The ICANN GNSO "Business Constituency"

ICANN Business Constituency (BC) Comment on

Preliminary Issue Report on a Policy Development Process on DNS Abuse Mitigation

17-Oct-2025

Background

This document provides input from the ICANN Business Constituency (BC), from the perspective of business users and registrants. We advocate for ICANN policy that:

1. promotes end-user confidence because it is a safe place to conduct business
2. is competitive in the supply of registry and registrar and related services
3. is technically stable, secure and reliable.

General Comment:

Thank you for the opportunity to comment on policy development to address the critical matter of DNS abuse.

Context: DNS abuse is endemic and increasing

By any objective measure, abuse perpetrated through the domain name system (DNS) has become endemic and is further on the rise. Many independent studies – including these below – confirm that online abuse leveraging the DNS is quickly growing:

- Interisle Consulting Group's Phishing Landscape 2025: An Annual Study of the Scope and Distribution of Phishing
  https://interisle.net/insights/phishing-landscape-2025-an-annual-study-of-the-scope-and-distribution-of-phishing

- Internet Crime Complaint Center (IC3) 2024 Annual Report:
  https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

- Anti-Phishing Working Group 2nd Quarter 2025 Phishing Trends Report:
  https://docs.apwg.org/reports/apwg_trends_report_q2_2025.pdf

- DNS Research Federation - Why are European ccTLD abuse rates so low?
  https://dnsrf.org/blog/habits-of-excellence--why-are-european-cctld-abuse-rates-so-low-/index.html

- M3AAWG Best Practices on DNS Abuse Prevention and Mitigation Practices for Registrars and Registries:
  https://www.m3aawg.org/sites/default/files/dns_abuse_prevention_remediation_and_mitigation_practices_for_registrars_and_registries.pdf

Abuse is outpacing ICANN's ability to address it through existing policy development procedures

While the BC is pleased to see and participate in abuse-related policy development, it has become clear that ICANN's existing policy development framework is no longer sufficiently nimble or flexible to deal with such a rapidly increasing and evolving problem.

Following development and implementation of the 2024 contract amendments targeting abuse, ICANN Org and Generic Name Support Organization (GNSO) participants repeatedly assured a concerned community that "highly targeted" policy development processes (PDPs) addressing abuse would ensue, with a 12-month targeted completion window. Neither Org nor the GNSO, however, has delivered on this assurance.

In fact, even with an extremely narrow focus on two agreed-upon areas of policy development, the PDP apparatus (inclusive of policy development, Board consideration, and implementation review) will yield enforceable results in well over a year – two years or more is likely. Meanwhile, DNS threat vectors continue to widen and strengthen, without further planned attention from the community or Org.

Were all gaps identified by the GNSO and documented in the issues report to be handled concurrently, the extended PDP timeline still would be insufficient to effectively meet the threat. Org already has indicated that, due to the soon-to-open new gTLD round in 2026, it may not be able to make resources further available to help the GNSO and community combat abuse through policy development. GNSO time and resources are similarly constrained. The BC reluctantly concludes that, as a result, completion of GNSO-led work on *existing* gaps would not finish for approximately another five years or more. This does not take into account *additional* needed responses to threats may arise in the interim.

This is a shortcoming on the part of the organization and community tasked with DNS security and stability. Threats to the DNS – and thus to the business users of the Internet that the BC represents – will continue to develop and evolve and now will be accelerated by deployment of artificial intelligence (AI). Two- to three-year PDPs, sequentially handled, would merely nibble at the expanding problem and perpetuate the current cycle of ICANN playing catch-up to the rising problem of abuse.

ICANN Org and the community must embrace a faster, better and continual process for ongoing abuse-related work

In light of this shortcoming, the BC advocates, again, for a more efficient and credible process. Specifically, ICANN Org should:

- Enter into contract negotiations with registries and registrars to amend the Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) to implement new obligations for mitigating DNS abuse; and / or
- Implement into contracts, as it did during the 2012 new gTLD program, such new provisions.
- Assist the community in carrying out Recommendation 10.2 of the 2021 Second Security, Stability, and Resiliency (SSR2) Review, which recommends the following:

  Establish a staff-supported, cross-community working group (CCWG) to establish a process for evolving the definitions of prohibited DNS abuse, at least once every two years, on a predictable schedule (e.g., every other January), that will not take more than 30 business days to complete. This group should involve

stakeholders from consumer protection, operational cybersecurity, academic or independent cybersecurity research, law enforcement, and e-commerce.

Further to this point, the BC proposes a new idea for consideration. Specifically, a GNSO standing committee (much like the ccNSO's DNS Abuse Standing Committee) which would be tasked with advising ICANN Org and the GNSO regarding policy development and strategies for the prevention and mitigation of DNS abuse. Because abuse is and will be a long-term, persistent problem, continual attention is warranted to employ timely and impactful tactics for combating it effectively. The committee – which could be dovetailed with the above-referenced CCWG – could have standing to make recommendations (based on independent research) regarding abuse-related policy development, contract updates, and best practices.

Further failing to take these urgent and warranted steps risks not only exacerbating the DNS abuse problem, but also potentially damaging ICANN's credibility as the steward of DNS security and stability.

Evolving definitions of DNS abuse

The BC must again raise the issue of definitions of DNS abuse. ICANN Org says the following in footnote 24 of the preliminary issues report:

SAC115 defines each of these DNS Abuse forms. ICANN used the definition of those terms (malware, botnets, phishing, pharming, and spam used to deliver abuse) named in SAC115 to shape its definition for the purpose of the RA and RAA.

The Security and Stability Advisory Committee (SSAC) in fact **has not** produced a definition of DNS abuse. For the sake of accuracy, in its 2023 comment on proposed abuse-related contract amendments, the SSAC instead said:

For clarity, Section 2.1 of SAC115 does not contain SSAC's definitions of abuse, and the proposed contract definitions of abuse are not endorsed by SSAC. SAC115 Section 2.1 quoted, for discussion and illustration purposes, definitions from the Contracted Parties' DNS Abuse Framework and the Internet and Jurisdiction Policy Network's "Operational Approaches, Norms, Criteria, Mechanisms" document. SAC115 stated a qualification about those definitions: "To be clear there are additional abuses that are worthy of discussion. SSAC finds some of the specific definitions [in section 2.1] limited, and the above do not provide a general definition of abuse that may accommodate the evolving natures of abuse and cybercrime over time."

The BC respectfully requests that ICANN Org makes this clarification publicly known during ongoing discussions so the community is accurately informed.

Comment on identified "gaps"

The BC thanks colleagues, particularly on the GNSO's DNS Abuse Small Team, for working diligently to produce a list of "gaps" between ICANN policy and abuse mitigation needs. Our comments on each follow:

P1: Unrestricted Access to Application Programming Interface (APIs) allowing for high-volume registrations

The BC supports and is participating in policy development work on this issue.

P2 and P3: Lack of Proactive/Timely Contact Verification

The BC views this as a top priority. Registrars' existing verification requirements – which as ICANN Org notes are inconsistently employed – obviously are doing little as an abuse mitigation measure. Syntactical and operational "verification" is barely verification at all and is very easily gamed by nefarious registrants.

Registrars already employ more rigorous verification procedures when it suits their business needs. For example, as of April 2024, GoDaddy has required domain name auction participants to complete a reasonably stringent verification procedure that includes submission of government-issued identification, a photograph of the user, and a copy of proof of address (e.g., a utility bill or credit card statement). Such measures, also widely and successfully employed by various ccTLD managers and further recommended by the European Union's Network and Information Security directive (NIS2), would very likely have the greatest positive impact on abuse rates and severity. The BC strongly advocates for inclusion of more stringent verification requirements as a tactic for **proactively** preventing abuse.

P6. Challenges in Real-Time Detection of Short-Lived Abuse

ICANN Org states in the issues report:

> *Overall, combating short-lived DNS abuse requires a multi-layered approach that combines advanced detection techniques with proactive monitoring, information sharing, and rapid response capabilities. Thus, this might be tackled outside policy (e.g., through technology improvements or threat intel sharing), but shows that, similar to the gap above, focusing or introducing more preventative measures can reduce DNS Abuse more effectively than reactive measures.*

The BC disagrees that this gap may be better addressed away from the ICANN sphere. As stated above, preventative measures (e.g., more stringent verification) are squarely within ICANN's remit and would be a full system approach of tackling abuse at multiple levels, with a far bigger impact on reducing harm caused versus leaving it to one party to address. P7. Underuse of Predictive Algorithms for Early Detection

Org correctly states:

> *Some companies/organizations likely use predictive systems (e.g., some large registrars have internal fraud detection and some registries collaborate with security firms to vet registrations in sensitive TLDs).*

However, Org goes on to say:

> *Contractually requiring specific security measures based on an algorithm may be challenging, given the chance for false positives and the reality that technology-specific mandates can quickly become outdated. Given the technical nature of this issue, it does not appear best suited for ICANN policy. A more feasible path might be inclusion in a non-binding best practices document.*

The BC disagrees that this measure is unsuited for binding policy. If ICANN is to carry out its duties as the steward of DNS security and stability, enforceable measures such as **pre-emptive** tactics are and will become more necessary as DNS abuse threats intensify. The BC supports development of contracted party requirements in this realm. Best practices would be only sporadically employed and would merely play at the edges of abuse mitigation. This is no time for quasi solutions.

P8. No Post-Registration Identity Checks for Suspicious Activity

The BC, individually and as a member of the CSG in its call for action, supports bridging this gap. Again here, best practice suggestions are merely that – suggestions. Use of validation procedures are proven to mitigate abuse and deserve to be enforceable policy.

A1. Unactionable Complaints to ICANN

The BC agrees that not all abuse complaints (no matter where submitted) are actionable. Even in our business community, only a fraction of DNS users know how to submit a proper complaint or are even aware such reporting pathways exist.

Part of the issue at play is standards and procedures that differ by registrar or registry. This perhaps can be addressed by the community's cooperation on standardization of agreed to parameters for abuse reporting that optimize complaints for constructive action. The BC is prepared to contribute to this type of collaboration.

A3. Malicious vs. Compromised - Clarifying Responsibility

While the BC does not agree that compromised domains are expressly outside ICANN's remit, we acknowledge that it may be prudent to focus initially on mitigation of maliciously registered names. This dovetails with our support of the use of predictive algorithms and preemptive action instead of relying on post-harm measures; the latter permits infliction of damage to businesses and their customers at a too rapid rate.

C1. Limited Transparency in Mitigation Actions taken

The BC believes contracted parties have an opportunity to respect those who correctly report legitimate, actionable abuse. "Closing the loop" with abuse reporters is a reasonable step to ensure that appropriate relief has been provided. Leaving reporters in the dark prompts uncertainty and unnecessary follow-up.

C2. No Requirement to Check for Associated Domains

The BC supports and is participating in policy development work on this issue.

C3. Lack of Standard Dispute/Recourse Mechanism for Registrants

The BC supports development of a mechanism for registrants to be heard in cases of disputed action taken on domain names.

C4. Unregulated Subdomain Abuse

The BC supports the proposed solution to the growing problem of subdomain abuse as put forward in the issues report. The BC also suggests that ICANN Org should continue to proactively monitor and report on this problem as a function of the SSR2's recommended ongoing community review of DNS abuse definitions.

C6 and C7. Due Diligence and Transparency in Mitigation

While the BC agrees that abuse-related investigations should be appropriately thorough, we caution that abuse experienced by businesses and their customers unfolds in matters of minutes and hours. Prompt action is required to minimize financial, reputational and other forms of harm. The BC supports the NCSG's suggestion that contracted parties immediately notify registrants regarding action taken against their domain name(s) with accompanying rationale.

C8. Inconsistent Responses - Seeking Standardization

The BC disagrees with ICANN Org's position and recommendation on this gap. Org writes:

> *The amended ICANN contracts deliberately did not include rigid timelines, to allow flexibility. Instead, they say "promptly" and allow for case-by-case circumstances to dictate appropriate actions…*

Businesses and their customers under cyberattack do not enjoy "flexibility," nor does a loose definition of "promptly" contribute to constructive outcomes commensurate to the level of an experienced threat. Yet again, the suggestion that a best practice will suffice is unlikely to make a helpful change to the now inconsistent and insufficient status quo. Businesses and their customers, and the broader internet community, would benefit from contracted party help with standardizing responses and timing.

Relation to other gaps in the DNS Abuse Small Team Matrix: E5 and E6. No Rapid Takedown Requirement (Desire for 24-hour response) and Lack of Feedback Loop.

Please see the BC's input to C8 above.

E2. No Clear Escalation of Sanctions for Recurring Non-Compliance, and E3. Delayed ICANN Enforcement Actions

The BC applauds ICANN Compliance's recent actions regarding enforcement of updated contract terms. However, we underline the fact that even with new RA and RAA terms, DNS abuse continues to increase. This is not a reflection of the efforts of the Compliance team at ICANN, but of the realities of the abuse environment and the relative lack of effectiveness of current tools.

CC1. Lack of Coordination during Domain Generation Algorithm (DGA) Botnet Attacks

The BC supports the community's efforts to evaluate this need and considers this the best mechanism for addressing it. The BC would support this work continuing in parallel to any other work effort.

CC2. No Mechanism to Update DNS Abuse Definitions (Periodic Review)

ICANN Org *correctly* says that SAC115 recommends periodic review of abuse definitions, as did the recommendations from the SSR2 team. The BC finds that these are reasonable, easily implementable steps for the overseer of DNS security and stability to take – that is, periodically reviewing the definition of DNS abuse with the

full community's participation (e.g., not merely ICANN Org and contracted parties). The BC also strongly recommends the participation of the SSAC in definitional reviews, as the community's expert in abuse trends.

Relation to other gaps in the DNS Abuse Small Team Matrix: C5. Imposter Domain Names (Exact Matches to Trusted Names)

ICANN states:

> *During ICANN81 the CPH and CSG held a session discussing this topic and how the DNS Abuse definition established by the ICANN contract amendments is not sufficient to address this type of DNS Abuse.*

This is correct – the contract amendments, as they currently exist – are insufficient to address this type of abuse. The BC, however, advocates for community consideration of precisely this type of abuse, which is rapidly growing. The BC acknowledges that "exact match" domain abuse may be considered by some to be an intellectual property matter and thus outside ICANN's remit; the BC disagrees and believes this addressing exact match impostor domain names (many of which seek to harvest personally identifiable information or other critical records) is a commonsense step that need not be divisive to the community. The Trademark Clearinghouse (TMCH) could serve as a database of trusted names for registries and registrars to validate if the registration of a domain is an exact match to a trusted name.

Comment on Single PDP vs. Subsequent PDPs

The BC appreciates the pros and cons identified by ICANN Org regarding a single PDP vs. multiple PDPs.

We observe that regardless of the PDP mechanism employed, PDPs are very likely to take too long to meet head-on the difficulties of the current abuse environment. Already, the community and Org have backtracked on the planned 12-month PDP timeline, and the BC has identified that further delays are likely.

The BC strongly encourages ICANN to deploy resources to much faster timelines and parallel working methods that are worthy of its role as the protector of the DNS and address the abuse environment as it actually exists.

Voluntary Daily Zone File Publication by Commercially Used ccTLDs - Increasing Transparency & DNS Security via CZDS

The BC further offers the following comment regarding the use of the Centralized Zone Data Service (CZDS). This is not directly tied to this request for comment; however, the BC offers in good faith its ideas for improving CZDS as an abuse mitigation tool.

Why Address This Now?

Commercially popular ccTLDs (.ai, .io, .co, .tv, .gg, .vc, etc.) play a major role in the global DNS but are not currently publishing daily zone files to ICANN's CZDS. Daily publication by new and legacy gTLDs has proven essential for monitoring domain registration activity and improving DNS abuse detection and mitigation.

Zone files serve as the authoritative source of record for domain registrations, providing verification independent of cached DNS responses that may be subject to DNS cache poisoning attacks. Daily publication enables verification of legitimate domain ownership and detection of unauthorized changes.

Current Gap

The absence of daily zone files from ccTLDs limits the ability of researchers, industry, and stakeholders to analyze short-lived and potentially malicious domain names. This hinders both the responsiveness of technical communities and the reputation of widely used ccTLD domains.

Addressing the Window of Invisibility

Recent academic research has demonstrated that at least 1% of domain names exist in a "window of invisibility" – registered and used maliciously within the 24-hour gap between daily zone file publications (Sommese et. al., 2024). These domains often complete their attack lifecycle before security researchers can detect them. Moving from daily to sub-daily (hourly) zone file publication would dramatically shrink this window, enabling near real-time threat detection and response.

Invitation to Participate

Voluntary participation by ccTLDs in daily CZDS zone file publishing would immediately:

- Strengthen transparency and trust in ccTLD operations;
- Aid the global DNS community in improving security posture; and
- Position participating ccTLDs as leaders in responsible registry management.

Upcoming Improvements:

ICANN, through CZDS operations, is actively developing daily delta (differential) zone files that will provide only the changes between publications - dramatically reducing bandwidth consumption and processing requirements for all consumers. This innovation will make it feasible for more organizations to monitor zone file changes in real time, improving the speed and scale of abuse detection. As delta files reduce the cost of consumption, more frequent (sub-daily) publication becomes economically and technically viable.

Looking Forward:

The BC views these enhancements as mutually reinforcing: delta files reduce the cost of consumption, making more frequent publication economically viable, and encouraging ccTLD participation by demonstrating CZDS as an efficient, modern platform. Together, these improvements would significantly enhance the global community's ability to detect and respond to DNS abuse.

Early voluntary participation will help shape best practices and put technically advanced ccTLDs at the forefront for future policy and technical enhancements.

The BC invites the ccNSO and its members to discuss this opportunity at ICANN84 and explore collaborative models for voluntary daily publication, with a view toward sub-daily publication as technical capabilities advance.

Conclusion

Driving Urgent, Enforceable Action on DNS Abuse

The BC's analysis underscores a critical truth: DNS abuse is a persistent, evolving threat that demands more than aspirational language and non-binding best practices. ICANN Org must move beyond passive facilitation and embrace a leadership role that prioritises enforceable, timely, and scalable solutions. The BC calls for:

- **Accelerate the use of existing contractual mechanisms and policy tools** to implement enforceable DNS abuse mitigation obligations ensuring that improvements are deployed swiftly and effectively, without waiting for prolonged procedural cycles;
- **Provide Leadership to a standing, expert-led advisory group,** either by leveraging existing structures or creating a new, purpose-built body that reflects the shared responsibility of all internet stakeholders registries, registrars, service providers, cybersecurity professionals, civil society, and commercial actors. To lead on policy evolution and ensure agile, coordinated cross stack responses to emerging DNS abuse threats;
- **Implementation of periodic, time-bound reviews** of DNS abuse definitions, ensuring they remain relevant and actionable;
- **Adoption of proactive, preventative measures**—including rigorous identity verification, proactive analytics, and rapid response protocols, as enforceable standards, not optional guidelines.

The BC urges ICANN Org and the broader community to commit to a future where DNS abuse is not just discussed, but systematically and effectively mitigated through enforceable policy, operational accountability, and continuous improvement.

We look forward to constructive cooperation with ICANN and the wider community going forward on the enduring issue of DNS abuse.

This comment was drafted by Leo Angelo, Chris Lewis-Evans, Ching Chiao and Vivek Goyal. It was approved in accordance with our Charter.