DNS AXE's comment on:
Preliminary Issue Report on DNS Abuse Mitigation

Date: 18 October, 2025

Drafters:

- Mark W. Datysgeld (DNS AXE, Governance Primer, ICANNWiki)
- Ron Andruff (DNS AXE, IGSherpa, ONR Consulting)

Position

Support initiation of a PDP focused on (1) Unrestricted API access for high-volume registrations; (2) associated-domain checks; while (3) handling DGA/botnet coordination on a parallel, non-PDP track for speed and operational flexibility.

Continuity and context

The report builds on the community's post-amendment posture: April 2024 RA/RAA changes raised the floor, but left discrete mitigation gaps that are appropriate for uniform policy. The staff framing and scope support a tightly-scoped PDP with measurable outcomes.

1. Unrestricted API access (Support)

We support a consensus policy that introduces activity-based friction before new or untrusted customers receive programmatic/bulk-registration capability. That risk-based gating directly targets the automation and marginal-cost dynamics that amplify abuse, while preserving legitimate high-volume use.

Asks for the Charter:

- Require registrars to document thresholds and publish summaries that can be understood by non-technical audiences, making clear the logic being followed by the ICANN community.
- Explicitly cover wholesale/reseller flows so controls remain enforceable when all traffic is API-based.

2. Associated-domain checks (Strong support)

We **strongly support** a uniform obligation for registrars to pivot from a confirmed abusive domain to associated domains within the same account or tightly-linked identifiers (e.g., registrant email, payment instrument), with proportionality and auditability. This effectively shifts response from single-label takedowns to campaign-level disruption.

Asks for the Charter:

- Define "association" minimally and testably: account ID where available; otherwise registrant email plus one corroborant (e.g., payment fingerprint, cluster correlation, or repeated abuse reports).
- Set a reasonable look-back window, require documented steps, and mandate cooperation pathways for reseller contexts where account-level signals are opaque.

3. DGA/botnet coordination (Support outside-PDP track)

We agree with handling DGA list distribution and cross-TLD action coordination outside a PDP so it can be stood up faster (especially in relation to standardized evidence intake).

Additionally: Scoping guardrails

- To avoid overreach and false positives, keep policy language technology-neutral; avoid hard-coding detection algorithms.
- For both topics, separate consensus-policy obligations from recommended practices in the charter text (the report itself prompts this split).

Conclusion

A two-topic PDP, with DGA work proceeding in parallel via implementation channels, matches the report's own prioritization and offers the best blend of consensus viability, operator feasibility, and abuse-reduction at scale.