DNS Abuse Mitigation

Presentation to the At-Large CPWG

- **At-Large DNS Abuse High-Level Strategy Development**
- **GNSO Council DNS Abuse Small Team Input Sought**

Justine Chew
ALAC Co-Vice Chair
ALAC Liaison to GNSO

25 June 2025

ICANN
AT-LARGE

Agenda

1. At-Large DNS Abuse High-Level Strategy Development

2. Input for GNSO Council DNS Abuse Small Team

Per GNSO Council DNS Abuse Small Team Assignment Form, small team is tasked to:

- Evaluate broader DNS Abuse mitigation efforts across ICANN
- Assess the impact of the Contract amendments on DNS abuse mitigation efforts
- Discuss and provide a summary on the insights from the INFERMAL study and how these insights can help inform next steps on DNS abuse

Expected Outcome – Report to GNSO Council, including:

- Findings from review of available data sources;
- List of gaps the Small Team may have identified;
- Recommendations on next steps on what other work (policy, further research, etc.) might be needed to address DNS abuse.

At-Large DNS Abuse High-Level Strategy Development

Intersessional Work

- GNSO Council DNS Abuse Small Team
- GNSO Policy Development Process
- ALAC-GAC PSWG bilaterals
- CP Discussions
- etc

Remedial / Review

- To be determined

Identify & Consider

- Research on DNS Abuse - OCTO, NetBeacon etc
- GAC Public Safety WG (PWSG)
- At-Large Plenaries
- Contracted Parties (CP) Summits
- etc

Progress Check

- At-Large Plenaries
- etc

Note: Strategy should consider preventive, in addition to curative measures

At-Large DNS Abuse High-Level Strategy Development

- ICANN83 Policy Forum
  - **At-Large Policy Session with OCTO** [Capacity Building]
    - Work, tool to support DNS Abuse Mitigation
    - Domain Metrica
    - Other Research – Batch Registrations, Abuse uptime, Parked domains
    - INFERMAL Report
  - **At-Large Plenary 2: Progressing DNS Abuse Mitigation Efforts Within ICANN**
    [Engaging community towards Policy Development]
    - At-Large Community
    - Commercial Stakeholder Group (CSG)
    - GAC Public Safety WG (PSWG)
    - Registry Stakeholder Group (RySG)
    - Registrar Stakeholder Group (RrSG)
    - NetBeacon Institute
    - Non-Commercial Stakeholder Group (NCSG)
- What's Next?
  - **GNSO Council DNS Abuse Small Team Work**
    [Path towards possible Policy Development or further contract amendments]
  - Intersessional work with partners
  - At-Large Policy Session with OCTO – follow up?
  - ICANN84 At-Large Plenary on DNS Abuse Mitigation

GNSO Council DNS Abuse Small Team Work

- **Preliminary Input** sought on:
  - **29 gaps** identified so far, clustered into **12 themes**, out of:
    1. GNSO Council DNS Abuse Small Team Report (Oct 2022)
    2. INFERMAL Report – Inferential analysis of maliciously registered domains (Nov 2024)
    3. ICANN Org Report on DNS Abuse mitigation requirements (Nov 2024)
    4. NetBeacon Blog – Analysis of Impact of ICANN Contract Amendments (Dec 2024)
    5. NetBeacon PDP Whitepaper (May 2025)
  - Any other (feasible) gaps?
  - What gaps to address as a priority?
  - *Note: Solutions are for later*

GNSO Council DNS Abuse Small Team Work (1st Look)

High Priority

6. Introduce friction in access to "bulk/batch" registrations	G2 Withhold unrestricted API access for new customers [5]
	G9 Lack of syntactic & operational registrant data validation [2]
	G12 Lack of proactive/timely verification at registration [2]
	G25 Lack of data on bulk registration abuse [1]

1. Associated domain check	G1 Investigate associated domains [4]
	G10 Broaden use of abuse data for preventive action [2]
12. Proactive vs reactive	G11 Minimal deterrent effect of reactive measures [2]
	G23 Challenges in real-time detection of short-lived abuse [4]
	G26 Underuse of predictive algorithms for early detection [1]

2. Complainant reports	G17 25% unactionable complaints [3]
	G27 Awareness on reporting abuse [1]
5. Enforcement challenges	G13 Disparate registrar abuse mitigation responses [3]
	G15 No sanctions/deterrents for recurring non-compliance by CPs [3]
	G20 Delayed ICANN enforcement actions [4]
	G29 Ambiguity in RAA, RA language ('reasonable', 'prompt') [3]
10. Mitigation info from CPs	G18 Measurement challenges due to 'uncharacterized' domains [4]
	G22 Limited transparency in mitigation actions taken reducing accountability & oversight [4]

← Preventive

Curative →

7. Forbid incentives promoting abuse	G21 Inconsistent registrar credential performance [4]
	G6 'Discounts' more prone to DNS abuse [2]
	G7 Free services more likely to be abused by threat actors [2]
11. Subdomains	G3 Unregulated subdomain abuse [5]

3. Compromised vs Malicious	G19 Attention to hijack legitimate domains [4]
	G24 Lack of definition [1]
4. Dispute Resolution	G4 Recourse mechanism for legitimately aggrieved registrants [5]
8. Industry coordination	G5 Inefficient coordination on DGA-based abuse to support LEA [5]
9. Lack of research/data	G8 Lack of empirical research on abuse factors [2]
	G14 No ICANN overview of mitigation actions outside of contract enforcement [3]

Low Priority

Source:

[1] GNSO Council DNS Abuse Small Team Report (Oct 2022)
[2] INFERMAL Report – Inferential analysis of maliciously registered domains (Nov 2024)
[3] ICANN Org Report on DNS Abuse mitigation requirements (Nov 2024)
[4] NetBeacon Blog – Analysis of Impact of ICANN Contract Amendments (Dec 2024)
[5] NetBeacon PDP Whitepaper (May 2025)

Input to GNSO Council DNS Abuse Small Team Work

- Next steps (subject to discussion herein)

Who	What	When
JC / Staff	Issue Survey through CPWG to gather feedback on gaps & priorities	Post CPWG Call on 25 June 2025
CPWG Members	Provide feedback via Survey	By 30 June 2025 at 23:59 UTC
JC	Tabulate & analyze Survey data	1-2 July 2025
CPWG Members	Confirm position based on Survey data as preliminary input	CPWG Call on 2 July 2025 at 14:00 UTC
JC	Relay preliminary input to GNSO Council DNS Abuse Small Team	3 July 2025