IPC Comments on the Preliminary Issue Report for a PDP on DNS Abuse Mitigation

I. Introduction

The Intellectual Property Constituency (IPC) welcomes the Preliminary Issue Report (PIR) on a PDP for DNS Abuse Mitigation (8 September 2025). As advocates for consumers and intellectual property (IP) rights, the IPC has long stressed the close overlap between DNS abuse and intellectual property infringement. Many phishing and malware schemes exploit trusted trademarks or brand names to ensnare users. We appreciate that the PIR acknowledges both the progress (e.g., 2024 RAA contract amendments) and the remaining gaps in curbing DNS abuse.

A. DNS Abuse is Escalating

Recent studies establish that DNS abuse is *growing* in scope and impact, underscoring the urgency for stronger mitigation policies. For example, the annual Interisle *Phishing Landscape 2025* study found nearly **1.96 million phishing attacks** reported from May 2024 to April 2025 – a **182% increase since 2021**.[1] Over **1.5 million domain names** were used for phishing in that period, the highest on record.[2] Crucially, **77% of phishing domains were maliciously registered** (not merely compromised) by criminals – a 3% year-over-year rise (2024-2025).[3] This confirms that most DNS abuse is intentional at the point of registration, not incidental. The FBI's Internet Crime Complaint Center reports over **$16.6 billion** in direct losses to U.S. businesses and consumers from cybercrime in 2024 alone.[4] Phishing is a gateway to further harm – according to U.S. authorities, over **90% of cyberattacks** begin with a phishing lure.[5] These trends show no signs of abating. Notably,Anti-Phishing Working Group's (APWG) quarterly trends report observed **1.13 million phishing attacks in Q2 2025**, up from 1.00 million in Q1.[6]

Such data reinforces the IPC's long-standing call to treat DNS abuse as a systemic threat to consumer trust, public safety, and brand integrity. It is not coincidental that phishing campaigns often impersonate famous brands or services – the Statistical Analysis of DNS Abuse in gTLDs Final Report noted 85% of abusive .top domains in one sample contained terms like "Apple" or "iCloud," indicating a coordinated phishing campaign using these brands.[7] Criminals deliberately

---

[1] Interisle Consulting Grp., Phishing Landscape 2025: An Annual Study of the Scope and Distribution of Phishing 1 (Sept. 9, 2025), https://interisle.net/phishinglandscape2025.
[2] *id.*
[3] *id.*
[4] *id.*
[5] *id.*
[6] Anti-Phishing Working Group, Phishing Activity Trends Report for the 2nd Quarter 2025, at 3–10 (2025), https://docs.apwg.org/reports/apwg_trends_report_q2_2025.pdf (accessed Oct. 4, 2025).
[7] Maciej Korczyński et al., Statistical Analysis of DNS Abuse in gTLDs: Final Report (Aug. 9, 2017), https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf (accessed Oct. 4, 2025).

register domains bearing trademarks to deceive users relying upon the trust and goodwill that these trademarks have garnered. The IPC, therefore, views DNS abuse mitigation and intellectual property protection as intertwined goals – ultimately to protect both IP owners and consumers. An online environment rife with abusive domains erodes consumer confidence in brands – and conversely, robust anti-abuse measures help protect brand owners and Internet users from fraud and phishing.

B. Need for Swift & Adaptive Measures

The IPC strongly supports additional improvements to the mitigation policies and contract requirements related to DNS Abuse, whether through the initiation of a GNSO Policy Development Process (PDP) focused on DNS abuse or through additional bi-lateral contract negotiations, whichever is quicker. We agree with the PIR's identification of two high-priority topics – Unrestricted Bulk Registration APIs and Associated Domain "Portfolio" Checks – as initial targets. We urge the GNSO Council to launch this PDP without delay. At the same time, the IPC believes that additional gaps highlighted in the PIR should be addressed concurrently or in parallel, rather than postponed for years. Rather than endure years of policy making, ICANN should consider contract negotiations as an alternative approach to a PDP. Traditional PDP timelines are lengthy, yet the abuse problem is dynamic and accelerating. The community cannot afford to tackle these issues sequentially over a half-decade. Instead, we echo the Business Constituency's call for a more *nimble, iterative policy process* that can adapt and expand as new DNS abuse vectors emerge. The GNSO should:

i. Implement PDP 1 immediately on the two agreed topics (bulk API access and associated domain checks – detailed below). These alone can significantly reduce abuse at scale by adding "friction" for bad actors and disrupting large malicious campaigns. The IPC believes that a good idea is to further split these two topics into their own PDP tracks, so as to be as efficient as possible.
ii. Plan PDP 2 (or work tracks) to begin addressing additional known gaps in parallel. Notably, Registrant identity verification, the use of predictive algorithms, post-registration validation for flagged domains, and standardized abuse reporting mechanisms. The IPC specifically advocates including these in scope:
    a. *Proactive contact verification:* Many abusive domains slip through with fake or unverified registration data. IPC supports stricter pre-registration and immediate post-registration validation of registrant information (as championed in SSR2 Recommendation 7 and by the EU's NIS 2 directive) since most phishing and similar abusive attacks are conducted shortly after the registration of the domain name.[8] Requiring *timely* email/phone verification for new registrations (not 15 days later) and performing identity or address checks for high-risk registrations would greatly deter throwaway abuse registrations. This was identified as gap P2/P3 in the PIR, and we urge it to be folded into policy work, not left to best practices.

[8] See information published by INFOSEC on the phishing attack timeline: 20 hours from target to detection (accessed Oct 13, 2024).

b. *Predictive anti-abuse algorithms:* Large registrars and some ccTLDs already use fraud detection algorithms to flag suspicious domain orders (e.g. detecting bulk sequential names, obvious brand typos, or false registration data). IPC believes such automated screening for known red flags should be encouraged or required across the industry, with appropriate care to minimize false positives. The PIR (gap P7) hesitates to mandate evolving technology, but IPC sees value in at least setting a policy *framework* where registrars are expected to make reasonable use of commercially available abuse prediction and scoring services. At minimum, ICANN should facilitate sharing of best practices and data feeds (as SSR2 recommended).[9]

c. *Post-registration checks for suspected abuse:* The IPC supports establishing obligations for registrars to re-verify or suspend a domain if there is strong evidence it is engaged in DNS abuse (gap P8). Today, if a domain is flagged in malware or phishing feeds, there is no duty to re-check the registrant's identity or other domains – an abuse loophole that attackers exploit. We agree with the PIR and other CSG members that *best practices are not enough* here – enforceable policy is needed to ensure suspicious cases trigger action (e.g. requiring the registrant to provide ID within a short window or face suspension). This is important post-GDPR since it's effectively impossible for the abuse reporter itself to identify other potentially-related abusive domains.

d. *Improved abuse reporting mechanisms:* It remains too difficult for victims or security researchers to report DNS abuse in a standardized way. A unified abuse complaint system (as recommended in SSR2 Rec.17)[10] would increase actionable reports and help contract compliance identify patterns. We also encourage ICANN to ensure the Centralized Zone Data Service (CZDS) and Domain Abuse Activity Reporting (DAAR) data are easily available to researchers and include ccTLD data where possible, to improve insight into global abuse trends.

In short, if alternative approaches to a PDP are not feasible, the IPC urges the GNSO to treat the PIR's gap list holistically – launch the first PDP on the two core items, but simultaneously lay the groundwork (charters, drafting teams, staff support) to address the other critical gaps through additional policy work or other means. We note and support the PIR's suggestion that some issues might be handled outside formal policy if faster results are achievable. For instance, ICANN *Contractual Compliance* could tighten enforcement of existing obligations (by terminating bad acting registrars that fail to meet their DNS abuse obligations) or negotiate additional RAA amendments, and the community could form a cross-functional task force to handle certain operational fixes and suggest negotiation topics. The IPC is open to innovative approaches – what matters is results. We appreciate that the PIR (and the DNS Abuse Small

---

[9] Second Security, Stability, and Resiliency (SSR2) Review Team, Second Security, Stability, and Resiliency (SSR2) Review Team Final Report (Jan. 25, 2021), https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf (accessed Oct. 4, 2025). Second Security, Stability, and Resiliency (SSR2) Review Team, Second Security, Stability, and Resiliency (SSR2) Review Team Final Report (Jan. 25, 2021), https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf (accessed Oct. 4, 2025).

[10] *Id.*

Team's report) highlights the need for an "agile and responsive" framework to evolve with emerging threats.

C. **Adopt SSR2 Recommendation 10.2 – Periodic Definition Review**

The IPC reiterates SSR2 Review Team *Recommendation 10.2*, which calls for ICANN to establish a staff-supported cross-community working group that will evolve the definition of DNS Abuse on a predictable 2-year cycle, with each cycle taking no more than 30 business days. In our view, implementing this would go a long way to ensure policy keeps up with new abuse phenomena. The Security and Stability Advisory Committee (SSAC) noted in SAC115 that abuse definitions must be able to expand over time as criminals invent new tricks. IPC urges ICANN to immediately initiate such a biennial definitions review process (involving stakeholders from consumer protection, cybersecurity, law enforcement, and e-commerce as envisioned). For example, the current narrow definition (malware, botnets, phishing, pharming, and spam-as-delivery) might need to be broadened to include things like mass "imposter" domains (exact-match brand spoofing) or large-scale "social engineering" domains that are not captured today. The IPC is prepared to participate actively in such reviews. We believe a standing DNS Abuse WG with regular update cycles would complement the PDP's work by flagging new issues and recommending when policy adjustments are needed. ICANN org should assist the community in carrying out this plan, as the SSR2 final report recommended. The bottom line: DNS abuse policy cannot be a one-and-done effort; it requires ongoing adaptation in partnership with experts (e.g. SSAC).

D. IPC Positions on Specific DNS Abuse "Gaps"

The Preliminary Issue Report identified a range of gaps in the current DNS abuse mitigation framework (numbered P1–P11, A1–A3, C1–C8, E2–E3, CC1–CC2). The IPC's comments on each gap are summarized below:

Gap (PIR reference)	IPC Comment
P1. Unrestricted API Access for Bulk Registrations	The IPC fully supports requiring "gating" and friction for high-volume registration tools. New accounts should not get bulk API access until they've met trust thresholds (e.g. time as customer with no abuse reports). We agree with imposing identity verification or volume limits on new API users. This will significantly curtail automated mass-abuse campaigns. IPC notes the INFERMAL study's finding – unrestricted APIs correlate with 401% higher abuse rates – and views gating as an effective remedy.

P2 & P3. Lack of Proactive/Timely Contact Verification	Requiring prompt identity and contact verification for new registrations is one of IPC's top priorities. We urge eliminating the 15-day grace period – key contact info should be verified before or immediately after activation. Also, apply *risk-based checks*: e.g., additional ID proof for suspicious registrations (high-value keywords, known fraud patterns). These steps were championed by SSR2 and are mandated in EU NIS 2. In IPC's view, inconsistent or lax verification is enabling abuse, so we favor making verification requirements stricter and uniform via Consensus Policy.
P6. Challenges in Detecting Short-Lived Abuse	The IPC agrees real-time detection is hard – by the time a domain is flagged, the harm is done. We believe the answer lies in preventing such domains from ever going live, via measures like P2/P3 and P7 (verification and predictive blocking). Within the PDP, we support emphasizing *pre-registration due diligence* as the best way to reduce short-lived abuses. ICANN should facilitate data sharing and technology tools to help registrars identify high-velocity abuse (e.g. feed of domains generated by DGAs or reported in near-real-time).
P7. Underuse of Predictive Algorithms	Include as a policy recommendation or guideline. IPC believes contracted parties should deploy automated anti-abuse scoring to the extent practical. We recognize that one cannot mandate specific algorithms, but policy can require registrars to have a fraud detection mechanism in place and act on its output. Leading ccTLD registries already do this. ICANN should encourage such programs industry-wide. At a minimum, this could be a best practice codified in policy (e.g., "registrars *should* utilize available threat intelligence to vet registrations").

P8. No Post-Registration Identity Re-checks	The IPC supports that when a domain is reported for serious abuse (with evidence), the registrar should be obligated to re-confirm the registrant's identity and details. For example, require the registrant to provide a valid government-issued ID or additional verification *promptly* once their domain is the subject of a credible abuse complaint. If they fail or the info is invalid, the domain should be suspended. This addresses the "bad actors cycling fake registration data" problem. Right now, an abuser can operate until a formal Registration Data inaccuracy procedure concludes, which is frustrated by the difficulty in getting disclosures and the use of privacy/proxy registrations. The IPC supports making this an enforceable duty (the PIR suggested it could be policy or a best practice). Legitimate registrants have nothing to fear from a spot-check; bad actors will be exposed.
P9 & P10. Economic Incentives Prone to Abuse	The IPC acknowledges that ICANN cannot directly regulate pricing or promotions under current contracts. However, the clear link between cheap domains and high abuse (as INFERMAL showed – malicious domains averaged $4.71 vs $8.62 for benign) needs addressing. We support exploring voluntary frameworks or future contract incentives. For instance, SSR2 Rec.14 suggested adjusting fees to discourage high-abuse TLDs. At a minimum, transparency is important and registries/registrars should report volume of discounted registrations and associated abuse rates so the community can shine a light on problematic practices.
A1. Unactionable Complaints to ICANN	The IPC agrees that many abuse complaints are misrouted or incomplete. We support efforts to standardize the DNS abuse reporting intake process, and the community should define what constitutes an "actionable" abuse report (fields, evidence required and other elements of actionable report) and ensure complainants are guided to provide. The IPC notes that abuse reporting mechanisms used by some registrars are needlessly challenging to use, and can involve design flaws that frustrate the reporting process -- e.g. a web form requiring input of

	a full URL for a domain being reported on email abuse grounds (i.e. no active website use) or forms that don't allow the reporter to actually attach evidence of abuse such as a phishing email thread. This needs to change to ensure all abuse reporting mechanisms are equally functional and consistent. The IPC agrees that actionable DNS abuse complaints require the education of abuse complainants. However, it is equally important for registrars and registries to provide documented and well-reasoned, clear rationales for their decisions to act or not act on an abuse complaint. It is only with this level of communication that we can begin to improve the DNS abuse process and the submission of actionable complaints.
A3. Malicious vs. Compromised Domains – Clarifying Responsibility	The IPC supports that policy efforts should focus on malicious registrations (within ICANN's remit), but encourage cooperative action on compromised domains. The IPC agrees with the PIR's note that policies should clearly scope to what registrars can impact. Maliciously registered domains – where the domain itself was obtained to perpetrate abuse – are squarely in remit and must be dealt with by registrars (suspension, associated checks, etc.). Compromised legitimate domains (hijacked / hacked websites) are tougher: the fix lies with the hosting or the site owner, not the registrar. We caution, however, that distinguishing the two is not simple, and from a user's perspective, both are dangerous. Therefore, while we don't propose expanding contractual duties to broadly "fix" compromised sites, we do think registrars should assist where feasible – e.g., notify the registrant and relevant CERTs if their domain is being used in a botnet or phishing unbeknownst to them.

C1. Limited Transparency in Mitigation Actions	Increase transparency and feedback loops. The IPC believes abuse reporters deserve to know the result of their complaint – did it lead to suspension or not? We support requiring (via policy or procedure) that registrars send a response to the abuse reporter when a case is resolved (even if just "We reviewed domain X and have suspended it" or "…found no violation"). BC members have noted the frustration of filing detailed reports and seeing the domain still active with no feedback. Closing that loop will build confidence and also reduce duplicate reports or needless follow-ups. On a broader level, IPC supports ICANN Compliance, providing more granular public reporting: e.g. list of registrars with the most abuse reports and how many resulted in action. Sunshine can be a deterrent. We also support exploring a mechanism for notifiers to see status (NetBeacon already does this for participating registrars). In summary, transparency is relatively low-cost and uncontroversial – we encourage the PDP to include recommendations to improve communication and data-sharing around abuse mitigation outcomes.
C2. No Requirement to Check for Associated Domains ("Portfolio" checks)	This is one of the two priority items the IPC wants to see adopted. Registrars should be required to investigate a customer's other domains when one is found to be abusive. Organized crime rarely registers just a single domain – they register batches. Policy should implement a "Know Your Customer's Portfolio" approach: when domain X is suspended or terminated for abuse, check domains Y and Z in the same account or with the same registration data details. The absence of this today is a glaring gap – it lets bad actors sacrifice one domain at a time ("whack-a-mole"). The NetBeacon Institute's white paper (and the BC) specifically recommends this "Associated Domain Check" requirement, and the IPC concurs. We note that some registrars already do this informally. Making it standard will dramatically increase the impact of abuse takedowns by turning off an entire malicious campaign instead of one node. Implementation detail: the policy should define what triggers an associated check (e.g., a domain

	suspended for malware/phishing) and define the scope (same registrant, same account, etc.). The IPC is committed to working out those details.
C3. Lack of Standard Recourse Mechanism for Registrants	The IPC recognizes the importance of due process. While we advocate aggressive anti-abuse action, we also support giving legitimate registrants a chance to respond if they believe an error was made. We support the concept of a registrant recourse mechanism (as proposed in the PIR and by NetBeacon). This could be as simple as requiring registrars to offer a point of contact for suspension disputes, and to promptly review any evidence provided by the registrant. It does not mean a suspended domain must be reactivated during review – safety comes first – but it ensures fairness. The IPC notes that truly false positives are rare if the criteria are sound, but this mechanism will help build trust in the system. Importantly, such a process should be quick (days, not weeks), require the appellant to disclose themselves and not be overly burdensome to avoid abuses by criminals. We support including this in the PDP.
C4. Unregulated Subdomain Abuse	The IPC is keenly concerned about subdomain abuse, which can host phishing or other abusive activity while the base domain looks benign. We agree with the recommendation that ICANN institute a requirement that registrants offering subdomain services must have an abuse contact and take action on abuse in their subdomains. This essentially pushes the obligation down to the level of the subdomain provider. While this might be tricky to enforce, it can be implemented via registrars' terms of service – i.e. require registrants to agree they will monitor and mitigate abuse on any subdomains they operate, or else face suspension of their domain. The IPC also calls for continued data collection on subdomain abuse (DNS Research Federation studies show European ccTLDs have generally avoided this problem by strict policies). Coordinating with ccTLD operators via the ccNSO to share best practices (some ccTLDs forbid wildcard subdomain services entirely) could be very fruitful. In summary, IPC is in

	favor – subdomain-based abuse should not slip through the cracks.
C6 & C7. Due Diligence and Transparency in Mitigation	Support balanced best practices. The IPC agrees that abuse handling should be diligent and, where feasible, registrants should be informed of actions on their domain. In practice, most registrars already investigate reports – our concern has been speed and consistency, not that they act frivolously. So we have no objection to reinforcing that evidence-based, documented investigations are expected (indeed, that helps if actions are later challenged). As for transparency to registrants: yes, if a domain is suspended for abuse, the registrant should promptly be told why (e.g. “We received evidence of phishing targeting Bank X”). This dovetails with our call for reporter feedback – communication all around is beneficial. Importantly, such notice to the registrant should not delay the mitigation (it can be simultaneous or after the fact). The IPC believes these can be handled as best practice recommendations in the PDP report, and potentially integrated into Registrar Accreditation Agreement (RAA) amendments or contractual compliance expectations.
C8. Inconsistent Responses – Seeking Standardization	The IPC understands why the contracts used flexible language – cases vary – but we share the concern that “promptly” is too elastic. Businesses under attack benefit from predictable response times. We support exploring the feasibility of setting baseline response targets as well as incentives to reward registrars within a preferred timeframe (such as credits back on registration fees). For instance, the community could agree that an abuse complaint with sufficient evidence should be processed within 24 hours in normal circumstances. If a registrar consistently takes much longer, that might warrant scrutiny. While writing exact SLAs into contracts could be difficult, the PDP could recommend that the PDP provide some guardrails around the definition of “promptly” as for instance, “within 1–2 business days, absent extenuating factors.” The IPC also encourages the adoption of standard operating procedures for abuse handlers (many already coordinate via the DNS

	Abuse Framework). In short, we favor pushing the laggards to match the best performers.
E2. No Clear Sanction Escalation for Recurring Non-Compliance	The IPC supports using all available levers to motivate compliance. For example, if a few registrars are responsible for an outsized share of abuse, ICANN should be able to initiate audits or impose conditions on accreditation renewal. The IPC supports the concept of an escalation path beyond just breach notices. While implementing new sanction regimes might fall to the ICANN Board or contract renegotiation, the PDP can recommend that the Board consider such measures. In sum, IPC wants to ensure that chronic bad actors face tangible consequences.
E3. Delayed ICANN Enforcement Actions	The IPC appreciates that ICANN Compliance has ramped up enforcement. If any systematic delays are observed, we would urge allocating more resources or streamlining processes. Ensuring Compliance has sufficient staff and an unambiguous mandate to prioritize DNS abuse is key – the IPC would support any recommendations the PDP might make to reinforce these positions. The IPC also notes that ICANN Compliance should attempt to transition from reactive to proactive on abuse mitigation measures.
CC1. Lack of Coordination for DGA Botnet Domains	The IPC is very concerned about DGA-based abuse. We strongly support the concept (from the PIR and NetBeacon White Paper) that ICANN should serve as a central hub for DGA takedown coordination. If the GNSO PDP cannot directly mandate it, the PDP should at least formally recommend that ICANN org implement the community DGA framework (already developed by the GAC PSWG and RySG). The IPC stands ready to support any such cross-community solution.

CC2. No Mechanism to Update DNS Abuse Definition (Periodic Review)	As detailed above, IPC wants a periodic review process for DNS abuse definitions with community consensus. This gap is essentially the same point – that without a built-in update process, our policies may become outdated. We cannot stress enough that the IPC fully endorses periodic definition review. For example, one abuse type on the fringes today is mass “exact-match” impersonation of brands (sometimes dismissed as purely an IP issue). If data shows this tactic is being used overwhelmingly for fraud/phishing (which it often is), the community might agree to bring it under the “DNS Abuse” scope in a future cycle. Only a regular review can accommodate that. We are pleased the BC and others concur that this is “reasonable and easily implementable” by ICANN.

II. **Conclusion**

The IPC appreciates the opportunity to comment and the inclusion of community input like ours in shaping the PDP’s charter. In summary, the IPC supports swift initiation of the DNS Abuse PDP with an initial focus on bulk registration API gating and associated domain checks, which we believe will materially reduce abuse volumes; and urges the GNSO to concurrently address additional gaps – especially registrant verification, abuse prediction, post-compromise measures, and reporting standardization – through parallel policy work, contract negotiations, or advisory recommendations, rather than leaving them entirely for a later date. The IPC stresses the need for an agile, ongoing policy process (via SSR2 10.2’s periodic reviews) so the community can adapt to new abuse methods.

The IPC is committed to playing a constructive role in the PDP and subsequent implementation. We will continue to bring the perspective of intellectual property stakeholders, who have a keen interest in a safer DNS where consumers and brands are less vulnerable to abuse. By enacting the measures outlined in the PIR and ensuring the policy framework can evolve, ICANN will make the DNS a more resilient space for all legitimate participants. The IPC looks forward to the Council’s resolution on this PDP and stands ready to contribute our expertise to translating these recommendations into reality.