ICANN84 DNS Abuse Session Agenda (90 minutes)

Agenda

a) *Welcome (5min)*

b) *Issue 1 -- Unrestricted API Access for High-Volume Registrations (30min)*

Problem statement: Ungated/batch/API tools can enable rapid, large-scale malicious registrations; some registrars already apply friction; others do not.
Supporting Research: This gap was noted as high priority for a consensus policy by the 2025 DNS Abuse Small Team. Studies (e.g., INFERMAL) observed a strong association between unrestricted APIs and higher malicious registrations.
Questions for discussion:

- Minimum safeguards before granting API/batch access to *new* accounts (e.g., waiting periods, clean transaction history, abuse checks)?
- Revocation triggers and reinstatement conditions for existing customers after confirmed malicious registrations.
- Retail vs wholesale distinctions: where API use is the norm (wholesale), what's proportionate and feasible?

c) *Issue 2 -- Associated-Domain Checks (30min)*

Problem statement: Malicious campaigns often use portfolios of related domains; today there is no uniform duty to pivot from a confirmed malicious domain to potential associates.
Supporting Research: This gap was noted as high priority for a consensus policy by the 2025 DNS Abuse Small Team. The Netbeacon White Paper proposes for a PDP to examine whether registrars, upon obtaining actionable evidence that a domain name is used for DNS Abuse, should be required to review other domain names within the same account and/or registered by the same registrant.
Questions for discussion:

- Whether registrars should be required to investigate "associated" domains once one domain is confirmed malicious?
- Defining "association" (e.g., account ID, registrant email, payment instrument) in a privacy-respecting, practicable way?
- Scope and depth of a "reasonable investigation"; timeframes; documentation; reporting to ICANN; metrics for effectiveness; Compliance oversight?
- Wholesale considerations: where account data may be limited, is registrant-level pivoting a workable baseline?

d) PDP Structure and Working Methods (20min)

Question for discussion:

- Is it better to be ambitious and start with two topics, knowing that course correction is available?
- Is it better to be conservative/realistic, and start with a phased approach from the start, knowing again, that course correction is available?
- Regardless of approach, which issue should be addressed first in the PDP?
    - Based on lifecycle, API access makes sense.
    - Does one of the topics seem easier to reach consensus?
    - Does one of the topics seem like it will be more impactful in reducing DNS Abuse?
    - Any other factors to consider in determining the order?

e) Next Steps (5min)