NCSG Positions on DNS Abuse in ICANN Policy 2018–March 2026

Executive summary

Across 2018–March 2026, the Noncommercial Stakeholder Group (NCSG) has argued for a **narrow, DNS-layer definition of "DNS Abuse"**, strict adherence to **ICANN's technical mission**, and strong **human-rights and due-process safeguards** whenever abuse mitigation can result in domain suspension or, takedown, disclosure of registrant data, and strong human-rights and due-process safeguards for any mitigation action. This long-running throughline appears consistently in NCSG submissions on review-team work (notably the Competition, Consumer Trust and Consumer Choice Review, and SSR2), its opposition to "mission creep" and content regulation, and its later framing of DNS-abuse mitigation as requiring **qualitative success measures** (not just counts of domains disrupted). *[1]*

The most visible inflection in the record (2024–2026) is NCSG's move from general mission/due-process critiques to a **repeatable "human rights impact assessment (HRIA)" workflow** designed to be used by the community and by PDP working groups. This includes tool-building such as the "DNS & IHRL Cheat Sheet," and explicit calls for PDP charters and outcomes to embed **necessity/proportionality**, **minimization of impact on innocent domain** , and **accessible remedy/recourse** for registrants. *[2]*

On substance, NCSG's most sustained disagreements with other parts of the community have centered on: (a) **expanding "DNS Abuse" beyond technical security harms into "content abuse," intellectual property, or "illegal content" questions**; (b) **algorithmic/predictive or otherwise "proactive monitoring" proposals** that NCSG characterizes as surveillance- and censorship-enabling; and (c) **"associated domain checks" (ADC)** and identity-verification measures that can scale harm from one flagged domain to many domains or to identifiable registrants. NCSG does not reject associated-domain investigations outright, but conditions acceptability on strict thresholds, evidence standards, and procedural protections. *[3]*

Community outcomes partially reflect NCSG's framing, but not fully. The NCSG led some work via the CCWP-HR, such as creating an initial HRIA framework, and longstanding advocacy to create a definition of DNS abuse. This set the stage for the contractual amendments, which not only defined DNS abuse for the first time within the ICANN context but also compelled mitigation action. With these changes, the PDPs on mitigation could kick off. [4] The 2024 contractual amendments created enforceable obligations to mitigate a defined set of technical DNS abuse categories and explicitly referenced "collateral damage," aligning in part with NCSG's concerns about overbroad disruption. *[4]* However, NCSG objected to parts of the amendments package especially the definitional and framing shift from contract language like

"Security Threat"/"DNS-related abuse" to "DNS Abuse," and the inclusion of "spam (as a delivery mechanism)" in the definition positions that did not prevail in the final contract text. *[5]*

Looking forward (as of March 26, 2026), NCSG has concentrated on **PDP charter safeguards and implementation constraints** for ADC and API-gating work (DNS Abuse Mitigation "PDP1"), and to continue pushing for *separate, explicit* community mechanisms for registrant **notification, challenge, and redress**, a "rights infrastructure" that NCSG argues is missing relative to the gravity of mitigation actions. *[6]* We're looking ahead to future PDP topics, with a priority topic being registrant access to recourse and remedy (this was identified in the GNSO small team's gap analysis but was ultimately not taken up as a priority item in the recommendations to the GNSO council). [6]

Methods and source base

This analysis prioritizes **primary materials** where NCSG speaks in an official capacity: public comments submitted under ICANN public-comment proceedings; statements delivered to the Generic Names Supporting Organization *[7]* Council record; and meeting transcripts/minutes where NCSG representatives explain positions. It also uses core process documents (Small Team reports, Issue Reports, charters) and contract/advisory texts that define the operative DNS-abuse obligations and enforcement expectations. *[8]*

In addition, the analysis is informed by selected civil society research outputs and expert commentary that engage with ICANN processes and DNS abuse from a digital rights perspective. These sources provide contextual insight into human rights implications, transparency challenges, and governance trade-offs, complementing NCSG's positions without being treated as formal NCSG policy.

Examples include work by organizations such as DigitalMedusa, ARTICLE 19 and the Electronic Frontier Foundation, as well as independent research initiatives examining ICANN's handling of DNS abuse and human rights considerations. [8][8][8]

Internal constituency "signals" were triangulated through publicly accessible mailing-list archives, including a message circulated in a dedicated DNS-abuse working-group list describing action points (mapping definitions and drafting a position paper). *[9]* A small amount of additional internal context comes from a publicly visible mirror of a message forwarded to a related listserv about DNS-abuse discussions (useful for chronology, but not a formal position). *[10]*

A note on mailing-list citations and individual attribution: this analysis draws on publicly accessible mailing-list archives only to establish chronology and to show that a given topic had reached the NCSG community agenda by a particular date. These citations are not intended to attribute institutional positions to individual contributors, whose messages reflect participation in

ongoing deliberation rather than adopted NCSG stances. Citing specific authors by name in a document of this kind carries the risk of conflating personal initiative with group consensus, and may generate territorial responses within the community. Accordingly, this document treats named individuals in mailing-list sources as contextual markers only, and relies on formal public comment submissions, GNSO Council statements, and officially adopted resolutions as the authoritative record of NCSG positions. Future versions of this analysis should apply the same standard consistently.

DNS Abuse at ICANN

Within ICANN's contracted-party framework, "DNS Abuse" is treated as **DNS-layer security harms**, malware, botnets, phishing, pharming, and spam where spam is a delivery mechanism for the other forms. In the 2024 global amendment to the Registrar Accreditation Agreement, the definition is embedded directly in the contract and explicitly tied to an SSAC report definition, and registrars must take "appropriate mitigation action(s)" when they have "actionable evidence," while accounting for the "possibility of associated collateral damage." *[4]*

The enforcement and implementation context matters to NCSG's positions. ICANN's compliance advisory explains that compliance determinations are evidence-driven and that mitigation actions can vary; crucially, it also frames the registrar/registry roles as distinct, and situates the obligations in a narrow focus on domains "used as vehicles or mechanisms for DNS Abuse." *[12]* ICANN's DNS Abuse Mitigation Program page likewise emphasizes a focus on DNS-level activities and notes that the bylaws prohibit ICANN from imposing rules on content/services except in narrow circumstances. *[13]* These "scope constraints" are repeatedly invoked by NCSG over the years as guardrails against expanding DNS abuse into content control or more generalized law-enforcement objectives. *[14]*

Two technical/policy vectors are especially important for 2024–2026:

- **High-volume registration tooling and API access**: The INFERMAL research program commissioned by ICANN org systematically examined drivers of malicious registrations and treated API offerings, bulk-search features, discounts, and proactive verification as measurable variables. It discusses how automation using APIs can enable large-scale acquisition of inexpensive domains and notes changes like restricting certain API features to accounts with larger portfolios (used as friction). *[15]*

- **Associated Domain Checks (ADC)**: The core idea is to require or standardize registrar investigations that "pivot" from one confirmed abusive domain to other domains linked by account, email, payment, or other identifiers, an approach aimed at disrupting campaigns faster than one-domain-at-a-time mitigation. The Final Issue Report and draft charter language for PDP1 treat ADC as "priority" policy work,

explicitly raising questions about triggers, definition of "association," evidence, timelines, and privacy safeguards. [16]

Chronological analysis of NCSG positions 2018–March 2026

2018: Mission-limits framing and early "abuse = content risk" warnings

In its comment on the CCT Review Team final report, NCSG repeatedly warns that "abuse" is often undefined in community discussions and that treating "abuse" as content/speech can force ICANN toward content monitoring. NCSG argues that ICANN's bylaws enshrine a narrow technical mission and that recommendations pulling ICANN into "police of the Internet" roles should be rejected. [17] This is an early articulation of a pattern that persists through 2026: *the more ambiguous or expansive the term "abuse," the more NCSG emphasizes mission creep and human-rights/censorship risk.* [18]

2019: The Internal salience increases amid GAC attention

A widely forwarded message from the then NCSG chair, Stephanie Perrin [19] encouraged members to follow a DNS abuse webinar and to review Governmental Advisory Committee [20] correspondence, describing DNS abuse as an "important issue" and a focus at an upcoming ICANN meeting. While not a formal policy statement, it is an observable marker that DNS abuse had become a strategic priority inside NCSG's community space. [10]

2020–2021: SSR2 review cycle as a major "scope" battleground

In NCSG's comment on the SSR2(Second Security, Stability, and Resiliency Review Team - an ICANN accountability review process mandated under ICANN's bylaws to evaluate how effectively ICANN ensures the security, stability, and resiliency of the Domain Name System, including its approach to DNS abuse and related mitigation mechanisms) draft report (March 2020), NCSG objects to a perceived broadening of ICANN's scope and to using DNS-abuse measurement/reporting as a pathway to punitive auditing rather than research; it stresses that the purpose and interpretation of programs like DAAR (Domain Abuse Activity Reporting - an ICANN initiative that aggregates and publishes data on DNS abuse trends across gTLDs using multiple reputation data sources; while widely used in policy discussions, its methodology and interpretation have been subject to debate within the community, including by NCSG, particularly regarding data accuracy, bias, and policy applicability) should not be transformed into a "punishment mechanism." [21]

In NCSG's SSR2 Final Report comment (April 2021), NCSG's position is even more explicit: it calls it "imperative" to keep ICANN's mission technical and the definition of DNS abuse limited to technical issues; it rejects the SSR2 annex definition that includes child exploitation, intellectual property infringement, and fraud, and labels such a definition "very objectionable." [22]

This period is an inflection point because NCSG's "anti-mission creep" stance is no longer only

about the next round of gTLDs or consumer trust; it becomes directly tied to *how DNS abuse is defined and operationalized across ICANN workstreams.* [23]

2021: Internal constituency organization around DNS-abuse policy

A public message in the NCSG DNS-abuse working-group list [24] lays out action points that include confirming coordination with a Contracted Party House working group, mapping "working definitions" of DNS abuse across the community, and beginning a position paper on "NCSG's DNS abuse working definition, concerns and process." [9] This is significant because it shows NCSG moving from reactive comments (on others' reports) to proactively setting out a coherent definition/process agenda. [9]

2022: The GNSO DNS Abuse Small Team formalizes a "lifecycle" frame and surfaces KYC as a policy concept.

The 2022 DNS Abuse Small Team report to the GNSO Council explicitly frames DNS abuse as a long-standing topic and organizes potential gaps into a "lifecycle" with phases (prevention, reporting, actionable complaints, action, enforcement). [25] This lifecycle model becomes a recurring scaffold in later work (the 2025 reconvened Small Team and the 2025 Issue Report). [26]

Notably, the 2022 report includes "Know Your Customer (KYC)" as a topic that could play a role in mitigating malicious bulk registrations. [25] Even though the report is not an NCSG document, it matters because many later NCSG interventions can be read as a rights-based response to exactly these classes of proposals (identity/verification, portfolio-based mitigation, proactive checks). [27]

2023: Contract amendments debate – NCSG's objections to definitional framing and "spam"

In its public comment on the proposed amendments to the Base gTLD Registry Agreement and Registrar Accreditation Agreement, NCSG opposes replacing earlier contract terms ("Security threat"/"DNS-related abuse") with "DNS Abuse," warning that "DNS Abuse" is "politicized" and more susceptible to expansive interpretation (including content) in the future. NCSG also argues against including "spam" in the definition because spam is an email-layer problem rather than a DNS-layer abuse, and it urges ICANN to keep DNS abuse tightly scoped. [28] However, NCSG was supportive of having a definition of 'DNS-related abuse' to prevent anything from being called 'abuse'.

This is a critical moment: NCSG treats the label "DNS Abuse" as not merely semantic, but as a pathway to future demands for content takedowns or non-technical enforcement. [29]

2024: Global amendments take effect; operational concepts "actionable evidence" and "collateral damage" become central

The adopted 2024 RAA amendment codifies the DNS Abuse definition (including spam-as-vector) and requires prompt mitigation actions when registrars have actionable

evidence, while explicitly considering collateral damage. [30] ICANN's compliance advisory emphasizes that evidence must be actionable and that contracted parties must be able to show compliance when investigated. [12]

From NCSG's perspective, the inclusion of "collateral damage" language is aligned with its long-standing concern about overbroad disruption, even as the definitional "DNS Abuse" label and spam inclusion reflect NCSG's earlier objections not carrying the day. [31]

Late 2024–2025: Human-rights tooling becomes a distinct NCSG workstream

The "DNS & IHRL Cheat Sheet" explicitly maps DNS-abuse mitigation obligations and typical mitigation actions to rights (privacy, expression, association, access to remedy/due process), and lists relevant instruments such as the UDHR, ICCPR, and UN Guiding Principles on Business and Human Rights, among others. [32]

In a March 2025 transcript of a GAC session featuring NCSG outreach, Rafik Dammak [33] and Farzaneh Badii and Michaela Shapiro [34] describe DNS-abuse HRIA work as a response to a perceived overemphasis on quantitative success (counts of mitigated names) and as a way to surface downstream harms from hasty takedowns or improper data disclosure. [35]

Two substantive "rights positions" appear crisply in NCSG's 2025 public comment record:

- **Identity verification vs. "contactability"**: NCSG argues that "data accuracy" should mean registrants are contactable, not that their identity is verified, because identity checks can endanger activists and violate privacy (with risks such as surveillance, arrest, or threats to life). [36]

- **Proactive monitoring/predictive algorithms**: NCSG frames broad proactive monitoring as a "staggering system of surveillance" that can chill expression and be co-opted by governments seeking to suppress speech; it urges strong scoping limits and safeguards. [37]

August–December 2025: Associated Domain Checks become the focal point of NCSG divergence

When the Small Team work crystallized into prospective policy topics, NCSG formally approved the Small Team report but recorded concern about associated domain checks. It warned that ADC can enable broad or arbitrary enforcement absent safeguards, and emphasized due process at registration, detection, and enforcement stages—explicitly noting that registrants are "not inherently criminals." [38]

In its October 15, 2025 comment on the preliminary issue report, NCSG's position becomes more operational:

- It does not deny that registrars may sometimes need to examine related domains to disrupt networks, but insists such investigations be grounded in **clear evidence**, not profiling, and must avoid "undue surveillance." *[39]*

- It demands PDP outcomes include **clear due-process elements** and accessible mechanisms for remedy/challenge. *[40]*

- It criticizes "takedown" dynamics when DNS-level mitigation can effectively remove lawful content from the Internet, offering a concrete example of how a registry serving a public-interest nonprofit could be compelled to take down an entire domain if broad definitions were applied. *[41]*

December 2025–January 2026: "PDP1" takes a chartered shape; NCSG presses for safeguards and stronger research base

The Final Issue Report (December 4, 2025) explicitly incorporates human-rights considerations and states that an HRIA will be included "by default" in the PDP. It also proposes splitting work into more targeted PDPs and includes detailed scoping questions for associated-domain checks and unrestricted API access. *[42]*

In an NCSG statement for the record (December 15, 2025), NCSG reiterates that ADC poses human-rights and profiling risks; criticizes the Issue Report for not adequately incorporating NCSG comments on transparency, due diligence, and remedy; and calls for independent research designed in consultation with the community to avoid overreliance on external studies that may not capture affected registrant perspectives. *[43]*

By mid-January 2026, the GNSO Council adopted a PDP charter for DNS Abuse Mitigation PDP1 (as documented in the Council motion record). *[44]* As of March 2026, external observers describe accelerated timelines and continued contention around the pace and safeguards of ADC work, with NCSG frequently grouped with registrars as urging adequate time and public-comment scrutiny. *[45]*

Comparing NCSG positions to process outcomes

NCSG's influence is most visible where the community has **institutionalized "rights-aware" process hooks** rather than adopting NCSG's most restrictive substantive positions.

The contract amendments and compliance guidance partly match NCSG's long-running concerns about overbroad disruption: the 2024 RAA text and related compliance advisory repeatedly stress "actionable evidence," "reasonable" actions, and "collateral damage." *[4]* The later policy roadmap likewise embeds human-rights considerations: the Final Issue Report notes HRIA inclusion, expects working groups to consider severity/affected groups, and includes privacy and data-protection frameworks as explicit charter considerations. *[46]*

Where NCSG's positions did not prevail, the strongest examples are definitional and scope-related. NCSG opposed shifting contractual framing to "DNS Abuse" and opposed incorporating spam into the definition; the final RAA amendment did both. *[5]* Similarly, while NCSG has argued consistently against broad "abuse" language that could reach content regulation, the broader community routinely continues to debate expansion candidates, forcing NCSG to repeatedly reassert mission limits in public comments and statements. *[47]*

In ADC and API gating, NCSG's impact is currently best understood as **shaping constraints** rather than rejecting the track outright. NCSG statements (Aug 2025 and Oct 2025) position ADC as conditionally permissible only with robust procedural protections, evidence thresholds, and recourse—and the PDP charter questions and Issue Report framing foreground exactly those dimensions (triggers, evidence, privacy safeguards, exclusions for compromised domains, and HRIA/DPIA considerations). *[48]*

Strategic recommendations for addressing the definitional and scope gap

Shift from defensive critique to affirmative counter-drafting. Across the 2023 contract amendments and earlier SSR2 debates, NCSG consistently identified what it opposed but had limited success embedding alternative language in final texts. The community repeatedly absorbed NCSG's objections without adopting NCSG's preferred framing, in part because objections without drafting alternatives are easier to note and set aside than to incorporate. In PDP1 working-group settings, NCSG should prioritize developing specific, usable definitional language for ADC triggers, evidence thresholds, scope exclusions, and recourse mechanisms that can be introduced as draft charter or policy text. Affirmative proposals occupy negotiating space that critiques alone do not.

Build and formalise partial coalitions before key working-group votes. NCSG's scope and safeguard positions on ADC and API gating track closely with Contracted Party House concerns about operationalizability, evidence standards, and procedural fairness. Formalising coordination with CPH representatives within PDP1—particularly registrar-side representatives who have their own compliance-cost incentives to support high evidence thresholds -- would give NCSG's positions greater weight in working-group deliberations than NCSG can achieve alone. Similarly, ALAC's alignment on due-process and remedy arguments creates a basis for joint statements or coordinated submissions that can anchor the working-group record on registrant-protection questions.

Engage the GAC's framing proactively rather than reactively. The ICANN82 transcript demonstrates that GAC members are receptive to rights-based arguments when grounded in governance accountability and international human rights obligations. NCSG's HRIA tooling and the DNS & IHRL Cheat Sheet are well-suited for this engagement, but their deployment has so far been episodic. A more systematic approach including written NCSG input into GAC advice-assessment cycles, and deliberate framing of NCSG positions in language that resonates

with government representatives' own human rights treaty obligations could reduce the gap between GAC and NCSG positions on proportionality, even where full alignment is not achievable.

Overview of Other Stakeholder Positions on DNS Abuse

Understanding where NCSG's positions stand relative to the broader community requires mapping the recurring postures of the Governmental Advisory Committee, the principal GNSO constituencies that most frequently oppose NCSG's framing, and the advisory bodies that serve as partial or conditional allies. This overview is not exhaustive but is intended to identify the key actors whose positions most directly shape the environment in which NCSG must operate.

Governmental Advisory Committee (GAC). The GAC has been one of the most consistent forces pushing for expansive DNS abuse obligations, and its posture has grown more operationally specific over time. Across GAC Communiqués from ICANN61 (2018) through ICANN82 (2025), the GAC has called for clearer and more uniformly enforced definitions, improved registrar and registry responsiveness to abuse reports, and enhanced ICANN accountability over contracted-party compliance. The GAC's framing tends to treat DNS abuse as a public-policy and consumer-protection concern that cannot be reduced to a purely technical remit, a view that directly tensions NCSG's mission-limits argument. The GAC has in several instances signalled receptiveness to including content-adjacent categories (such as fraud and consumer harm) within actionable abuse, and it has expressed support for proactive monitoring measures in terms that NCSG would characterise as disproportionate. At the same time, the March 2025 ICANN82 GAC–NCSG session demonstrated that GAC representatives are not uniformly hostile to rights-based framing; several GAC members engaged constructively with NCSG's HRIA arguments when those arguments were presented in terms of state obligations under international human rights law and governance accountability. The GAC is therefore best understood as a structurally expansive counterweight to NCSG's scope-boundary positions, but not an entirely closed audience for process-rights and proportionality arguments.

Intellectual Property Constituency (IPC) and Business Constituency (BC). Within the GNSO, the IPC and BC have been the most persistent advocates for a broad DNS abuse definition that reaches intellectual property infringement, fraudulent commercial activity, and consumer harm. The IPC has argued across multiple GNSO Council deliberations and working-group contexts that limiting DNS abuse to purely technical categories ignores the downstream harms that domain infrastructure enables, and it has consistently opposed definitional scoping that would remove IP-related abuse from registrar and registry obligation. The BC has similarly supported proactive monitoring mandates and enhanced identity-verification requirements as tools to deter bulk malicious registrations. Both constituencies frequently align with each other and with GAC advice when pushing for obligations that NCSG characterises as mission creep or overreach. In PDP1 working-group

deliberations, IPC and BC are likely to be the primary adversarial voices inside the GNSO against NCSG's scope and safeguard arguments. NCSG should anticipate IPC and BC resistance especially on definitional questions (ADC triggers, evidence thresholds) and identity-verification language, and should plan engagement accordingly.

At-Large Advisory Committee (ALAC). ALAC occupies a more ambiguous position relative to NCSG. It shares NCSG's structural concern for individual Internet users and has been sympathetic in multiple forums to arguments about collateral damage, overblocking, and the importance of registrant-accessible resource mechanisms. ALAC has echoed NCSG's call for evidence-based, proportionate mitigation in several working-group and advisory contexts. However, ALAC also represents users who are victims of phishing, malware, and fraudulent domains, and it has in some contexts supported broader notification and measurement obligations than NCSG endorses. This makes ALAC a partial and conditional ally: NCSG should expect ALAC support on due-process, remedy, and proportionality arguments, but not necessarily on definitional scope questions or opposition to proactive monitoring requirements. Targeted coordination with ALAC particularly on the registrant-recourse gap that both bodies have flagged represents a realistic coalition opportunity.

Security and Stability Advisory Committee (SSAC). SSAC's role has been primarily technical and definitional. Its DNS abuse taxonomy embedded in SAC115 and predecessor reports became the foundation for the 2024 RAA contractual definition, which NCSG only partially endorsed. SSAC generally defines DNS abuse narrowly in technical terms (malware, botnets, phishing, pharming, spam-as-vector), which aligns with NCSG's preferred scope more closely than IPC or GAC positions do. However, SSAC's framing is operational and security-oriented rather than rights-oriented, and it has supported measurement and reporting programs including DAAR that NCSG has cautioned against transforming into punitive or surveillance mechanisms. SSAC is therefore best understood as a technical ally on scope questions, and a useful co-reference for NCSG when defending narrow definitions against IPC/BC expansion arguments, but not a reliable ally on process-rights, HRIA, or anti-surveillance positions.

Strengths, weaknesses, and likely trajectories

NCSG's strongest contribution is a **coherent governance theory**: DNS-abuse mitigation must stay inside a narrow DNS-layer remit, must not drift into content policing, and must incorporate rights safeguards proportionate to the power of the remedies (suspension, takedown, disclosure). That theory has been consistent from at least the 2018–2021 review-team comment cycles to the 2025–2026 PDP era, and it has matured into practical tools (cheat sheets, scenario-based HRIA thinking) that make the argument more implementable in PDP working groups. *[49]*

NCSG's principal weakness is not conceptual but structural: it often lacks the same access to large-scale operational data and measurement programs as contracted parties, security firms, or

specialized institutes, and NCSG itself points out that external reports frequently do not incorporate registrant interviews or the perspectives of those most likely to be harmed by false positives or overbroad mitigation. *[50]* This can create an asymmetry: "evidence" in the process tends to mean abuse-volume metrics, registrar/TLD feature studies, and compliance case counts forms of evidence that may underrepresent experienced harms like chilling effects, discriminatory enforcement, or remedy gaps. *[51]*

This evidence asymmetry is not incidental, it reflects a structural feature of how ICANN processes aggregate information. Working-group deliberations, Issue Reports, and compliance assessments naturally draw on data that contracted parties and ICANN org generate: registrar compliance records, domain abuse volume datasets, TLD-level reporting, and commissioned quantitative research such as the INFERMAL program. These are the inputs that are readily available, standardised, and citable. Rights-based harms, chilling effects on registrant behaviour, over-suspension of legitimate domains, discriminatory enforcement patterns, failure of recourse mechanisms are not captured in these datasets. They require qualitative methods, registrant interviews, and sustained engagement with affected communities that no current ICANN-funded research program is designed to produce. NCSG has correctly identified this gap in its December 2025 statement for the record, but identification is not sufficient. Closing the gap requires NCSG to advocate within PDP1 charter negotiations for research design requirements that include affected-registrant perspectives, and to build relationships with academic and civil-society research institutions capable of producing the kind of qualitative evidence that can stand alongside abuse-volume metrics in working-group deliberations. Without that, the structural evidence asymmetry will continue to shape policy outcomes independently of the formal strength of NCSG's legal and governance arguments.

Trajectory (March 2026 outlook): NCSG is likely to prioritize three linked goals. First, ensure ADC policy (if adopted) is **non-automated**, evidence-based, and bounded to malicious registrations with clear carve-outs and strong registrant protections. *[52]* Second, push for standardized **notice, transparency reporting, and recourse** mechanisms as either part of PDP outputs or as parallel best-practice work because NCSG's core critique is that the ability to disrupt at scale is outpacing the rights infrastructure to correct mistakes. *[53]* Third, continue institutionalizing HRIA practice inside ICANN procedures (including GAC advice-assessment and GNSO PDP workflows), as reflected in meeting minutes documenting NCSG–GAC coordination and claims that HRIA requirements will be applied across PDPs. *[54]*

Timeline, topic matrix, and visuals

Timeline table of key NCSG documents and policy milestones

Date	Document / venue	What NCSG said or did	Why it mattered (driver / inflection)
Nov 27, 2018	NCSG comment on CCT Final Report & Recommendations	Warned that "abuse" language easily becomes content regulation; urged strict adherence to ICANN's limited technical mission and rejection of "policeman of the Internet" logic. *[17]*	Established the mission-limits and content-regulation risk frame that later becomes central to DNS-abuse debates. *[17]*
Oct 1, 2019	Forwarded note (internal signal)	Encouraged attention to DNS-abuse webinar and GAC correspondence, calling DNS abuse "an important issue." *[10]*	Shows DNS abuse becoming a strategic focus inside NCSG's community space. *[10]*
Mar 2020	NCSG public comment on SSR2 Draft Report	Critiqued scope expansion and objected to turning abuse reporting/measurement into punitive targeting; emphasized mission discipline. *[21]*	DNS-abuse definition becomes explicitly tied to "mission creep" concerns. *[21]*
Apr 7, 2021	NCSG public comment on SSR2 Final Report	Rejected broad definitions including IP/fraud/child exploitation; insisted DNS abuse remain technical and within ICANN remit. *[22]*	One of the clearest NCSG statements opposing expansive DNS-abuse definitions; foreshadows later objections to content-like "abuse" expansions. *[22]*

Feb 4, 2021	NCSG DNS-abuse working-group message	Action points: map definitions across community; draft position paper; coordinate with contracted parties; reference CPH definition. *[55]*	Marks internal organization toward a structured "NCSG definition + safeguards + process" approach. *[9]*
Oct 7, 2022	GNSO DNS Abuse Small Team report (Phase approach; KYC appears)	(Not an NCSG doc) but a key process input that surfaced KYC, lifecycle framing, and "gaps" that later drove PDP work. *[25]*	Created the lifecycle taxonomy and policy "gap" scaffolding later reused in 2025–2026. *[25]*
Jul 2023	NCSG public comment on proposed RA/RAA DNS-abuse amendments	Opposed "DNS Abuse" label replacing "Security threat/DNS-related abuse"; objected to including spam; warned of politicization and expansion risk. *[56]*	Directly contested the contract framing that ultimately governed DNS-abuse enforcement from April 2024 onward. *[30]*
Apr 5, 2024	RAA global amendment effective date	Contracts required mitigation on actionable evidence; defined DNS abuse (including spam as vector); recognized collateral damage. *[4]*	Converted debate into enforceable obligations and made "evidence," mitigation discretion, and collateral damage central features. *[57]*
Nov 2024	DNS & IHRL Cheat Sheet	Mapped DNS-abuse mitigation to rights and remedy; cited international human rights instruments (UDHR, ICCPR, UNGP). *[32]*	Tool-building phase: operationalizes NCSG's "rights + due process" arguments into a reusable assessment aid. *[32]*

Mar 9, 2025	GAC–NCSG transcript (ICANN82)	NCSG articulated HRIA as a way to add qualitative success measures and prevent hasty, rights-impacting takedowns/data disclosure. *[35]*	Shows NCSG taking HRIA arguments into cross-community dialogue and tying them to bylaw commitments. *[35]*
Aug 14, 2025	NCSG statement on DNS Abuse Small Team Report	Approved report but formally opposed ADC absent robust safeguards; emphasized due process and presumption that registrants aren't criminals. *[38]*	ADC becomes the central NCSG "red line" issue and leads into the Issue Report/PDP pipeline. *[58]*
Oct 15, 2025	NCSG comment on Preliminary Issue Report for DNS Abuse PDP	Called for evidence-based ADC, no profiling/surveillance, contactability not identity verification, and strong remedy mechanisms. *[59]*	Consolidates NCSG's mature "rights + safeguards + scope" framework for the upcoming PDPs. *[60]*
Dec 4, 2025	Final Issue Report on DNS Abuse Mitigation	Report states HRIA included by default; proposes targeted PDPs; details ADC and API questions and safeguards. *[42]*	Institutionalizes HRIA expectation and sets the formal scope of policy work. *[61]*
Dec 15, 2025	NCSG statement for the record on DNS Abuse Mitigation PDPs motion NCSG position paper on DNS abuse	Reiterated ADC human-rights/profiling risk; criticized insufficient attention to transparency/due diligence/remedy; called for independent research co-designed with community. *[43]*	Signals NCSG's bargaining position heading into chartering and early WG work. *[62]*

Jan 15, 2026	GNSO Council motion adopting PDP charter	Council adopts DNS Abuse Mitigation PDP1 charter (per motion record). *[44]*	Transition from scoping/issue report to active policy development where NCSG's safeguards agenda will be tested. *[63]*

Topic matrix: NCSG positions by recurring policy dimension

Topic	NCSG position (as evidenced 2018–2026)	Practical implication for DNS-abuse mitigation policy
Scope boundary	Keep DNS-abuse work within ICANN's technical remit; resist content regulation and expansion of "abuse" to IP/illegal content. *[64]*	Policies should define DNS abuse narrowly and avoid embedding content judgments or generalized illegality enforcement. *[65]*
Definition discipline	Opposed shifting contract terminology to "DNS Abuse" and opposed including spam; fears politicization and future expansion. *[56]*	Even when definition is fixed in contracts, NCSG pushes for periodic-review mechanisms that do not become an expansion vector. *[66]*
Takedowns / suspension	Mitigation must avoid disproportionate takedown of lawful content; collateral damage must be minimized; hasty takedowns can harm expression/access. *[67]*	Preference for granular, evidence-based actions and for procedural checks before full-domain disruption (where feasible). *[68]*
Associated Domain Checks	Not categorically rejected, but treated as high-risk: requires strict safeguards, no arbitrary enforcement,	ADC policy must specify triggers, human review, evidentiary thresholds,

	meaningful notice and recourse; risk of profiling/surveillance. [69]	privacy safeguards, and redress mechanisms. [70]
KYC / identity verification	"Accuracy" should mean contactability, not identity verification; identity checks can endanger activists and violate privacy. [71]	DNS-abuse policy should avoid mandatory identity verification and should treat anonymity as a legitimate safety need. [36]
Due process / remedy	PDP outcomes must include clear due process and accessible challenge/remedy mechanisms; NCSG views lack of recourse as a core gap. [72]	Expect pressure for standardized notice, appeal/review, and documentation requirements—especially where actions scale across portfolios. [40]
Transparency and accountability	Argues for transparency reporting on mitigation actions and consistent frameworks; criticizes reports that treat rights-based inputs as "lack of data." [73]	Likely advocacy for mandatory transparency reporting or standardized metrics beyond compliance case counts. [74]
Evidence standards	Insists mitigation pivots be grounded in specific evidence, not broad profiling; stresses "actionable evidence" as a key concept. [75]	Stronger definitions of "actionable evidence," documentation, and burden-of-proof norms inside ADC processes. [76]
"Proactive monitoring" and predictive algorithms	Treats broad proactive monitoring as surveillance; wants strong scoping limits and safeguards; skeptical of algorithmic mandates. [77]	Pushback against "always-on" monitoring requirements and against policy hard-coding specific security mechanisms. [78]

HRIA as a governance tool	Advocates HRIA as qualitative success measure and as a way to operationalize ICANN bylaw commitments; builds tools and pushes integration into PDPs. *[79]*	HRIA becomes a process constraint: policy work must explain impacts, affected groups, and mitigations or safeguards. *[80]*

Annotated source links used and recommended

PRIMARY NCSG PUBLIC COMMENTS / STATEMENTS

https://lists.icann.org/hyperkitty/list/comments-cct-final-recs-08oct18@icann.org/message/HU5CX2HB46H3YZNOOISI6VII42IWFNVP/attachment/4/CompetitionConsumerTrustandConsumerChoiceReviewTeamCCTFinalReportRecommendations-NCSGcomment.pdf
- NCSG's 2018 CCT comment: early, detailed mission-limits and "abuse/content" warnings.

https://lists.icann.org/hyperkitty/list/comments-ssr2-rt-draft-report-31jan20@icann.org/message/BNILGI7A6WS5ALS5QDGY3CWXWZ432AWU/attachment/4/NCSGCommentSecondSecurityStabilityandResiliencySSR2ReviewTeamDraftReport.pdf
- NCSG's 2020 SSR2 Draft Report comment: scope discipline and concerns about misuse of abuse metrics.

https://lists.icann.org/hyperkitty/list/comments-ssr2-final-report-28jan21@icann.org/message/JZRVMR4WRPPGVSDWKWN3OOHRGI4MCTZR/attachment/4/NCSGComment-SecondSecurityStabilityandResiliencySSR2ReviewTeamFinalReport.pdf
- NCSG's 2021 SSR2 Final Report comment: rejects broad "DNS abuse" definitions including IP/fraud/etc.

https://www.icann.org/en/public-comment/proceeding/amendments-to-the-base-gtld-ra-and-raa-to-modify-dns-abuse-contract-obligations-29-05-2023/submissions/non-commercial-stakeholder-group-ncsg-14-07-2023
- NCSG 2023 submission landing page (with attachment link).

https://www.icann.org/en/system/files/files/ncsg-comments-gtld-amendments-14jul23-en.pdf
- NCSG 2023 detailed comment: opposes "DNS Abuse" label shift; objects to spam inclusion; mission/scope framing.

https://gnso.icann.org/sites/default/files/policy/2025/presentation/ncsg-statement-dns-abuse-report-14aug25-en.pdfv
- NCSG Aug 2025 statement to record: approves report but flags Associated Domain Checks + due process.

https://itp.cdn.icann.org/public-comment/proceeding/Preliminary%20Issue%20Report%20on%20a%20Policy%20Development%20Process%20on%20DNS%20Abuse%20Mitigation-08-09-2025/submissions/Non-Commercial%20Stakeholder%20Group%20-%20NCSG/NCSG%20Comment%20-%20Preliminary%20Issue%20Report%20on%20a%20Policy%20Development%20Process%20on%20DNS%20Abuse%20Mitigation-15-10-2025.pdf
- NCSG Oct 2025 comment: evidence standards, contactability vs identity, due

process/recourse, surveillance concerns.

https://gnso.icann.org/sites/default/files/policy/2025/presentation/ncsg-statement-record-dns-abuse-mtigation-pdp-15dec25.pdf
- NCSG Dec 2025 statement for record: ADC human-rights/profiling risk + calls for safeguards and better research base.

CORE ICANN / GNSO PROCESS DOCUMENTS

https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf
- 2022 DNS Abuse Small Team report introducing lifecycle framing and listing "KYC" as a concept.

https://gnso.icann.org/sites/default/files/policy/2025/draft/dns-abuse-small-team-report-04aug25-en.pdf
- 2025 reconvened DNS Abuse Small Team report underpinning 2025 Issue Report work.

https://gnso.icann.org/sites/default/files/policy/2025/draft/issue-report-dns-abuse-mitigation-v04dec25-en.pdf
- Final Issue Report (Dec 2025): includes draft charters for PDP1/PDP2 and states HRIA inclusion by default.

https://icann-community.atlassian.net/wiki/spaces/gnsocouncilmeetings/pages/607420481/Motions+2026-01-15
- GNSO Council motion record (Jan 2026): documents charter adoption for DNS Abuse Mitigation PDP1.

CONTRACTUAL AMENDMENTS, COMPLIANCE GUIDANCE, PROGRAM PAGES

https://www.icann.org/en/contracted-parties/registry-operators/global-amendments/2024-global-amendments
- Background and resources for 2024 global amendments to RAA/Base RA regarding DNS abuse.

https://itp.cdn.icann.org/en/files/accredited-registrars/registrar-accreditation-agreement-global-amendment-05apr24-en.htm
- Contract text: defines DNS Abuse and sets registrar obligations (actionable evidence; collateral damage).

https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en
- Compliance advisory: interpretation and compliance expectations for the DNS Abuse amendments.

https://www.icann.org/dnsabuse
- ICANN DNS Abuse Mitigation Program page (definitions, scope, and program framing).

KEY EXTERNAL / EVIDENCE SOURCES (used to contextualize the policy debate)
https://rrsg.org/wp-content/uploads/2020/10/CPH-Definition-of-DNS-Abuse.pdf
- Contracted Party House definition of DNS Abuse (technical harms + spam as vector).

https://rrsg.org/wp-content/uploads/2022/01/CPH-Guide-to-Abuse-Reporting-v1.0.pdf
- Contracted parties' guidance on actionable reporting and where to direct complaints.

https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf
- INFERMAL technical report: evidence base linking registrar/TLD features (API, bulk tools, verification) to malicious registrations.

https://digitalmedusa.org/wp-content/uploads/2024/11/DNS-IHRL-Cheat-Sheet.pdf
- Rights mapping tool used in NCSG/HRIA framing (privacy, expression, remedy; ICCPR/UDHR/UNGP references).

https://gac.icann.org/transcripts/public/icann82-session-6-gac-open-mic-and-meeting-with-the-ncsg-sessions-en-transcript.pdf?language_id=1
- Transcript where NCSG presents HRIA-based approach and qualitative success measures (March 2025).

https://gac.icann.org/transcripts/public/icann84-session-7-gnso-dns-abuse-work-session-en-transcript.pdf?language_id=1
- ICANN84 DNS abuse work session transcript (cross-community preparatory discussion).

https://gac.icann.org/minutes/public/ICANN84%20GAC%20Minutes.pdf?language_id=1
- GAC minutes capturing NCSG–GAC discussions on HRIA, DNS abuse mitigation, and PDP HRIA integration.

https://www.centr.org/news/blog/icann84-highlights-from-the-discussions-on-dns-abuse-and-access-to-registration-data.html

- External synthesis of ICANN84 DNS abuse issues; notes controversies around ADC and rights impacts.

https://www.centr.org/news/blog/icann85-abuse-policy-discussions-expected-to-move-at-light-speed.html

- External synthesis of early 2026 dynamics: accelerated PDP1 timeline and safeguard debates.

https://digitalmedusa.org/domain-name-system-abuse-and-human-rights-impact-assessment-a-table-top-exercise/

- Secondary summary of HRIA tabletop framing; references "Human Rights Gap Analysis" even where the underlying doc is not publicly retrieved here.

- https://icann-community.atlassian.net/wiki/spaces/gnsononcomstake/pages/116558695/CCWP+on+ICANN+and+Human+Rights

- https://www.article19.org/resources/online-freedoms-safeguards-must-be-balanced-with-free-expression/

- https://circleid.com/posts/looking-ahead-icanns-upcoming-policy-on-dns-abuse-mitigation

- https://itp.cdn.icann.org/public-comment/proceeding/Preliminary%20Issue%20Report%20on%20a%20Policy%20Development%20Process%20on%20DNS%20Abuse%20Mitigation-08-09-2025/submissions/Non-Commercial%20Stakeholder%20Group%20-%20NCSG/NCSG%20Comment%20-%20Preliminary%20Issue%20Report%20on%20a%20Policy%20Development%20Process%20on%20DNS%20Abuse%20Mitigation-15-10-2025.pdf

https://gnso.icann.org/sites/default/files/policy/2025/draft/dns-abuse-small-team-report-04aug25-en.pdf

https://www.article19.org/wp-content/uploads/2021/06/A19-and-DIHR-pilot-project-outcome-report_FINAL.pdf

https://www.eff.org/deeplinks/2020/08/icann-must-respect-human-rights-and-avoid-content-regulation

https://digitalmedusa.org/domain-name-system-abuse-and-human-rights-impact-assessment-a-table-top-exercise/

https://digitalmedusa.org/law-enforcement-agencies-and-transparency-the-icann-issue/

https://digitalmedusa.org/the-governments-score-on-human-rights-a-look-at-icann82/

https://www.article19.org/wp-content/uploads/2021/06/A19-and-DIHR-pilot-project-outcome-report_FINAL.pdf

https://www.article19.org/resources/blog-icann-takes-one-step-forward-in-its-human-rights-and-accountability-commitments/

https://itp.cdn.icann.org/public-comment/proceeding/Pilot%20Holistic%20Review%20Draft%20Terms%20of%20Reference-30-08-2022/submissions/Cross-Community%20Working%20Party%20on%20ICANN%20and%20Human%20Rights%20(CCWP-HR)/Final%20CCWP-HR%20HRGA%20for%20Pilot%20Holistic%20Review%20Draft%20Terms%20of%20Reference-10-11-2022.pdf

CCWP-HR publications/resources can be found here:
https://icann-community.atlassian.net/wiki/spaces/gnsononcomstake/pages/116558695/CCWP+on+ICANN+and+Human+Rights

https://docs.google.com/document/d/1g1AtfROHirQpmRzo1arYvpyexO_72HHISNSERSJ-zAA/edit?tab=t.0

INTERNAL / COMMUNITY RECORDS (supporting evidence; not always "official positions")

https://lists.icann.org/hyperkitty/list/ncsg-dns-abuse-wg@icann.org/message/O3PA6ZO4C6HE6XWRLLBISBY2MG54VELQ/
- Public "action points" message showing internal NCSG organization around DNS-abuse definitions and position paper drafting.

https://lists.ncuc.org/pipermail/ncuc-discuss/2019-October/045571.html
- Public mirror of an internal message noting DNS abuse salience and pointing to GAC correspondence.

https://icann-community.atlassian.net/wiki/spaces/gnsononcomstake/pages/116557294/Policy+Development
- NCSG policy development hub linking to yearly public comments lists and policy statements.

https://icann-community.atlassian.net/wiki/spaces/gnsononcomstake/pages/116562144/Public+Comments+-+2023
- NCSG "Public Comments 2023" page linking to its DNS-abuse amendments submission.

[1] [8] [17] [18] [47] [49] [64]
https://lists.icann.org/hyperkitty/list/comments-cct-final-recs-08oct18%40icann.org/message/HU5CX2HB46H3YZNOOISI6VII42IWFNVP/attachment/4/CompetitionConsumerTrustandConsumerChoiceReviewTeamCCTFinalReportRecommendations-NCSGcomment.pdf

https://lists.icann.org/hyperkitty/list/comments-cct-final-recs-08oct18%40icann.org/message/HU5CX2HB46H3YZNOOISI6VII42IWFNVP/attachment/4/CompetitionConsumerTrustandConsumerChoiceReviewTeamCCTFinalReportRecommendations-NCSGcomment.pdf

[2] [7] [32] [34]
https://digitalmedusa.org/wp-content/uploads/2024/11/DNS-IHRL-Cheat-Sheet.pdf

https://digitalmedusa.org/wp-content/uploads/2024/11/DNS-IHRL-Cheat-Sheet.pdf

[3] [6] [11] [27] [36] [37] [39] [40] [41] [52] [53] [59] [60] [66] [71] [72] [75] [77] [78]
https://itp.cdn.icann.org/public-comment/proceeding/Preliminary%20Issue%20Report%20on%20a%20Policy%20Development%20Process%20on%20DNS%20Abuse%20Mitigation-08-09-2025/submissions/Non-Commercial%20Stakeholder%20Group%20-%20NCSG/NCSG%20Comment%20-%20Preliminary%20Issue%20Report%20on%20a%20Policy%20Development%20Process%20on%20DNS%20Abuse%20Mitigation-15-10-2025.pdf

https://itp.cdn.icann.org/public-comment/proceeding/Preliminary%20Issue%20Report%20on%20a%20Policy%20Development%20Process%20on%20DNS%20Abuse%20Mitigation-08-09-2025/submissions/Non-Commercial%20Stakeholder%20Group%20-%20NCSG/NCSG%20Comment%20-%20Preliminary%20Issue%20Report%20on%20a%20Policy%20Development%20Process%20on%20DNS%20Abuse%20Mitigation-15-10-2025.pdf

[4] [5] [30] [31]
https://itp.cdn.icann.org/en/files/accredited-registrars/registrar-accreditation-agreement-global-amendment-05apr24-en.htm

https://itp.cdn.icann.org/en/files/accredited-registrars/registrar-accreditation-agreement-global-amendment-05apr24-en.htm

[9] [33] [55]
https://lists.icann.org/hyperkitty/list/ncsg-dns-abuse-wg%40icann.org/message/O3PA6ZO4C6HE6XWRLLBISBY2MG54VELQ/

https://lists.icann.org/hyperkitty/list/ncsg-dns-abuse-wg%40icann.org/message/O3PA6ZO4C6HE6XWRLLBISBY2MG54VELQ/

[10] https://lists.ncuc.org/pipermail/ncuc-discuss/2019-October/045571.html

https://lists.ncuc.org/pipermail/ncuc-discuss/2019-October/045571.html

[12] [57] [68]
https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en

https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en

[13] [29] [65] https://www.icann.org/dnsabuse

https://www.icann.org/dnsabuse

[14] [22] [23]
https://lists.icann.org/hyperkitty/list/comments-ssr2-final-report-28jan21%40icann.org/message/JZRVMR4WRPPGVSDWKWN3OOHRGI4MCTZR/attachment/4/NCSGComment-SecondSecurityStabilityandResiliencySSR2ReviewTeamFinalReport.pdf

https://lists.icann.org/hyperkitty/list/comments-ssr2-final-report-28jan21%40icann.org/message/JZRVMR4WRPPGVSDWKWN3OOHRGI4MCTZR/attachment/4/NCSGComment-SecondSecurityStabilityandResiliencySSR2ReviewTeamFinalReport.pdf

[15] [51]
https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf

https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf

[16] [19] [26] [42] [46] [61] [70] [76] [80]
https://gnso.icann.org/sites/default/files/policy/2025/draft/issue-report-dns-abuse-mitigation-v04dec25-en.pdf

https://gnso.icann.org/sites/default/files/policy/2025/draft/issue-report-dns-abuse-mitigation-v04dec25-en.pdf

[20] [24] [38] [48] [58] [69]
https://gnso.icann.org/sites/default/files/policy/2025/presentation/ncsg-statement-dns-abuse-report-14aug25-en.pdf

https://gnso.icann.org/sites/default/files/policy/2025/presentation/ncsg-statement-dns-abuse-report-14aug25-en.pdf

[21]
https://lists.icann.org/hyperkitty/list/comments-ssr2-rt-draft-report-24jan20%40icann.org/message/DU56RRY3VULSHCFI7HY2ECUSVUWVKDM5/attachment/4/SecondSecurityStabilityandResiliencySSR2ReviewTeamDraftReport-NCSGComment.pdf

https://lists.icann.org/hyperkitty/list/comments-ssr2-rt-draft-report-24jan20%40icann.org/message/DU56RRY3VULSHCFI7HY2ECUSVUWVKDM5/attachment/4/SecondSecurityStabilityandResiliencySSR2ReviewTeamDraftReport-NCSGComment.pdf

[25]
https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf

https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf

[28] [56]
https://itp.cdn.icann.org/public-comment/proceeding/Amendments%20to%20the%20Base%20gTLD%20RA%20and%20RAA%20to%20Modify%20DNS%20Abuse%20Contract%20Obligations-29-05-2023/submissions/Non-Commercial%20Stakeholder%20Group%20%28NCSG%29/NCSG%20Comment%20-%20Amendments%20to%20the%20Base%20gTLD%20RA%20and%20RAA%20to%20Modify%20DNS%20Abuse%20Contract%20Obligations-14-07-2023.pdf

https://itp.cdn.icann.org/public-comment/proceeding/Amendments%20to%20the%20Base%20gTLD%20RA%20and%20RAA%20to%20Modify%20DNS%20Abuse%20Contract%20Obligations-29-05-2023/submissions/Non-Commercial%20Stakeholder%20Group%20%28NCSG%29/NCSG%20Comment%20-%20Amendments%20to%20the%20Base%20gTLD%20RA%20and%20RAA%20to%20Modify%20DNS%20Abuse%20Contract%20Obligations-14-07-2023.pdf

[35] [67] [79]
https://gac.icann.org/transcripts/public/icann82-session-6-gac-open-mic-and-meeting-with-the-ncsg-sessions-en-transcript.pdf?language_id=1

https://gac.icann.org/transcripts/public/icann82-session-6-gac-open-mic-and-meeting-with-the-ncsg-sessions-en-transcript.pdf?language_id=1

[43] [50] [62] [73]
https://gnso.icann.org/sites/default/files/policy/2025/presentation/ncsg-statement-record-dns-abuse-mtigation-pdp-15dec25.pdf

https://gnso.icann.org/sites/default/files/policy/2025/presentation/ncsg-statement-record-dns-abuse-mtigation-pdp-15dec25.pdf

[44] *[63]*
https://icann-community.atlassian.net/wiki/spaces/gnsocouncilmeetings/pages/607420481/Motions%2B2026-01-15

https://icann-community.atlassian.net/wiki/spaces/gnsocouncilmeetings/pages/607420481/Motions%2B2026-01-15

[45]
https://www.centr.org/news/blog/icann85-abuse-policy-discussions-expected-to-move-at-light-speed.html

https://www.centr.org/news/blog/icann85-abuse-policy-discussions-expected-to-move-at-light-speed.html

[54] *[74]*
https://gac.icann.org/minutes/public/ICANN84%20GAC%20Minutes.pdf?language_id=1

https://gac.icann.org/minutes/public/ICANN84%20GAC%20Minutes.pdf?language_id=1

Annex I: Glossary of Terms and Acronyms

I.1 Purpose of this Annex

This Annex provides a structured glossary of key terms, acronyms, and concepts used throughout this report. Terms are organized according to their functional relevance within the analysis of DNS abuse and the positions of the Noncommercial Stakeholder Group.

This glossary is intended to support readability and ensure a common understanding of technical, policy, and governance terminology.

I.2 ICANN Ecosystem and Governance Structures

I.2.1 ICANN – Internet Corporation for Assigned Names and Numbers; the global multistakeholder body responsible for coordinating the Domain Name System (DNS).

I.2.2 DNS – Domain Name System; the hierarchical system that translates human-readable domain names into IP addresses.

I.2.3 Multistakeholder Model – A governance approach involving governments, private sector, civil society, and the technical community in decision-making processes.

I.2.4 GNSO – Generic Names Supporting Organization; develops and recommends policies for generic top-level domains (gTLDs).

I.2.5 GAC – Governmental Advisory Committee; provides public policy advice to ICANN from national governments and intergovernmental organizations.

I.2.6 ALAC – At-Large Advisory Committee; represents the interests of individual Internet users within ICANN.

I.2.7 SSAC – Security and Stability Advisory Committee; provides advice on the security and integrity of the DNS.

I.2.8 ccNSO – Country Code Names Supporting Organization; develops policies for country code top-level domains (ccTLDs).

I.3 Stakeholder Groups and Community Structures

I.3.1 NCSG – Non-Commercial Stakeholder Group; represents civil society and noncommercial interests within the GNSO.

I.3.2 NCUC – Non-Commercial Users Constituency; focuses on policy advocacy related to civil liberties and Internet user rights.

I.3.3 NPOC – Not-for-Profit Operational Concerns Constituency; represents operational concerns of nonprofit organizations.

I.3.4 CPH – Contracted Party House; includes registries and registrars that have contractual agreements with ICANN.

I.3.5 RySG – Registry Stakeholder Group; represents domain name registries.

I.3.6 RrSG – Registrar Stakeholder Group; represents domain name registrars.

I.3.7 IPC – Intellectual Property Constituency; represents intellectual property interests within ICANN.

I.3.8 BC – Business Constituency; represents commercial and business users of the Internet.

I.3.9 Non-Contracted Parties – Stakeholders within ICANN that are not bound by ICANN contractual agreements (e.g., NCSG, IPC, BC).

I.4 DNS Abuse: Definitions and Scope

I.4.1 DNS Abuse – The malicious use of the Domain Name System to carry out harmful activities, typically including malware distribution, phishing, botnet command-and-control, pharming, and spam when used as a delivery mechanism for these threats.

I.4.2 Malware – Software designed to disrupt, damage, or gain unauthorized access to systems.

I.4.3 Phishing – Fraudulent attempts to obtain sensitive information by impersonating trustworthy entities.

I.4.4 Botnet – A network of compromised devices controlled remotely to perform coordinated malicious activities.

I.4.5 Pharming – The redirection of users to fraudulent websites through DNS manipulation.

I.4.6 Content vs. Infrastructure Debate – The policy distinction between regulating illegal or harmful content and addressing technical abuse occurring at the DNS layer.

I.5 Types of Abuse and Technical Threats

I.5.1 DoS (Denial of Service) – An attack aimed at making a system or service unavailable.

I.5.2 DDoS (Distributed Denial of Service) – A coordinated attack using multiple systems to overwhelm a target.

I.5.3 DNSSEC – Domain Name System Security Extensions; a protocol that ensures the authenticity and integrity of DNS data.

I.5.4 Abuse Reporting – Processes and mechanisms for reporting suspected DNS abuse to registrars or registries.

I.6 Policy Development and ICANN Processes

I.6.1 PDP – Policy Development Process; the formal mechanism used by the GNSO to develop ICANN policies.

I.6.2 EPDP – Expedited Policy Development Process; a fast-tracked PDP for urgent issues.

I.6.3 Consensus Policy – A policy developed through ICANN's multistakeholder process that becomes binding on contracted parties.

I.6.4 Public Comment Proceeding – A formal consultation process allowing stakeholders to provide input on policy proposals.

I.6.5 Preliminary Issue Report – A document assessing whether a PDP should be initiated.

I.6.6 PDP on DNS Abuse Mitigation – The ongoing policy process addressing definitions, scope, and mitigation obligations for DNS abuse.

I.7 Contractual Frameworks and Compliance

I.7.1 RA (Registry Agreement) – Contract between ICANN and registry operators governing gTLD operations.

I.7.2 RAA (Registrar Accreditation Agreement) – Contract between ICANN and registrars outlining obligations and compliance requirements.

I.7.3 Contracted Parties – Registries and registrars bound by ICANN agreements.

I.7.4 ToS (Terms of Service) – Rules governing user interactions with domain services.

I.8 Human Rights, Safeguards, and Accountability

I.8.1 HRIA – Human Rights Impact Assessment; a framework used to evaluate the impact of policies or actions on human rights.

I.8.2 FoE (Freedom of Expression) – The right to seek, receive, and impart information without undue interference.

I.8.3 DP (Data Protection) – Safeguards ensuring personal data is processed lawfully and securely.

I.8.4 GDPR – General Data Protection Regulation; EU regulation governing personal data protection.

I.8.5 Due Process – Fair and transparent procedures before enforcement actions are taken.

I.8.6 Proportionality Principle – Ensuring that actions taken are appropriate and not excessive relative to the harm addressed.

I.8.7 Overblocking – The unintended restriction of legitimate content or domain names as a result of enforcement actions.

I.9 Transparency, Investigation, and Enforcement Principles

I.9.1 Due Diligence – Reasonable steps taken to assess and address DNS abuse before action.

I.9.2 Safe Harbor – Legal protection granted to entities acting in good faith within defined frameworks.

I.9.3 Data Minimization – Limiting data collection to what is necessary for a defined purpose.

I.9.4 Transparency – Providing clear and accessible information regarding actions, criteria, and processes.

I.10 Data Access and Technical Protocols

I.10.1 WHOIS – A protocol used to query domain registration information.

I.10.2 RDAP – Registration Data Access Protocol; a modern replacement for WHOIS with enhanced privacy and security features.

I.11 Cross-Community Coordination Mechanisms

I.11.1 CCWG – Cross-Community Working Group; collaborative groups involving multiple ICANN stakeholder bodies.

I.11.2 SADAG – SSAC DNS Abuse Analysis Working Group; provides analysis on DNS abuse trends and mitigation.

I.12 Usage Note

This glossary should be read in conjunction with the main report. Terms are referenced contextually in relevant sections to support clarity and comprehension for both technical and non-technical audiences.