INTERNET SERVICE PROVIDERS AND CONNECTIVITY PROVIDERS CONSTITUENCY (ISPCP)

Early Community Input — GNSO DNS Abuse Mitigation (DNSAM) PDP1

Submitted to: DNSAM PDP1 Working Group / GNSO Secretariat (gnso-secs@icann.org)
Submitted by: Internet Service Providers and Connectivity Providers Constituency (ISPCP)

1. Introductory Statement

The Internet Service Providers and Connectivity Providers Constituency (ISPCP) welcomes the opportunity to provide early input on the DNS Abuse Mitigation Policy Development Process. As ISPs and connectivity providers, our members occupy a distinct and operationally critical position in the DNS ecosystem. We are neither registrars nor registries, yet we are routinely on the front lines of DNS abuse incidents as they affect end users and downstream networks. Our members operate core internet infrastructure and have direct experience with the real-world impact of coordinated DNS abuse campaigns, including phishing, malware distribution, and botnet command-and-control infrastructure.

ISPCP broadly supports the principle that contracted parties should take DNS abuse seriously and act with reasonable diligence when abuse involving a domain under their management is identified. We offer the following input in the spirit of constructive, technically grounded policy development, and we urge the Working Group to ensure that any framework adopted is operationally feasible, legally sound, proportionate, and protective of legitimate registrant rights. ISPCP approaches this issue from the perspective of operational internet stability and end-user protection, recognizing that effective abuse mitigation must be both technically sound and institutionally legitimate.

ISPCP notes at the outset that the charter explicitly excludes compromised domains from the scope of this PDP. We support this carve-out as essential and urge the WG to be precise in the final framework about how a registrar should distinguish between a domain registered with malicious intent versus a legitimate domain that has been compromised or hijacked. These two categories require fundamentally different responses and conflating them would produce unjust outcomes for innocent registrants.

The ISPCP supports early contributions to the PDP proposing contractual amendments for the Registrar Accreditation Agreement which would quickly find consensus in the group, provide a common basis for next steps and reduce the initial suggested timeline.

2. Responses to Charter Questions

Q1 What triggers the requirement to investigate associated domain names?

ISPCP recommends that the trigger for an associated domain check should be set at a meaningful evidentiary threshold, not merely the receipt of any abuse report. The appropriate trigger should be:

- A determination by the registrar following investigation of an individual reported domain that the domain was registered for malicious purposes (not merely suspected but concluded based on available evidence).
- The determination must relate specifically to one of the DNS abuse categories defined in the RAA (malware, botnets, phishing, pharming, or spam as a delivery vector for those categories).
- The registrar should have a reasonable basis to believe that associated domains may be part of the same campaign (e.g., registration patterns, infrastructure clustering, or behavioral indicators) rather than being required to pivot automatically based solely on account linkage.

ISPCP cautions strongly against triggers based solely on the receipt of third-party abuse reports. Reports vary widely in quality, reliability, and substantiation. A framework that requires pivoting upon receipt of any report, without a prior determination of abuse, would risk over-enforcement and could create procedural instability by treating unverified allegations as sufficient grounds for action.

Q2 What criteria should define "association" between domains?

ISPCP recommends a tiered approach to association criteria, recognizing that different signals carry different levels of reliability and different risks of false positives.

Association may be established using one or more criteria, depending on the available evidence and the operational judgment of the registrar. The framework below is intended to illustrate the relative evidentiary strength of different signals, rather than to create a mandatory checklist that must be assessed in every case.

High-confidence association signals:

- Domains registered under the same verified customer account (billing entity, payment fingerprint, or other verified account identifiers).
- Domains using an identical nameserver cluster in combination with other behavioral abuse indicators.
- Domains registered in rapid sequence from the same session or IP range, particularly when correlated with known abuse patterns.

Medium-confidence association signals:

- Shared registrant email address, noting that email addresses may sometimes be reused or spoofed.
- Overlapping WHOIS or registration data, including address or phone number fields.

Lower-confidence / supportive indicators:

- Lexical or pattern similarity across domain names registered under different accounts.
- Shared historical abuse-report patterns without confirmed malicious purpose.

Lower-confidence indicators should generally be treated as supportive signals rather than standalone evidence for establishing association.

The Working Group should explicitly clarify that shared hosting infrastructure alone (such as a common IP address or hosting provider) is not a sufficient basis for determining association, as such infrastructure is commonly shared among unrelated registrants.

The policy should also account for privacy and proxy service scenarios, where registrant identification may not be directly visible, and provide an appropriate escalation path when further verification is required.

Q3 What constitutes a "reasonable investigation" by a registrar?

ISPCP recommends that a "reasonable investigation" for associated domain checks should be defined as a structured review process that includes:

- Querying at least one criterion of the registrar's own internal records to identify domains sharing the same customer account, registrant email, or other high-confidence association criteria identified in Q2.
- To the extent that high-conficence association cannot be established, the registrar should increase the confidence by including at least one of the following vectors:
- Reviewing available technical indicators (DNS data, nameserver configuration, registration timestamps) for identified associated domains.
- Consulting available abuse intelligence sources (blocklists, threat feeds) where technically and legally feasible.
- Documenting the steps taken, findings, and the basis for any resulting action or decision not to act.

Critically, ISPCP emphasizes that "investigation" and "action" must remain distinct obligations. Investigation findings should determine what, if any, action is warranted, and such action should be proportionate to the evidence found. Registrars should not face compliance pressure that creates an implicit incentive to suspend first and investigate later.

We recommend to require investigation standards that are easy to follow and implement regardless of the size and operational setup of a registrar. The approach to require at least one data element to be investigated and leave more investigations to the registrar appears to allow for that. In case the WG wishes to be more prescriptive - which might not be advisable as a consensus policy should not be an advisory for wrongdoers on how to game the policy - the WG should consider the proportionality of investigation requirements relative to registrar size. A uniform "reasonable investigation" standard applied without regard to registrar capacity would be effectively unenforceable for smaller accredited registrars who lack dedicated trust-and-safety teams. The WG may wish to develop guidance or minimum standards that are calibrated to registrar volume or capacity.

Q4 What data access and privacy safeguards are necessary?

ISPCP urges the WG to engage directly with data protection and privacy experts before finalizing any framework, given that pivot investigations inherently involve correlating and processing personal data across multiple registrations. Key considerations include:

- GDPR and applicable data protection law compliance: Registrars processing personal data for the purpose of abuse investigation must have a lawful basis for doing so. The framework should clarify what legal bases apply (e.g., legitimate interest, legal obligation) and should not assume that abuse investigation creates a blanket exemption from data protection obligations.
- Data minimization: Registrars should only access and correlate data that is strictly necessary for the pivot investigation, and only for the duration of the investigation.

Q5 Are there remedies if associated domain checks have an adverse impact on registrants?

Yes, and ISPCP considers robust remedies to be essential to the legitimacy of any pivot framework. Recommended remedies include:

- Pre-suspension notice: Except in narrowly defined emergency circumstances where continued operation of associated domains presents an immediate and demonstrable harm, registrants should receive timely written notice before any suspension of domains identified through a pivot investigation, with an opportunity to respond.
- Accessible appeals mechanism: There should be a clear, standardized, and timely appeals process by which a registrant can contest a suspension decision, with defined timelines for registrar response and resolution.
- Expedited reinstatement: Where a pivot investigation results in the suspension of domains that are subsequently found not to be malicious, reinstatement should occur promptly and without penalty to the registrant.
- Transparency reporting: Registrars should periodically report on the number of associated domain investigations conducted, actions taken, appeals received, and outcomes enabling systemic review of whether the framework is producing proportionate results. The reports should be sent to ICANN and be treated confidential. ICANN should only publish accumulated figures as wrongdoers should neither be able to use reported data to identify registrars that investigate less nor to attack registrars that investigate a lot.

Q6 What are appropriate timelines and thresholds for initiating and concluding the associated domain check?

ISPCP recommends the following as a starting framework for timeline discussions, recognizing that these figures should be informed by operational input from registrars during the PDP:

- Initiation: A pivot investigation should be initiated asap and concluded within a defined window following the registrar's determination that a domain was registered for malicious purposes for example. This timeline should be realistic relative to registrar operational capacity.

- Conclusion: A reasonable upper bound for completing the investigation (not necessarily taking action but reaching a conclusion on the associated domains identified) might be 7 to 14 calendar days, with provisions for extension in complex cases.
- Volume thresholds: The WG should consider whether a minimum scale threshold should apply before the pivot obligation is triggered. For instance, where an investigation identifies only one or two associated domains with no corroborating abuse signals, a full formal pivot investigation may not be warranted. A de minimis threshold would prevent the framework from generating disproportionate overhead for marginal cases.

These parameters should be reviewed periodically as part of the framework's overall effectiveness assessment to ensure they remain appropriate as threat actor tactics evolve.

Q7 What should be mandatory policy vs. best practices vs. registrar discretion?

ISPCP recommends a layered approach that distinguishes between core obligations suitable for mandatory policy and operational details that are better addressed through best practices or registrar-level discretion:

- Mandatory policy obligations: The obligation to initiate an associated domain check when the specified trigger criteria are met; the requirement to document the investigation; the requirement to maintain records of actions taken; and minimum registrant notice and appeals requirements.
- Best practices / guidance: The specific technical tools or data sources used during an investigation; the sequencing of investigative steps; the format of documentation; and communication templates for registrant notice.
- Registrar discretion: The specific internal workflow for conducting investigations; the staffing model used to fulfil the obligation; and the specific action taken in response to investigation findings (subject to the proportionality constraints set by the mandatory policy).

Q8 What metrics will be used to evaluate the policy's effectiveness?

ISPCP recommends that the framework include a defined set of metrics to enable ongoing evaluation of both effectiveness and proportionality. Suggested metrics include:

- Volume metrics: Number of pivot investigations initiated per reporting period; number of associated domains identified; number of domains suspended, transferred, or otherwise actioned as a result.
- Accuracy metrics: Number of appeals filed; number of appeals upheld (indicating a false positive); number of domains reinstated following appeal.
- Impact metrics: Reduction in DNS abuse uptime attributable to pivot investigations; third-party corroboration via abuse intelligence feeds where available.

- Periodic review: The framework should specify a review cycle (e.g., every two years) at which aggregate metrics are assessed and the framework adjusted if evidence of systematic over-enforcement or ineffectiveness is identified.

Q9 How can registrars demonstrate compliance with the obligation?

ISPCP recommends the following mechanisms for demonstrating compliance, bearing in mind the need to balance accountability with operational realism for registrars of different sizes:

- Investigation records: Registrars should maintain contemporaneous records of each pivot investigation, including: the trigger event, the association criteria applied, the domains identified, the steps taken, and the outcome. These records should be retained for a defined period and available for review by ICANN compliance upon request.
- Periodic compliance reporting: Registrars should submit periodic aggregate reports to ICANN Compliance (in a standardized format to be developed by the WG) covering the metrics outlined under Q8.
- ICANN audit rights: ICANN Compliance should have the right to audit registrar compliance on a sample or triggered basis, with audit procedures defined in the implementation guidance accompanying the policy.

3. Impact on Human Rights

ISPCP considers it important that the WG conduct a thorough human rights impact assessment of any proposed framework. Our assessment is that the potential human rights impact of a mandatory pivot obligation is medium to high, depending on how broadly or narrowly the framework is scoped, and that the following groups are most likely to be affected:

- Small businesses and sole traders who register multiple domains for legitimate business purposes, and who may share account or contact data in ways that could superficially resemble the patterns used by malicious actors.
- Journalists, activists, and civil society organizations that register domain portfolios for campaigns, and who may be particularly harmed by suspension of digital infrastructure with little or no notice.
- Resellers and hosting providers whose customers share infrastructure in ways that could create false association signals.

Necessity

ISPCP accepts that some form of pivot obligation may be necessary to address the structural gap in the current RAA regime, which allows threat actors to sustain multi-domain abuse campaigns by losing only one domain at a time. However, necessity should be assessed relative to the least restrictive means of achieving the objective. The WG should consider whether voluntary frameworks, best practice guidance, or contractual incentives could achieve similar results before mandating a universal obligation.

Proportionality

The proportionality of the framework depends critically on the strictness of the trigger threshold, the definition of association, the adequacy of due process protections, and the existence of effective remedies for false positives. A narrowly scoped framework with robust due process protections is more likely to be proportionate than a broad obligation with minimal safeguards. ISPCP urges the WG to treat proportionality as a design constraint, not an afterthought.

Legitimacy

ISPCP considers a well-scoped mandatory pivot obligation to be a legitimate policy intervention provided it is grounded in a technically accurate definition of DNS abuse; transparent in its obligations and compliance requirements; subject to independent oversight; and inclusive of meaningful remedies for affected registrants. Legitimacy also requires that the framework be developed through a genuine multi-stakeholder process which the PDP mechanism is designed to provide rather than unilateral industry or registry action.

4. Impact on the Global Public Interest

ISPCP's assessment is that a well-designed associated domain check framework serves the Global Public Interest by:

- Reducing the operational viability of large-scale DNS abuse campaigns, which cause measurable harm to internet users through phishing, identity theft, malware infection, and financial fraud.
- Improving the overall security and stability of the DNS, a core component of the global internet commons.
- Closing a structural enforcement gap that currently allows sophisticated threat actors to exploit the "one-at-a-time" limitation of the existing RAA regime.
- Protecting Internet users and businesses as customers of commercial entities that are victims of DNS abuse campaigns.

However, ISPCP cautions that the Global Public Interest may be harmed — not served — by a framework that is over-broad, poorly defined, or inadequately protective of legitimate registrant rights. Specifically, the GPI would be negatively impacted if the framework:

- Produces large-scale suspension of legitimate domains through low-confidence association criteria.
- Chills legitimate domain registration activity by creating undue legal risk or uncertainty for registrants.
- Is weaponized to target political, journalistic, or civil society actors under the guise of abuse enforcement.
- Creates compliance burdens disproportionately falling on smaller registrars, reducing market competition and consumer choice in domain registration.

5. Additional Considerations

Narrow Definition of DNS Abuse

ISPCP reiterates the importance of maintaining a narrow, technically grounded definition of DNS abuse throughout this PDP. The five categories recognized in the RAA: malware, botnets, phishing, pharming, and spam as a vector should remain the operative definition.

Content-layer abuse, including fraud, illegal content, or hate speech, is not DNS abuse and should not be drawn into this framework. ICANN's narrow technical mandate and the prohibition of content regulation should be kept in mind and respected,. Expanding the definition would extend registrar obligations well beyond their technical competence, raise serious rule-of-law concerns, and create significant risks for freedom of expression. Additionally, this could constitute a violation of ICANN's Bylaws.

Role of ISPs in the Broader Abuse Mitigation Ecosystem

The ISPCP would like to emphasize that fighting DNS and other types of abuse successfully requires collaboration of the different types of intermediaries. Registries and registrars have the least nuanced and binary tool to deploy, namely to allow for a domain name to resolve or to corrupt its functionality with far-reaching consequences. This should only be used with care and where a proportionality test permits. There are scenarios where e.g. hosting companies are better suited to take action. This is particularly true for cases of compromised domain names, which are not the subject of this PDP, but help illustrate that compromised webspace leading to perpetrators using such webspace for illegal action should be fixed by the hosting company.

The WG should recognize that ISPs and connectivity providers already undertake substantial abuse mitigation activity, including null-routing malicious infrastructure, blocking known command-and-control domains, and cooperating with law enforcement and CERTs. ISPCP would welcome dialogue on how information sharing between registrars and the broader DNS abuse mitigation community could be structured to improve the effectiveness of pivot investigations without creating privacy or legal risks. Various initiatives and projects exist with whom a dialogue could be initiated or intensified, e.g. the Netbeacon Institute, eco's topDNS initiative, the IIF or i2c's Secure Hosting Alliance.

6. Conclusion

ISPCP supports efforts to reduce DNS abuse and appreciates the Working Group's careful, structured approach to this topic. We believe that a well-scoped, proportionate, and operationally realistic associated domain check framework has the potential to meaningfully disrupt large-scale DNS abuse campaigns while respecting the rights of legitimate registrants.

We urge the WG to proceed with precise definitions, clear operational parameters, strong due process protections, robust privacy safeguards, and a realistic assessment of registrar capacity diversity. The framework's ultimate legitimacy and effectiveness will depend on the care taken in these foundational design choices. Getting these design choices right at the outset will be critical to avoiding unintended consequences that could undermine both trust in the DNS and confidence in ICANN's compliance framework.

ISPCP will participate actively in the PDP through its nominated Working Group representatives and looks forward to advancing these positions and engaging constructively on all relevant issues as the deliberations progress. ISPCP also welcomes broader dialogue with ICANN staff and other stakeholder groups on any of the matters raised in this submission.

Internet Service Providers and Connectivity Providers Constituency (ISPCP)

GNSO Constituency | ICANN

Submitted via email to: gnso-secs@icann.org

For inquiries, please contact the ISPCP Chair or designated representative.