretionary Implementation

The BC recommends that the following remain within registrar discretion and best practices:

- automated scoring and prioritization systems,
- exact correlation thresholds,
- tooling and detection methodologies,
- internal abuse of intelligence frameworks.

This approach improves adaptability and avoids creating a published blueprint for malicious actors.

10. Charter Question 8: What metrics will be used to evaluate policy effectiveness?

The BC recommends outcome-based metrics that measure campaign disruption and systemic abuse reduction, including:

10.1 Effectiveness Metrics

- average reduction in abuse uptime,
- number of associated domains mitigated per confirmed seed domain,
- percentage of confirmed seed domains that resulted in associated domain checks,
- recurrence rate of DNS abuse associated with the same registrant/account,
- time-to-mitigation for associated domains.

10.2 Fairness and Error Metrics

- rate of successful recourse requests (as a proxy for false positives),
- average time-to-restoration for legitimate registrants impacted in error.

10.3 Practical Considerations

Metrics collection should avoid requiring publication of sensitive portfolio or PII information. Reporting should be aggregated and anonymized wherever feasible.

11. Charter Question 9: How can registrars demonstrate compliance and what evidence is appropriate?

The BC recommends that compliance focus on procedural evidence, rather than requiring registrars to disclose sensitive registrant portfolio details.

11.1 Recommended Compliance Evidence

Registrars should demonstrate compliance through:

- timestamped logs showing associated domain check initiation and completion,
- documentation of investigation steps taken,
- evidence of mitigation action when abuse is confirmed,
- confirmation of an accessible recourse channel,
- anonymized summary statistics for compliance review.

11.2 Avoid “Disproving a Negative”

The BC notes concerns raised in community discussions that registrars should not be required to prove the absence of abuse across an entire portfolio.

The policy should clarify that compliance requires:

- a reasonable investigation process, and
- documented execution of that process in good faith.

Registrars acting in good faith under documented procedures should not face enforcement simply because future abuse is later discovered that was not identifiable at the time of investigation.

12. Human Rights Considerations

The BC recognizes that associated domain checks may create concerns regarding privacy, profiling, and unintended suppression of lawful activity. Accordingly, the BC supports safeguards to ensure that policy actions are:

- necessary to achieve the legitimate goal of reducing DNS abuse,
- proportionate to the harm being mitigated,
- legitimate within ICANN’s mission and contractual scope.

The BC recommends that the Working Group explicitly incorporate:

- data minimization principles,
- procedural transparency, and
- registrant recourse mechanisms

as core safeguards to reduce unintended negative impact.

13. Global Public Interest Considerations

The BC believes that reducing DNS abuse is directly aligned with the Global Public Interest, as DNS abuse causes widespread harm to consumers, businesses, and public institutions, including through phishing, credential theft, malware distribution, and botnet infrastructure.

A well-designed associated domain check policy can:

- reduce systemic harm to Internet users,
- increase trust in the DNS,
- reduce fraud costs for businesses and consumers,
- improve stability and resilience of the Internet ecosystem.

However, achieving these outcomes requires balancing security improvements with due process safeguards to avoid unjustified disruption of legitimate registrants and lawful business activity.

14. Conclusion

The BC supports PDP 1 as a targeted and practical policy effort to reduce DNS abuse at scale. The BC recommends that the Working Group adopt an evidence-based, enforceable, and commercially reasonable approach that:

- triggers associated domain checks only after confirmed DNS Abuse,
- defines association through minimum Tier 1 criteria with optional Tier 2 signals,
- requires proportionate investigation steps,
- includes registrant recourse mechanisms,
- establishes practical compliance and metrics requirements, and
- avoids overly prescriptive technical mandates that could be exploited by attackers.

This comment was drafted by the ICANN Business Constituency (BC). It was approved in accordance with our Charter.