Government of India Comments on the Preliminary Issue Report on DNS Abuse

1. Introduction

The Government of India appreciates ICANN's effort in preparing the Preliminary Issue Report on a Policy Development Process (PDP) on DNS Abuse Mitigation. India supports launching the single, narrowly scoped PDP recommended in the report to address the two priority gaps, P1 (unrestricted API access) and C2 (associated domain checks), because these issues directly enable bulk malicious registrations. Beyond those two, the report catalogues a set of "later/future work" gaps across the DNS abuse life-cycle. India offers the following comments on those gaps.

India's comments are grounded in public-interest considerations: protecting consumers from phishing and fraud, ensuring equitable treatment of registrants, and maintaining a secure and stable DNS. Citations refer to passages in the Preliminary Issue Report where each gap and proposed solutions are described.

2. Distinguishing Consensus Advice from Issues of Importance in Recent GAC Communiqués

Distinguishing Consensus Advice from Issues of Importance in Recent GAC Communiqués

In the last five ICANN meetings (79–83), the GAC has repeatedly raised DNS abuse in its communiqués. It is important to differentiate between consensus advice and issues of importance when referencing these documents:

- **ICANN83 (Prague, June 2025)**: The only recent communiqué that includes consensus advice on DNS abuse. In section "Policy Development Related to DNS Abuse" (page 11), the GAC advises the Board to urge the GNSO Council to commence targeted, narrowly scoped PDPs on DNS abuse, focusing on bulk registration of malicious domains and associated domain checks. This advice, adopted by GAC consensus, is binding unless rejected by a supermajority of the Board; it emphasises urgency ahead of the next new gTLD round and highlights specific PDP topics.

- **ICANN82 (Seattle, March 2025)**: Contains a detailed issue of importance (not formal advice) in section "DNS Abuse." The GAC appreciates data from the INFERMAL report and calls for more information on contract amendment implementation; it considers whether a targeted PDP might be warranted but does not advise the Board. This issue flagged bulk registrations, economic incentives, and proactive practices as areas for further work.

- **ICANN81 (Istanbul, November 2024):** Another issue of importance. The GAC welcomes constructive discussions on DNS abuse, notes increased abuse reporting after contract amendments, and expresses interest in potential narrowly scoped PDPs while calling for regular reporting from ICANN Compliance.

- **ICANN80 and ICANN79 (Kigali and Cancun, 2024):** The communiqués for these meetings also treat DNS abuse as an **issue of importance**; they encourage monitoring the effectiveness of contract amendments and exploring further measures, but they do not contain formal consensus advice. As such, policy positions based on these communiqués are interpretive rather than binding.

In this submission, India carefully distinguishes between consensus advice (from ICANN83) and issues of importance (ICANN79–82). Recommendations that call for new PDPs or contract amendments are grounded in consensus advice; where only issues of importance exist, India's analysis relies on national priorities and broader community discussions.

3. Table 1: India's Position/Comments on Prioritized Gaps

Issue (Gap ID, Title, Phase)	India's Analysis and Policy Position
P1: Unrestricted API Access (high-volume registrations)	India supports adding vetted controls to high-volume registration. INFERMAL analysis found 4× more abuse when APIs are ungated, and the NetBeacon white paper recommends trust thresholds or delays for new accounts. In line with GAC ICANN83 advice to prioritize bulk-registration abuse, India urges a narrowly scoped PDP to require registrars to vet new API clients (e.g. via verification, KYC, credentialing) before granting full access or the registrar should limit how many domain registrations an API user can make per minute/hour/day **for new clients more strictly and for established clients more leniently over time** and introduce friction (e.g. predefined waiting periods) to deter automated abuse.
C2: No Requirement to Check for Associated Domains .	India strongly supports this being addressed by the narrowly scoped PDP and recommends specific contract amendments. Associated domain checks would require registrars, upon receiving an actionable abuse report, to review all domains registered by the same account or linked by common identifiers and, where warranted, suspend them. India advocates amending **RAA Section 3.18** to add an "Associated Domain Investigation" clause and creating a new section in the **RA** obligating registries to support registrars in these investigations (e.g., facilitating bulk suspension requests). This approach aligns with GAC consensus advice at ICANN 83, urging action on bulk registrations.

4. Table 2: Later/Future Gaps – Preliminary Solutions vs. India's Position

Issue (Gap ID, Title, Page, Phase, Summary & Preliminary Proposed Solution)	India's Analysis & Position (Policy Instrument, Rationale, Amendments)
1. **Phase 0 (Preventative)**	
P2 & P3: Lack of Proactive/Timely Contact Verification	India supports strengthening verification via contract amendment and, if necessary, a narrowly scoped PDP. India recommends amending the RAA's Section 3.7 and the RDDS Accuracy Program Specification to mandate instant (simultaneous) email and phone verification via OTP at the time of registration, thus eliminating the current 15-day window. This requirement should apply uniformly to all registrations, whether single or bulk, ensuring that domains do not activate until contact details are verified. Instant/simultaneous verification will not adversely affect registrar operations; on the contrary, it enhances WHOIS accuracy, mitigates DNS abuse at the registration stage, and prevents anonymity from being used as a shield by malicious actors. The lacuna in the existing systems is that it is anonymous by design. Therefore, removing 15 days for registrant verification and instead, instant/simultaneous verification will balance user safety and trust with privacy concerns. Instant/simultaneous verification will directly address Preventative Gaps P2 and P3 (lack of timely verification) and also mitigate Gap P6 (short-lived abuse, fast-flux hosting, and one-hour domains) identified in the Preliminary Issue Report on DNS

	Abuse. Requiring OTP-based validation before activation prevents attackers from exploiting unverified contacts for rapid, short-lived abuse. India supports implementing this through contract amendments, and, if necessary, a narrowly scoped PDP to establish uniform verification timelines and triggers. Consistent with the GAC Communiqué released at ICANN 83 under Issues of Importance (Accuracy of Registration Data), India emphasizes that these obligations must be codified contractually, ensuring global uniformity, enforceability, and accountability across all registrars.
P5: Minimal Deterrent Effect of Reactive Measures (Uptime)	India concurs that a PDP is not needed and endorses focusing on prevention rather than punitive uptime policies. Reactive takedowns can inadvertently harm legitimate users and do little to deter sophisticated attackers. Instead, India supports voluntary best-practice guidance encouraging registrars to improve rapid takedown protocols while investing in preventive measures (such as friction in registration processes and better threat intelligence). ICANN and the DNS Abuse Institute should also publish case studies demonstrating how preventative measures reduce abuse.
P6: Real-Time Detection of Short-Lived Abuse	India recognizes that to curb short-lived abuse (Gap P6), domains spun up, abused, then dropped within hours, the critical moment of control is before domain activation. Therefore, as proposed by us for P2 and P3 above, the root cause of the problem can be addressed through instant/ simultaneous verification along with other approaches as follows: 1. **Instant/ Simultaneous verification before activation (eliminating 15-day window):** • Amend RAA as mentioned in India's position for P2 and P3. • A domain must not be activated until verification succeeds. • This ensures that no domain ever becomes live with unverified or fraudulent contact data. • This approach addresses P2 & P3 (lack of timely verification) at the root, and prevents the exploitation that gives rise to P6. 2. **Complementary technical measures (optional but helpful):** Even with instant verification, additional detection tools improve security, though these could be adopted via guidelines, not necessarily requiring a PDP. Examples include: • Real-time threat intelligence feeds: registrars integrate abuse lists to flag suspicious new registrations before activation. • Enhanced logging and telemetry: collecting domain lifecycle data, registration timestamps, account behavior, and DNS query patterns to detect anomalies early. • Registrar suspension or hold triggers: if verification fails subsequently or abuse signature is detected, the registrar can pre-emptively suspend or hold the domain.

	3. **Guidelines before PDP (if possible):** India prefers that these obligations be captured only via contract amendments for P2 and P3, while P6 is addressed via technical measures through guidelines, and PDPs may be explored later. A narrowly scoped PDP would only be considered as a fallback to ensure baseline verification triggers and timelines. This approach maintains global uniformity, enforceability, and accountability across all registrars, while minimizing procedural overhead. Simultaneously, it is also worthwhile to note that the preliminary report points to technological improvements and information-sharing frameworks, which are indeed valuable. However, India stresses that the key question is whether registrars will voluntarily deploy such real-time solutions in the absence of contractual obligations. Past experience shows that voluntary approaches often lead to uneven adoption, with proactive registrars investing in detection while others become safe havens for abuse. India, therefore, supports a multi-layered approach combining technology, intelligence sharing, and machine learning–based monitoring, but underscores that these measures should be first tested before being contractually enforced.
P7: Underuse of Predictive Algorithms	Predictive algorithms can help detect abusive registrations early, but concerns about false positives must be addressed. By calibrating models using sensitivity, specificity, and ROC/AUC thresholds, false positives can be minimized while still capturing most abusive domains. However, technical calibration alone is insufficient; there must be compliance safeguards (rapid appeal, transparency, oversight) so registrants are not unfairly harmed if their domain is wrongly flagged. India notes that relying only on voluntary adoption will lead to uneven practices, as not all registrars invest equally in abuse prevention. To ensure consistent and fair deployment, baseline obligations should eventually be included in the Registrar Accreditation Agreement (RAA) and Registry Agreement (RA). At the same time, India recognizes that the community has limited experience with such models. **Therefore, these tools should first be tested and evaluated, and based on lessons learned, appropriate amendments to RAA/RA can be made later to mandate their deployment along with safeguards.**
P8: No Post-Registration Identity Checks for Suspicious Activity	India supports the findings of the preliminary issue report to establish risk-based re-verification. When a registrant repeatedly registers abusive domains, registrars should re-verify the registrant's identity. India proposes amending RAA Section 3.7 or adding a new section requiring triggered KYC-style checks after specific thresholds of abuse (e.g., multiple abuse reports within 30 days). Best practices could guide registrars and registries to adopt uniform triggers and due-process safeguards, ensuring consistency across registrars and avoiding over-collection of personal data.
P9 & P10 – Economic Incentives Prone to Abuse (Discounted Pricing & Free Services)	India agrees that pricing is beyond ICANN's contract authority; no PDP is warranted. ICANN should, however, encourage registrars to consider the abuse impact of steep discounts by publishing educational materials and best practices. Voluntary "responsible pricing" guidelines could help registrars monitor abuse associated with heavily discounted registrations. Consumer-protection agencies (including India's CERT-In) should remain vigilant but policy intervention is not advised.

P11 – Limited Use of Abuse Feeds/Threat Data	India agrees with the potential solution suggested in the preliminary issue report.
Phases 1–2 Abuse reporting	
A1 – Unactionable Complaints to ICANN	India believes education is necessary but not sufficient; contract amendments should set minimum complaint-intake standards. While training stakeholders to file complete reports is important, registrars and registries must also facilitate reporting. India proposes narrowly scoped PDP amending RAA Section 3.18.4 to require registrars to publish a clear abuse reporting user-friendly web form with mandatory fields (e.g., domain name, evidence of abuse) and step-by-step guidance with FAQs to assist the complainants, combined with best-practice educational materials, will reduce unactionable reports and improve responsiveness. This approach aligns with the GAC communique (ICANN 81–83) stresses the need for accessible reporting and responsiveness.
A3: Malicious vs. Compromised Domains	India notes that under Gap A3 (Malicious vs. Compromised Domains), the lack of clarity around whether registrar obligations extend to compromised (hacked) websites causes inconsistent responses and delays. India supports clarifying that DNS abuse obligations focus on malicious registrations, but also insists registrars be required to publish clear FAQs and guidance for registrants whose domains have been compromised, explaining how they may contact agencies (e.g. national CERTs, cybercrime units), what documents must be submitted (identity proof, domain ownership evidence, security logs), and what procedural steps are available to restore suspended or blocked sites. Such measures help distinguish genuine compromise cases from abuse by malicious registrants. A PDP may not be required at this stage, and further community discussion should proceed within ICANN to refine these obligations and best practices.
Phase 3 Contracted-party mitigation	
C1 – Limited Transparency of Mitigation Actions	India supports a contract amendment complemented by best practices to establish transparency in reporting mitigation actions by registrars/registries. In this context, amending RAA Section 3.18.4 (handling and tracking abuse reports) by setting up obligations upon the registrars to publish periodic statistics (e.g., number of abuse reports received, time to resolution, outcomes) while protecting personal data. Best-practice guidelines should outline the format and granularity of reports. Transparency enables community oversight.
C3: Lack of Standard Registrant Recourse/Appeal .	India agrees with the potential solution suggested in the preliminary issue report.
C4 – Unregulated Subdomain Abuse	India supports a consensus policy (PDP) to address **subdomain abuse**, accompanied by contract amendments. Subdomains are increasingly used for phishing, and ignoring them leaves a major enforcement loophole. The PDP should define obligations for registrants offering subdomain services—such as maintaining a monitored abuse contact, prohibiting abusive use in their terms of service, and promptly responding to credible reports. Registrars should be required via RAA amendments to incorporate these obligations into their registration agreements with registrants who act as subdomain providers; likewise, the RA should empower registries to suspend domains used to host abusive subdomains if providers fail to act.

	However, it is critical to note that **these obligations for registrars and registries under the RAA and RA do not apply to registrants who operate as registry-like providers at the second level**. For example, the associated domain-name checking requirement or gated API access prioritized in the Issue Report on DNS abuse for bulk registration will not properly extend to a registrant that is effectively running a registry at the second level (e.g., permitting public third-level registrations under their second-level domain). In that scenario, abuses under subdomains may fall outside the ICANN contractual remit, and victims have no effective recourse unless that gap is closed via the proposed PDP. Exempting abuses through the usage of a subdomain will also render the policy development process for associated domain name checks and other similar issues redundant. Two scenarios must be distinguished clearly: 1. A registrant holding a second-level domain (e.g. **xyzresort.com**) may create subdomains for internal or branch offices (e.g. **delhi.xyzresort.com**, **mumbai.xyzresort.com**) for legitimate use. 2. A registrant acting like a public registry (e.g. **hotel.com** allowing **abc.hotel.com**, **xyz.hotel.com** registrations) essentially opens up third-level registration access. In such public subdomain models, when abuse occurs, it often escapes ICANN's enforcement because the registrant registers as a "normal registrant" rather than as a registrar or registry. India urges the PDP to close this gap by clearly assigning accountability for subdomain operators and ensuring that abusive third-level registrations under registry-style operations are covered under ICANN's anti-abuse regime.
C6 & C7 – Due Diligence & Transparency in Mitigation	India recommends developing best practices now and assessing the need for policy once more data is available. Proportionate investigation and timely notification are good governance practices, but imposing a policy without data could have unintended consequences. ICANN should monitor mitigation practices and publish anonymised case studies to inform whether a PDP is needed. In the meantime, India supports voluntary guidelines that encourage registrars to investigate allegations appropriately and notify registrants when action is taken. Due process should be followed subsequent to the action taken by the competent authority.
Phase 4 ICANN Compliance Enforcement	
E2: No Clear Escalation of Sanctions for Recurring	India favours exploring a PDP to establish graduated sanctions, balanced with due process. Chronic non-compliance erodes trust. A PDP could consider measures such as temporary suspension of registrar accreditation, financial penalties, or posting compliance bonds, with clear thresholds and appeal rights. Amendments to the RAA and RA should introduce such sanctions, referencing the existing two-stage compliance process. India cautions that sanctions must be appropriate and not punitive for isolated errors.
E3: Delayed ICANN Enforcement Actions	India agrees that a PDP is not needed and emphasises continued transparency. ICANN Compliance appears to be enforcing the 2024 contractual amendments actively. India encourages ICANN to publish periodic enforcement statistics and share lessons learned, ensuring the community remains informed. We recommend that ICANN needs to investigate and identify the actual reasons for these gaps and delays, and build strategies to address them effectively.

Cross-Cutting (CC) categories	
CC1 – Lack of Coordination During DGA Botnet Attacks	ICANN-issued directives without contractual liability. This aligns with GAC Public Safety Working Group advice (ICANN 81–83) emphasising better coordination on botnet takedowns. India also agrees with the findings of the preliminary report that although the issue is potentially appropriate for policy development, this item does not necessarily require further policy work and can be implemented outside the contractual requirements. India further supports the findings of the NetBeacon White Paper that proposes a PDP on "Establishing a Centralized ICANN Coordination Role for DGA-Related Malware and Botnet Mitigation," and the five point proposed policy elements in the preliminary issues report. However, India recommends that the proposed ICANN coordination hub take cognizance of not only final court orders but also interlocutory (interim) court orders, so as to enable rapid preventive action and avoid irreparable loss in cases of large-scale DGA or botnet attacks.
CC2 – No Mechanism to Update DNS Abuse Definitions	India supports the findings of the Preliminary Issues Report on this subject.
P4 – Lack of Data on Bulk Registrations	India supports the findings of the Preliminary Issues Report on this subject.
DT2 – Lack of Empirical Research on Abuse Factors	India supports the findings of the Preliminary Issues Report on this subject. Empirical data is essential for sound policymaking. India urges ICANN to continue funding studies on abuse patterns, mitigation efficacy, and the impact of contractual obligations.

****