Policy Development Process on DNS Abuse Mitigation - Addressing the gaps

Meta appreciates the work done by the GNSO and the DNS Abuse Small Team to identify gaps within current policy that can be solved within ICANN's multistakeholder model. The INFERMAL report (and, separately, the Commercial Stakeholder Group) has identified key gaps that should be addressed regarding DNS abuse; the study highlights that reactive actions (like takedowns) are often too slow to prevent or deter abuse, as many attacks successfully take place within minutes or hours. Preventative measures, such as predictive algorithms and better registrant validation, are needed but not widely implemented. Meta hopes that with widespread support for these initiatives ICANN can ***swiftly*** address these gaps through the policy development process to meet an urgently rising threat.

Meta is one of the most frequently targeted brands for DNS abuse, including phishing, malware, and brand impersonation. In addition to the INFERMAL report, other industry authorities document that "over the last five years, Meta's brands have consistently ranked at the top for phishing abuse, with Facebook being the #1 most-phished brand in four out of five years."[1] Addressing the gaps identified in these reports will benefit internet users and global brands that are the target of DNS abuse.

Meta believes that the ICANN community would widely support these initiatives, and we are hopeful that ICANN's processes can move expeditiously to address shortcomings. It is well known that adversarial actors leverage the DNS at scale to perpetrate a variety of harms, including phishing, malware distribution, fraud, scams, spam, botnets, etc., which harms business, platforms and end users. Even as ICANN and the industry are behind in addressing these trends (which will be accelerated by artificial intelligence), we have the ability and opportunity to close the gaps quickly, potentially matching bad actors' ability to rapidly pivot. To timely fulfill its duties as the guardian of DNS stability and security, ICANN should address these concerns *within the next calendar year*. Kicking off and completing these policy changes within 12 months or less must be the goal. Any timeline longer than the twelve-month window expected by the community highlights a significant flaw in the process.

 # 1. Advocate for Stronger Registrar Safeguards on Bulk Registrations and API Access - Support for a separate, narrowly scoped PDP

Malicious actors register substantial numbers of domains for abuse. As the Netbeacon Institute's White Paper also documents, easy API access without vetting "allows for the rapid setup of malicious infrastructures." Meta supports the recommendation for an ICANN policy that requires registrars to implement friction and trust thresholds before

[1] Interisle Consulting Group, Phishing Landscape 2025

granting API or bulk registration access (as some already do for discrete parts of registrar operations). This includes encouraging waiting periods for new accounts, verifying and validating account activity and history to ensure no prior abuse reports, and implementing tiered access based on risk signals. This approach will reduce the speed and scale at which attackers can launch phishing and impersonation campaigns.

Bulk registration must be defined as being in-scope for the PDP, and calling this policy initiative an "API issue" is in some ways confusing. The GNSO should clarify that bulk registrations made for abusive purposes are the main problem that needs to be solved. The ICANN GAC has formally recommended to the ICANN Board that a PDP here should be "prioritizing bulk registration of malicious domain names."[2] We also agree with M3AAWG that "APIs" or "access to APIs" are an aspect of the problem, and are how some of this abuse is carried out, but access to APIs is not exactly the problem itself, and that "limiting access to APIs" is perhaps not the entire solution. As M3AAWG has noted, "An ICANN policy should recognize that APIs are often a tool used somewhere in the process, but just "restricting access to APIs" will not solve the problem and may have loopholes."[3]

 # 2. Require Associated Domain Checks for Confirmed Abuse - - Support for a separate, narrowly scoped PDP

Meta supports this proposal as one that can disrupt at scale entire abuse campaigns targeting large global brands. ICANN must evolve to embrace advanced technologies that provide modern solutions to modern abuse problems. Accordingly, Meta supports the following abuse-related recommendations:

- **Mandate proactive investigation by registrars:** Registrars should be required to investigate and act on *all* domains directly linked through registration data or payment method to a registrant or account (e.g., as identified by email address, payment method, etc.) when one domain is confirmed as abusive. This requirement should apply to both retail and wholesale registrars.
- Define "association" broadly (e.g., by account ID, email address, payment method) to ensure comprehensiveness.
- **Promote automated tools and intelligence sharing:** Encourage the use of automated tools and the sharing of intelligence between registrars to quickly identify linked domains.

---

[2] GAC ICANN83 Prague Communique, section V. https://gac.icann.org/contentMigrated/icann83-prague-communique

[3] https://www.icann.org/en/public-comment/proceeding/preliminary-issue-report-on-a-policy-development-process-on-dns-abuse-mitigation-08-09-2025/submissions/messaging-malware-and-mobile-anti-abuse-working-group--m3aawg--07-10-2025

Such an approach, which would disrupt entire abuse campaigns, would be far more efficient than the current domain-by-domain takedown process.

We also highlight the need for data accuracy. (See SAC129 report on data accuracy). Closing existing loopholes that allow bad actors to evade verification for 15 days provides a significant window for abuse to thrive.

 # 3. Strengthen DGA-Based Botnet Mitigation and Coordination - Support for a separate, narrowly scoped PDP

Meta supports the following initiatives:

- **Centralized Clearinghouse:** Establish a central ICANN clearinghouse for DGA domain lists and law enforcement orders.
- **Coordinated Response:** Develop tools that effectively identify DGA abuse and promote swift and unified action among all registries upon detection of DGA-based abuse.

Meta supports more consistent takedowns of botnet infrastructures used in large-scale phishing and malware attacks. As the prevalence of automated attacks continues to expand, ICANN also must adopt policies that identify threats that leverage machine learning technologies.

4. Promote Best Practices and Transparency

While best practices make sense for suggestions that may be more challenging to implement universally, they lack the teeth to be adopted and may not lead to actionable results. Meta instead supports binding policy that is subject to Compliance enforcement.