# ICANN 83 Session Report:
# CPH DNS Abuse Community Update

On 9 June 2025[1], ICANN Contracted Parties House DNS Abuse working group convened community members to discuss new ideas to enhance the industry's approach to DNS Abuse Mitigation, including exploring topics for a series of targeted, narrowly-scope Policy Development Processes (PDPs). This session marked the first of a series of CPH-led community sessions aimed at finding common ground on this issue.

For this session, the CPH DNS Abuse WG brought forward four topics that the group believes are worthy of consideration. As, for this engagement (and future ones), we want for these conversations to be collaborative and constructive in nature, and grounded on the following principles:

- **Narrow in scope**: the issue is short and constrained—to solve for a specific, definable, problem.
- **Technology agnostic**: the discussion avoids prescribing specific tools—because tools can become obsolete over time.
- **Business model agnostic**: discussions should take into account the diversity of contracted parties—our aim is for an uniform framework that can be adapted to unique business realities.

Each topic was discussed using this framework:

A. **Policy question**: In other words, what do we want to achieve or what is it that we are solving for?
B. **Potential value**: A high level statement of the benefit in addressing the issue.
C. **Other areas of further exploration**: A running list of questions or dependencies that warrant further discussions.

[1] Session Link: https://icann83.sched.com/event/246R0/gnso-cph-dns-abuse-community-update

# Topic 1: A Requirement to Pivot on Actionable Reports of Malicious Registered Domains

| |
|---|
| **Policy Question:** Should registrars have a requirement to inspect other domains in a customer account, or registered with the same registrant information, when they are investigating an actionable DNS Abuse report? |
| **Potential Value**: Creating a requirement for registrars to pivot from an actionable DNS Abuse report may contribute to mitigating or disrupting other malicious registered domains, associated with the reported domain name. |
| **Other areas of further exploration**: Applicability to business models (e.g., wholesale, retail), flexibility to determine circumstances to pivot, considerations for collateral damage, implementation/enforcement will need granularity and nuance. |

Registrars in the room explained this is already in practice by some. Methods vary but the gist of it is similar. When there is an actionable report of DNS Abuse (like phishing) the registrar takes a holistic view to determine the appropriate outcome to mitigate the harm. Sometimes the investigation leads to identifying the same patterns in other domain names registered by the same registrant. When this happens, the registrar takes steps to mitigate, including suspension of the domain name(s).

Other community non-CPH members support further work on this.

Then, the thesis is whether to make this a universal practice among all ICANN accredited registrars.

During the workshop, the audience pointed out certain areas that require attention and thoughtful consideration. In no particular order:

- Diverse business models: retail registrars have a very different vantage point than that of wholesale registrars. While the former group likely has more detailed information about the registrant (and/or account information), the latter group has limited visibility of registrant account information. Thus, it is important to emphasize a uniform framework but allow flexibility in implementation. Also, some called attention to avoiding being too prescriptive and providing bad actors with a blueprint on how to avoid detection.

- Privacy of data: consideration for privacy laws that may define limits on how to use certain types of data.
- Scalability: a requirement to conduct an expanded investigation has to be within reasonable terms to avoid burdensome tasks. For example, if a benign registrant account with multiple domain names is compromised by a bad actor and the bad actor uses the account to register a domain name for the sole purpose of launching a phishing attack (a compromised account), what would a reasonable next step for the registrar be under the “pivot” premise? There’s the need to provide the registrar some discretion and latitude for decision making.
- Enforceability: If this becomes a contractual obligation, how would it be enforced by ICANN Compliance? Elements such as burden of proof and data privacy must be taken into account during any deliberations on this subject matter.

Some also suggested this practice to be documented as a Best Practice and that policy would create a binding obligation to implement the Best Practice.

# Topic 2: Strengthening of API Clauses to Address Bulk Registrations

**Policy Question**: Should the Registrar Accreditation Agreement (RAA) require certain obligations pertaining to the use of API?

**Potential Value**: RAA could be improved to ensure registrars that offer API registration have a requirement of vetting their customers prior to allowing API access.

**Other areas of further exploration:**

- Basic KYC obligations by the registrar prior to offering API access.
- Exploring whether wholesale registrars should also impose certain requirements upon resellers.

The premise here is to strengthen the requirement for registrars offering API domain registration to introduce a gating system to add friction to automated registrations using an API or similar tool. This, in part, addresses the issue of “bulk registration” as discussed in the INFERMAL report—not as a threshold number problem but focusing on the means of registration.

Based on the conversation and input, this topic received good support.

# Topic 3: Mitigation of Batch Registered Domain Names Generated by a Botnet Algorithm

**Policy Question**: Should there exist a clearinghouse to verify DGA lists that can be distributed to gTLD registry operators pursuant to DNS Abuse Mitigation obligations? If so, who can function as the clearinghouse? What functions would this clearinghouse perform?

**Potential Value**: Cybercriminals and botnet operators may use a DGA or Domain (Name) Generation Algorithm to create a large number of domain names they can use to launch cyber attacks, including some forms of DNS Abuse.

To counter these threats, there are special purpose organizations that analyze a DGA to extract the list of domain names, including a corresponding activation date. This information is not widely spread and may be hard to vet at scale, making it hard for registries to act upon.

Opportunity: Develop an operational framework to provide (all) gTLD registry operators with a verified list of botnet generated domain names to prompt proactive action at scale; optionally provide this list to ccTLD registry operators, either where they are also gTLD registry operators or otherwise are interested in aiding in the combatting of DNS Abuse.

**Other areas of further exploration:**

- If a registered domain name that is actioned by the registry operator pursuant to botnet mitigation, should there be relief for affected registrars and/or registrants? If so, in what circumstances?

We received mixed observations regarding the prevalence of botnet DGAs in the current cyber threat environment but most agreed that having a uniform approach to distributing the information to registries and a clear process to action it would be good. A ccTLD member also opined in favor of such an approach as DGAs are agnostic to the notion of country code or generic TLDs (e.g., Avalanche), so ccTLD managers could opt-in to such operational approach.

A registrar observed that any work on this needs to consider the final disposition of the domain name if it were to be sinkholed or locked under a registrar account. Specifically, determining the party liable for ongoing registration fees, etc.

A former law enforcement member and another SSAC member mentioned that collaboration from across the industry is vital to address DGAs in a holistic and effective manner. Not only is there a need for determining a response to disable the DGA but also enabling victim notification and analysis while minimizing false positives. Another attendee explained there's already a good amount of technical work that exists today, but when it is time to action any of it, there are ICANN waivers to issue, on a case by case basis.

Another registrar added that not all DGAs are created equal. There are some DGAs that are used for legitimate purposes, so we need to be clear we are referring to the DGA used for malicious purposes.

Attendees discussed what issues would be within scope for additional technical discussion and policy development but there was good support for further discussion overall. Given the existing situation, there may be room for additional policy work to add clarity to roles and responsibilities of parties and reduce procedural delays to the existing framework so that this type of security threat is mitigated on a faster timeline, while addressing concerns about the final disposition of domain names and associated costs.

# Topic 4: Best Practices for Reporting Phishing

**Policy Question**: Can we elevate the existing Best Practices for reporting phishing so that it reaches a critical mass of abuse reporters?

**Potential Value**: Phishing is the most common category of DNS Abuse and often misreported. The CPH/CSG abuse reporting workshop at ICANN 82 revealed there's still much room for improvement on how to report phishing to registrars (and registries when appropriate). Phishing reports that are incomplete or incorrectly evidenced create a bottleneck in contracted parties' anti-abuse team's queues; actionable reports contribute to reducing mitigation times overall.

**Other areas of further exploration:**

- Should ICANN org use such a Best Practices document to promote good phishing reporting practices among the ICANN community and external stakeholders to bring awareness and elevate the quality of reports and help support effective abuse mitigation?
- Is there any guidance from SAC115 that could be applied to abuse reporting practices? E.g., escalation paths.

A registrar observed this would be a good topic for community conversation. Reporter education would be beneficial for all of us.

# Next Steps

As a next step, the CPH DNS Abuse working group is going to create distinct papers that discuss each topic in more detail. The goal is that these papers help inform next steps on community discussions, including the work of the GNSO Council Small Team. We remain committed to open, collaborative, and constructive conversation to combat DNS Abuse.

The CPH DNS Abuse WG is also open to hear other groups' pain points on DNS Abuse. For this purpose, we created a website to collect community input. The website can be found at https://fightdnsabuse.how/.

Finally, the CPH DNS Abuse WG encourages the GNSO Council to start a PDP on DNS Abuse Mitigation by requesting an Issues Report that focuses on one of the preventative measures discussed on this session report: 1) A Requirement to Pivot on Actionable Reports of Malicious Registered Domains,  2) Strengthening of API Clauses to address bulk registrations, and 3) Discussing a gTLD-wide operational and policy framework to mitigate Botnet DGAs at scale.