APNIC 62

prop-172: Defining Internet Abuse through IP Addresses

A shared vocabulary for abuse — not new obligations, not new enforcement

Prepared for: APNIC sig-policy

Presented by: Alban Kwan, Co-founder and CEO, Trusted Notifier Network

#apnic62

MUMBAI, INDIA
4 – 10 September 2026

Problem Statement

- APNIC policy requires resource holders to maintain an abuse mailbox and respond to reports — but no APNIC policy defines what "abuse" actually means
- Without a shared definition, the community has no common starting point to discuss whether the response duty is being met
- Enforcement of the existing duty is effectively impossible: a "breach" of the response obligation has no defined anchor, and bulletproof hosting persists unchallenged
- Several jurisdictions already impose content-related obligations on hosts directly; absent a regional, technical definition, national rules will fill the vacuum unevenly — raising the risk of Internet fragmentation

Objective of Proposal

- Establish one narrow, agreed definition of "Internet Abuse through IP Addresses" for APNIC policy purposes
- Give the existing abuse-mailbox / response duty an anchor, so non-response can be identified
- Set out non-exhaustive categories of technical and content-adjacent conduct the definition covers
- Confirm that adjudication in the first instance rests with the resource holder, supported by a good-faith safe harbor
- ***This proposal is intentionally narrow and technical — it establishes shared vocabulary, not new obligations or enforcement powers.***

The Proposed Definition

"Internet Abuse through IP Addresses" means the use of an IP address, or set of IP addresses, registered to or held by an APNIC account holder, to conduct or facilitate activity that causes, attempts to cause, or creates a material risk of technical harm to the security, stability, or trust of the Internet, that the resource holder has the practical and operational ability to address.

This includes, but is not limited to, the non-exhaustive categories on the following slide.

Non-Exhaustive Categories of Abuse

- Distributing or hosting malware, including botnet command-and-control (C2) infrastructure
- Originating, amplifying, or reflecting Distributed Denial of Service (DDoS) traffic
- Unauthorised scanning and intrusion
- Routing-layer abuse (e.g., BGP hijacking)
- Fraudulent resource acquisition or transfer
- Hosting infrastructure used for phishing, fraud, scam, or impersonation of a legitimate entity for deceptive purposes

Supported by RFC 4084, RFC 4732, RFC 4778, and RFC 4948.

Definition Safeguards

Built-in carve-outs that keep the definition narrow and fair

Protection against operational errors

Good-faith operational errors that are identified and promptly corrected — including inadvertent routing misconfigurations — do not constitute abuse. The same applies to conduct by a third party (customer, user, employee) that the resource holder addresses promptly once notified.

Adjudication responsibility

Adjudication of whether reported conduct constitutes abuse rests, in the first instance, with the resource holder — where notice comes from a party with a legitimate basis to report and the holder has the practical ability to act. An isolated, delayed, or imperfect response does not, on its own, constitute abuse; the definition targets patterns of non-response, not individual lapses.

Good-faith reliance protected

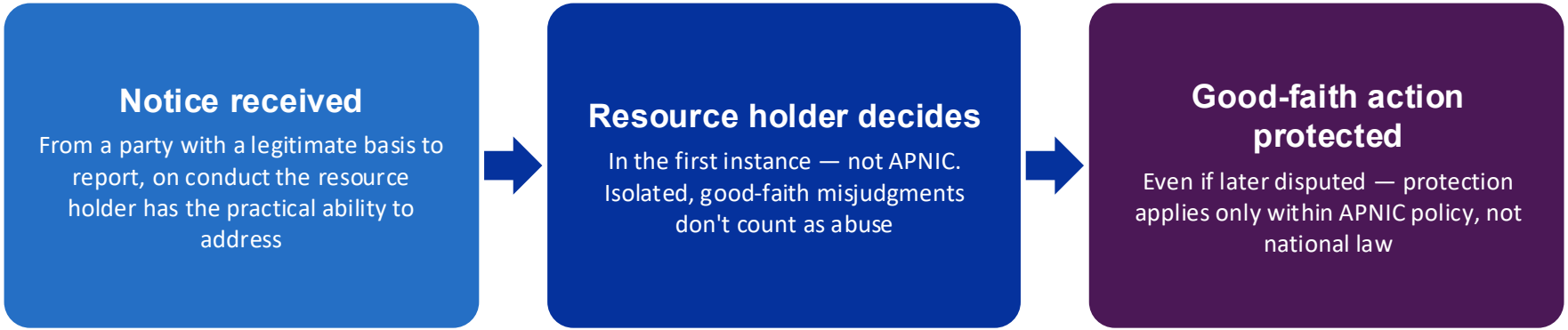
Acting in good faith on a substantiated notice does not itself constitute abuse, even if the resource holder and complainant later disagree. It creates no broader monitoring obligation and no admission of liability. Holders are encouraged, not required, to keep a record of notices and actions taken.

Limits on APNIC's power

APNIC does not have the power to adjudicate abuse. As steward of Internet number resources, APNIC's role is limited to ensuring resource holders do not neglect their stewardship responsibility — for example, by ignoring legitimate reports in bad faith — not to determining whether a case is abuse.

Who Decides?

Self-adjudication, with a good-faith safe harbor — not a central authority



APNIC's role: hold resource holders accountable for responding — never for the merits of the call itself.

In Scope / Out of Scope

In scope

- One narrow, agreed definition of "IP address abuse"
- Non-exhaustive categories of technical and content-adjacent conduct
- Who decides in the first instance (the resource holder)
- A good-faith safe harbor, scoped to APNIC policy only

Explicitly out of scope

- New obligations, reporting requirements, or compliance mechanisms
- Any APNIC power to adjudicate whether conduct is abuse
- Misinformation, disinformation, defamation, or other speech-based complaints
- Ordinary commercial or contractual disputes
- “Unlawful” as part of the definition

Advantages

- Gives the community a shared, agreed vocabulary for "abuse" where none currently exists
- Provides an anchor for enforcing the existing abuse-mailbox / response duty — closing a real enforcement gap
- Reduces fragmentation risk by establishing a regional technical baseline before national rules fill the vacuum unevenly
- Preserves resource-holder autonomy: self-adjudication in the first instance, not a central authority
- Includes an explicit good-faith safe harbor, protecting isolated errors and promptly-corrected mistakes
- Deliberately narrow and technical — excludes speech-based, commercial, and jurisdiction-dependent conduct, limiting scope creep
- Grounded in recognised technical harms and supported by existing RFCs (4084, 4732, 4778, 4948)
- Creates no new reporting obligations or compliance mechanisms — low implementation cost

Disadvantages / Open Risks

- Does not define "adequate response" or grant APNIC enforcement power — deferred to a future PDP, so today's enforcement gap is only partly closed
- A formal definition could narrow attention away from abuse types that fall outside its scope (raised by Japan Open Policy Forum)
- How APNIC would assess "adequate response" without adjudicating the underlying conduct remains unresolved (raised by Aftab Siddiqui)
- Key terms — facilitating, hosting, phishing, fraud, scam, impersonation — are not yet defined; left to a future working group
- Cross-jurisdictional conduct (e.g., gambling) is left to best practice rather than policy, risking inconsistent handling across resource holders
- The good-faith safe harbor is scoped only to APNIC policy, not national law, so protection may feel incomplete to operators facing local legal exposure
- As a first attempt at a shared definition, the proposal is intentionally designed to trigger community debate on scope and breadth

Effect on Resource Holders

- Gain a clearer basis for what "abuse" means for the purposes of their existing response duty
- Retain first-instance adjudication — no new compliance burden or process imposed
- Good-faith actions, including reasonable reliance on a substantiated notice, are protected even if later disputed
- No new record-keeping requirement — retaining notice/response records is encouraged, not mandated
- Need to distinguish isolated good-faith lapses (protected) from a pattern of non-response (not protected)

Effect on APNIC

- APNIC's role remains unchanged and limited: ensuring resource holders do not neglect stewardship responsibility (e.g., ignoring reports in bad faith)
- APNIC does not gain, and is not seeking, any power to adjudicate whether particular conduct is abuse
- No new administrative, reporting, or enforcement mechanism is created by this proposal — that work is deferred to a future PDP / internal process
- Provides the Secretariat and Policy SIG a defined, narrow vocabulary to ground future discussion of enforcement

What's Deliberately Left Open

Working group / best practice

- Terminology (facilitating, hosting, phishing, fraud, scam, impersonation)
- Role-based responsibility by resource holder type (access/transit vs. hosting vs. enterprise)
- Cross-jurisdiction conduct (e.g., gambling) — best practice, not policy
- Monitoring for narrowing effect / scope creep over time

Requires a future PDP / APNIC internal development

- Defining “adequate response” and APNIC's enforcement power and process
- Disagreement between a complainant and a resource holder
- Acknowledging/investigating a complaint vs. being required to stop the activity
- What exactly APNIC would assess if a complaint is escalated

Community Feedback So Far

v001 was posted to sig-policy on 10 August 2026 — feedback already incorporated into this draft

Commenter	Feedback
Jonathan Brewer	Broadened harm to include "attempts"; added scanning/intrusion category; suggested supporting RFCs
Terry Sweetser	Flagged "unlawful" as importing geopolitics into a technical process — now removed entirely
Aftab Siddiqui	Raised the structural question: how does APNIC assess "adequate response" without judging the underlying conduct?
Japan Open Policy Forum	Warned a formal definition could narrow attention away from abuse that falls outside it

What Changed in v2

- "Unlawful" removed entirely — the definition no longer depends on any jurisdiction's law
- Scanning / intrusion category added
- Good-faith safe harbor made explicit: scoped to APNIC policy only, does not touch national law
- "Adequate response" and enforcement power reclassified as requiring a future PDP, not just a working group
- Supporting technical references added (RFC 4084, 4732, 4778, 4948)

Discussion Invited

- **Working group scope**
  - Terminology, role-based responsibility, and cross-jurisdiction best practice — who wants to join?
- **"Adequate response"**
  - Should this require a standalone PDP, or be part of APNIC's internal process?
- **General feedback**
  - Does the conduct list strike the right balance — broad enough to matter, narrow enough to be safe?

Comments welcome on the sig-policy mailing list.