ICANN | ISPCP

Internet Service Providers & Connectivity Providers

ISPCP DNSAM PDP1

Summary of Submission

ISPCP supports the DNS Abuse Mitigation PDP 1 Initial Report and the Preliminary Recommendations and Implementation Guidance as a package. ISPCP supports the Leadership Team's proposed Full Consensus designations for all Preliminary Recommendations and Implementation Guidance. ISPCP appreciates that several foundational principles raised in its Early Community Input are reflected in the Initial Report, including the use of actionable evidence, the distinction between maliciously registered and compromised domains, reasonable and proportionate investigation, flexible association criteria, privacy and data minimization, recognition of registrar operational realities, effectiveness review, and demonstrable compliance. ISPCP also wishes to place several implementation-oriented observations on the record. These include the importance of recognizing differences in evidentiary strength among association indicators; avoiding weak or circumstantial indicators being treated as determinative in isolation; maintaining proportionality and attention to false-positive and collateral-impact risks; ensuring implementation remains practical across registrars with different capabilities and business models; considering meaningful effectiveness metrics during future review, including proportionality-related outcomes where appropriately aggregated; and recognizing the value of lawful coordination and information sharing across the broader DNS Abuse mitigation ecosystem. These observations are intended to support effective implementation and future policy review and do not alter ISPCP's support for the Preliminary Recommendations and Implementation Guidance as written.

3. Guided Submission — Individual Mandatory Selections and Rationale

Form Item	Exact ICANN Selection	Proposed ISPCP Rationale
PR1	**Support Recommendation as written**	ISPCP supports Preliminary Recommendation 1 as written. ISPCP welcomes the focus on actionable evidence and the explicit distinction between maliciously registered domains and legitimate domains that have subsequently been compromised.

IG1.1	**Support Implementation Guidance as written**	ISPCP supports Preliminary Implementation Guidance 1.1 as written. The guidance appropriately recognizes that abuse evidence may be current, recent, intermittent or recurring and that reports should contain sufficient information to support an investigation.
PR2	**Support Recommendation as written**	ISPCP supports Preliminary Recommendation 2 as written. The requirement for a reasonable investigation provides an appropriate foundation while avoiding a rigid investigative methodology.
PR3	**Support Recommendation as written**	ISPCP supports Preliminary Recommendation 3 as written. The emphasis on information reasonably accessible in the ordinary course of business, proportionality and differing registrar capabilities is consistent with ISPCP's Early Community Input.
IG3.1	**Support Implementation Guidance as written**	ISPCP supports Preliminary Implementation Guidance 3.1 as written. The recognition of reseller operating models and the practical allocation of investigative steps is useful for implementation.
PR4	**Support Recommendation as written**	ISPCP supports Preliminary Recommendation 4 as written. The flexible, non-exhaustive approach to determining association is preferable to a rigid checklist and appropriately leaves room for registrar judgment.
IG4.1	**Support Implementation Guidance as written**	ISPCP supports Preliminary Implementation Guidance 4.1 as written. The guidance appropriately identifies multiple possible indicators while recognizing that their relevance depends on the circumstances.
PR5	**Support Recommendation as written**	ISPCP supports Preliminary Recommendation 5 as written. The safeguards concerning applicable law, data minimization, proportionality and protection of Registered Name Holders appropriately address privacy and over-association concerns.
IG5.1	**Support Implementation Guidance as written**	ISPCP supports Preliminary Implementation Guidance 5.1 as written. The guidance provides useful clarification concerning lawful information use and sharing, retention, proportionality and protection of Registered Name Holders.
PR6	**Support Recommendation as written**	ISPCP supports Preliminary Recommendation 6 as written. The approach appropriately recognizes prompt action while allowing severity, immediacy, scale, complexity, collateral impact and operational realities to inform implementation.
IG6.1	**Support Implementation Guidance as written**	ISPCP supports Preliminary Implementation Guidance 6.1 as written. The guidance provides a practical framework for applying the timeline while recognizing circumstances that may affect the investigation.
PR7	**Support Recommendation as written**	ISPCP supports Preliminary Recommendation 7 as written. ISPCP welcomes the two-year effectiveness review and the use of limited aggregated data to assess whether the policy is achieving its intended outcomes.

PR8	**Support Recommendation as written**	ISPCP supports Preliminary Recommendation 8 as written. The documentation requirements provide a practical means of demonstrating that an investigation was undertaken and that decisions were reasonable and proportionate.

4. Rationale Comment Fields — Proposed Text

Form Rationale Field	Proposed ISPCP Text
PR1 + IG1.1	ISPCP has no additional objection to the rationales for PR1 and IG1.1. ISPCP welcomes the emphasis on actionable evidence, the distinction between malicious registration and compromise, and recognition that abuse evidence may be intermittent or recurring.
PR2–PR4 + IG3.1 + IG4.1	ISPCP supports the rationales and their overall approach. In particular, the emphasis on reasonable investigation, information reasonably accessible in ordinary operations, proportionality, registrar capabilities, reseller models and flexible association criteria is consistent with ISPCP's Early Community Input.
PR5 + IG5.1	ISPCP supports the rationale, particularly the treatment of applicable law, data minimization, proportionality, protection of Registered Name Holders, lawful information use/sharing and retention.
PR6 + IG6.1	ISPCP supports the rationale and welcomes the recognition that severity, immediacy, scale, complexity, collateral impact and operational realities may affect how timelines are applied.
PR7	ISPCP supports the rationale and welcomes the two-year effectiveness review and aggregated-data approach. ISPCP's additional observation concerning effectiveness metrics is set out in the Other Comments section below.
PR8	ISPCP supports the rationale and welcomes the focus on contemporaneous documentation sufficient to demonstrate the steps taken, information considered, resulting action and reasonableness/proportionality.

5. Comprehensive Impact Assessments — Proposed Comments

Impact Assessment	Proposed ISPCP Comment

Human Rights Impact Assessment	ISPCP supports the overall approach and welcomes the attention to proportionality, privacy, legitimate registrant interests and the potential for collateral impact. ISPCP encourages implementation and future effectiveness review to remain attentive to false-positive risks and to proportionate mechanisms for addressing erroneous association.
Global Public Interest Checklist	ISPCP supports the overall assessment. Effective DNS Abuse mitigation is an important public-interest objective, while implementation should remain proportionate, evidence-based and mindful of operational diversity across the registrar ecosystem.
Data Privacy Considerations	ISPCP supports the emphasis on applicable data protection law, data minimization and use of information reasonably necessary for the investigation. These safeguards should remain central to implementation and future review.
ICANN Consensus Policies	ISPCP supports the assessment and the policy approach as presented. ISPCP notes the importance of maintaining the defined scope of DNS Abuse and avoiding unintended expansion into broader content regulation or areas outside the contractual policy framework.

6. Other Comments — Proposed ISPCP Text

The following section is intended for the form's optional “Other Comments” field. It is deliberately separated from the individual guided selections so that the observations below do not alter ISPCP's support for the Recommendations and Implementation Guidance as written.

Evidentiary strength of association indicators

ISPCP's Early Community Input highlighted that association indicators can carry different levels of evidentiary strength. ISPCP supports the flexible approach in the Initial Report and encourages implementation to recognize that weaker or circumstantial indicators should not, in isolation, be treated as determinative.

Proportionality and false-positive risk

ISPCP encourages continued attention to proportionality, over-association and collateral impact during implementation and effectiveness review. Future assessment should, where feasible and appropriately aggregated, consider evidence of false positives, appeals or reinstatement as indicators of whether the framework is operating proportionately.

Registrar operational diversity

ISPCP welcomes the recognition of differing registrar capabilities and business models. Implementation should remain practical and proportionate across registrars of different sizes, technical environments and operational structures.

Effectiveness metrics

ISPCP supports the proposed two-year review and suggests that future effectiveness assessment consider not only volumes and actions, but also qualitative indicators of accuracy, proportionality and unintended impact, subject to privacy and data-minimization safeguards.

Broader DNS Abuse mitigation ecosystem

ISPCP's Early Community Input recognized that effective DNS Abuse mitigation involves a broader ecosystem beyond registrars and registries, including ISPs, hosting providers, CERTs and other relevant actors. Where appropriate and lawful, information sharing and coordination among these actors can complement ADC processes. In addition it’s important to mention AI role in DNS abuse detection and mitigation under the respect of ethics & privacy. It’s about integrating the voice of Infrastructure and AI Ethics.

Scope of DNS Abuse

ISPCP supports maintaining the narrow, contractual scope of DNS Abuse and avoiding unintended expansion into broader content regulation. The policy should remain focused on the DNS Abuse categories and contractual responsibilities within its defined scope.

_____XXXXXXXXXXXXXXXXXX_____