Associated Domain Checks

Comprehensive Update: NCSG Participation in DNS Abuse Mitigation PDP 1 and Action Needed from the NCSG Community.

Last update: 1st June, 2026

Dear NCSG members,

Following the earlier briefing shared on the DNS Abuse Mitigation PDP 1 Working Group, we are writing to provide a concise but comprehensive chronological update on the Working Group's progress from the first session held during ICANN85 to the latest meeting on 1 June 2026.

This update covers how the work has progressed, how NCSG has been participating, the key issues currently under discussion, and where community input is urgently needed as the Working Group moves toward ICANN86 and the review of preliminary recommendation language.

The DNS Abuse Mitigation PDP 1 Working Group is focused on Associated Domain Checks, or ADCs. In simple terms, the PDP is examining whether, when a registrar has evidence that one domain name is being used for DNS Abuse, the registrar should also be required to check other domain names that may be associated with the same registrant, customer account, or related registration context.

This work follows earlier GNSO DNS Abuse work, the 2024 contractual amendments to the Registry Agreement and Registrar Accreditation Agreement, and the GNSO Council's decision to launch a narrowly scoped PDP on DNS Abuse. The DNS Abuse Mitigation PDP 1 Charter was adopted by the GNSO Council on 15 January 2026.

This PDP is highly consequential for noncommercial users, civil society organizations, individual registrants, activists, journalists, researchers, small nonprofits, public-interest actors, and others who rely on domain names for lawful expression, association, organizing, advocacy, access to information, and service delivery.

If designed carefully, Associated Domain Checks may help identify coordinated malicious registration campaigns. If designed too broadly, however, they could create risks of overreach, account-level profiling, wrongful suspension, privacy intrusion, chilling effects on lawful speech, and harm to legitimate registrants.

NCSG's central position remains clear: we support effective DNS Abuse mitigation, but any Associated Domain Check obligation must be evidence-based, proportionate, technically feasible, privacy-respecting, rights-respecting, and limited to ICANN's remit.

Why this PDP matters to NCSG

The PDP raises issues that sit directly within NCSG's core policy concerns, including:

- protection of noncommercial registrants;
- freedom of expression and association;

- privacy and data protection;
- proportionality and due process;
- prevention of collateral damage;
- clear limits on ICANN's technical coordination role;
- protection against content regulation through DNS Abuse processes;
- fair treatment of smaller, regional, and resource-constrained registrars;
- transparency and accountability in enforcement;
- meaningful remedies where legitimate registrants are harmed.

The concern is not whether DNS Abuse should be addressed. It should. The concern is whether the policy response is properly developed with safeguards in place.

A poorly designed ADC obligation could allow a single abuse report, or one confirmed abusive domain, to become the basis for broader investigation of a registrant's entire domain portfolio. This could especially affect registrants who hold multiple domains for legitimate reasons, including civil society groups, journalists, activists, human rights defenders, community organizations, researchers, small businesses, political movements, or organizations operating in sensitive environments.

The better policy question is therefore:
How can ICANN policy help address coordinated DNS Abuse while preventing unjustified surveillance, over-removal, false positives, and harm to legitimate registrants?

That is the lens NCSG has been bringing to the Working Group.

Chronological update from the first session to date

Below is a brief timeline of how the Working Group has progressed from the first session through the latest meeting.

7 March 2026 — ICANN85 Session 1: Kick-off meeting
The first Working Group session was held during ICANN85. This was the formal kick-off meeting. The session introduced the Working Group, reviewed the project plan, discussed meeting frequency and scheduling, reviewed the DNS Abuse Mitigation PDP 1 Charter, and introduced the early input request from the community.
The session also introduced potential impact areas, including Global Public Interest, Human Rights, Data Protection, and the relationship with existing consensus policies.

NCSG relevance: From the beginning, the process recognized that the PDP is not only a technical abuse-mitigation exercise. It also requires careful consideration of human rights, data protection, proportionality, and policy impact.

7 March 2026 — ICANN85 Session 2: Consensus-building exercise
The second session focused on consensus-building. The WG reviewed expectations for how members would deliberate, engage, and work toward policy recommendations.

NCSG relevance: This session was important because the ADC issue involves competing interests. NCSG's role is to participate constructively, identify risks clearly, and offer text that can help the WG reach balanced outcomes.

9 March 2026 — ICANN85 Session 3: Charter Question 1 and SME input
The third session focused on Charter Question 1 and included subject-matter expert input on Associated Domain Check practices. The discussion began to explore what should trigger an ADC and how registrars currently think about associated domains.

NCSG relevance: CQ1 remains one of the most important questions for us because the trigger determines when a registrar must begin looking beyond the first domain. NCSG has been concerned that a single-domain trigger, without additional safeguards, may be too broad.

9 March 2026 — ICANN85 Session 4: Scope, purpose, methodology, and CQ1 discussion
The fourth session continued the discussion on the scope, purpose, and methodology of the PDP and further considered CQ1.

NCSG relevance: This was an early opportunity to reinforce that the PDP should remain within ICANN's remit, focus on DNS Abuse as contractually defined, and avoid content regulation or broader account-level surveillance.

23 March 2026 — First regular WG call after ICANN85
The 23 March meeting reviewed what took place at ICANN85, updated the Vice-Chair selection process, introduced WG members, reviewed the work plan, and continued discussion of CQ1.
The notes show that WG members raised themes such as implementability, pragmatism, enforceability, proportionality, respect for human rights, scalability, and the need to make a practical contribution to DNS Abuse mitigation.
The WG also noted that compromised domains, ADCs across registrars, and dictating mitigation actions are outside the PDP's scope.

NCSG relevance: These themes align strongly with NCSG's concerns. We have consistently argued that ADC obligations must be practical, proportionate, rights-respecting, and carefully scoped.

30 March 2026 — Work plan, leadership, early input, and CQ1 themes
The 30 March meeting confirmed Nick Wenban-Smith as Vice-Chair, discussed meeting cadence and public holidays, reviewed the work plan, and continued deliberations.
A key point from this meeting was that early input had been received from several groups, including NCSG, and that each input would be added into the collaboration tool relative to the relevant Charter Question.
The WG also discussed the importance of flexibility, enforceability, reasonableness, proportionality, and whether a single maliciously registered domain should be enough to trigger ADC obligations.

NCSG relevance: This was important because NCSG's early input became part of the working record. Our position began to be reflected in the broader discussion on proportionality, reasonable investigation, and the risk of setting the trigger too low.

7 April 2026 — CQ1, CQ2, CQ3 and no convergence on key trigger issues

The 7 April meeting continued discussion of CQ1 and moved into CQ2 and CQ3. The WG discussed whether a registrar should perform an ADC when it has actionable evidence and has taken mitigation under RAA Section 3.18.2.

There was no convergence on several important issues, including:

- whether mitigation action must happen before conducting an ADC;
- whether one abusive or malicious domain is enough to trigger an ADC;
- the risk of a low threshold;
- workload concerns;
- the risk of guilt by association.

The WG also discussed business model differences and the impact of direct registrar versus reseller models on association criteria.

NCSG relevance: This is one of the central points for NCSG. We have argued that a single abusive domain should not automatically unlock review of an entire registrant portfolio. There must be credible evidence, objective indicators, and proportionality safeguards.

13 April 2026 — CQ2 association criteria, CQ3 reasonable investigation, and impact assessment approach

The 13 April meeting clarified WG roles and participation expectations, reviewed milestones, and discussed the iterative impact assessment approach.

The WG noted that by this point seven meetings had been completed, the leadership team had been finalized, the work plan and timeline had been sent to Council, the collaboration document had been established, and deliberations were continuing on Charter Questions 1–3.

The WG discussed CQ2 association criteria, including possible indicators such as the same account, same customer, same registrant, same end customer, common patterns, coordinated activity, and information reasonably available to the registrar. Members also noted that registrars have different business models and access to different data.

The WG also began deeper deliberation on CQ3, with some members emphasizing that investigation must remain distinct from enforcement.

NCSG relevance: This discussion is important because association criteria can either be narrow and evidence-based or broad and speculative. NCSG's concern is that weak signals such as shared infrastructure, reseller relationships, nameservers, or hosting should not be treated as proof of malicious control.

20 April 2026 — CQ2/CQ3 development, transparency concerns, and reasonable investigation

The 20 April meeting continued refining the discussion on association criteria and reasonable investigation. WG members discussed flexibility in registrar methods, transparency concerns,

business-model neutrality, and the risk that too much transparency could provide threat actors with a roadmap.
There was also discussion of whether transparency reporting could be relevant but potentially broader than the PDP's immediate scope.

NCSG relevance: NCSG should continue to support a balanced approach: registrars should have enough flexibility to respond to abuse, but there should also be sufficient documentation and accountability to prevent overreach and harm to legitimate registrants.

4 May 2026 — CQ3 refinement, CQ4 privacy safeguards, and start of CQ5
The 4 May meeting refined the CQ3 strawperson language, discussed CQ4 on data access and privacy safeguards, and began deliberations on CQ5 concerning adverse impact and remedies.
Several important issues were discussed:

- whether investigation obligations are limited to data reasonably available to registrars;
- the fact that registrars can only act on data they possess;
- the role of resellers where resellers may hold additional data;
- the need for flexibility for operational feasibility;
- whether "at least one data point" is sufficient or whether a reasonable number of indicators should be considered;
- the risk of superficial compliance;
- the need for baseline requirements without making the policy exhaustive.

The WG also asked NCSG to provide more granular language on potential adverse impact on registrants.

NCSG relevance: This was a significant moment for NCSG. The request for more granular NCSG language on adverse impact gives us a direct opportunity to shape the discussion around due process, registrant harm, and remedies.

11 May 2026 — CQ5 adverse impact/remedies and CQ6 timelines
The 11 May meeting began deeper deliberations on CQ5 and CQ6.
On CQ5, WG members discussed whether ADCs are primarily investigative mechanisms and how they relate to mitigation actions under existing RAA obligations. Some members noted that recourse mechanisms may be outside the current PDP scope, while others recognized that ADC-related processes themselves could create adverse impacts for legitimate registrants.
On CQ6, WG members discussed whether ADC reviews should be governed by fixed timelines or the existing RAA "promptly" standard. Many members supported maintaining a flexible standard because DNS Abuse cases vary in complexity, urgency, registrar size, and evidentiary requirements. Concerns were also raised that rigid timelines could create rushed investigations and false positives.

NCSG relevance: NCSG should continue to argue that registrant harm cannot be ignored simply because mitigation action is formally distinct from investigation. From a registrant's perspective, ADC-related processes may still create real harm. On timelines, NCSG supports "promptly" with accountability rather than rigid deadlines.

18 May 2026 — CQ5, CQ6, and start of CQ7

The 18 May meeting continued discussion of CQ5 and CQ6 and began deliberation on CQ7.
For CQ5, the WG discussed whether ADC-related activities could lead to account suspensions, takedowns, erroneous associations, or other adverse impacts even before a formal enforcement determination is finalized. The WG also acknowledged that future work may be needed on recourse issues.
For CQ6, the WG discussed the "promptly" standard versus fixed deadlines such as 72 hours. Many members supported retaining the existing "prompt" standard in RAA Section 3.18.2 and noted the trade-off between fast action and sufficiently complete, defensible investigations.
For CQ7, the WG began considering how current language could be categorized into Policy Recommendations, Rationale, and Implementation Guidance.

NCSG relevance: This meeting reinforced the importance of NCSG's position on remedies and timelines. We should continue to push for recognition of the recourse gap, documentation, notice where feasible, review channels, and correction of unsupported or disproportionate mitigation.

26 May 2026 — Preliminary recommendations, CQ5/CQ6 refinement, and impact assessment next steps
The 26 May meeting marked a shift from general deliberation to review of preliminary recommendation language.
The WG focused on:

- PDP updates;
- flash review of preliminary recommendations from CQ1 to CQ4;
- refinement of CQ5 and CQ6 strawpersons;
- next steps on impact assessments.

Support Staff introduced the Preliminary Recommendation Review Document as part of CQ7 discussion. This document is expected to contain preliminary recommendation language, rationale, and implementation guidance.
Key action items included:

- Support Staff to update and circulate the Preliminary Recommendation Review Document;
- refine language around minimum indicators;
- refine language concerning "all means within its control";
- better align and harmonize Recommendations 2 to 4;
- add preliminary recommendation language for CQ5 and CQ6;
- WG members to review language and provide substantive comments with proposed alternatives by 8 June 2026;
- Staff to share the Draft Scoped Impact Assessment with the WG for review.

NCSG relevance: This is where the work becomes more concrete. NCSG must now identify language that may create risk and propose alternative text that is operationally reasonable but safeguards registrants.

1 June 2026 — ICANN86 preparation, CQ8 metrics, and CQ9 compliance
The 1 June meeting focused on preparation for ICANN86 and the start of deliberations on CQ8 and CQ9.

The Chair introduced the objectives for the four ICANN86 sessions. These sessions will focus on reviewing preliminary recommendations, reviewing the scoped impact assessment, and developing preliminary recommendations for CQ8 and CQ9.

On CQ8, the WG discussed how to measure the policy's future effectiveness. Some members suggested a two-year review cycle. Members also questioned whether metrics such as "average uptime" or "reduction in uptime" are meaningful or measurable. There was support for seeking OCTO input on potential data sets and metrics, while recognizing that OCTO input should support, not delay, policy work.

On CQ9, the WG discussed how registrars can demonstrate compliance with ADC requirements. Staff noted that registrars typically demonstrate compliance by providing documented evidence showing what actions were taken, when, and why. WG members discussed whether registrars should show when the ADC obligation was triggered, what indicators were reviewed, what steps were taken, what conclusions were reached, and the rationale for those conclusions.

Key action items included:

- WG members to review the Preliminary Recommendation Review Document and identify any "cannot live with" areas before 8 June 2026;
- Staff to share the scoped Human Rights and Data Protection impact assessment;
- WG members to review the scoped impact assessment before 10 June 2026;
- identified concerns, feedback, and questions to be discussed during ICANN86 Working Sessions;
- Staff to develop straw proposals on CQ8 and CQ9.

NCSG relevance: CQ8 and CQ9 are critical because metrics and compliance language will determine whether safeguards are meaningful in practice. NCSG should insist that metrics measure accuracy, proportionality, wrongful suspensions, complaints, reversals, and time to remedy, not only the number of domains taken down.

NCSG's participation and policy contribution so far

NCSG representatives and participants have been actively engaging through:

- participation in WG meetings;
- review of strawperson text;
- input into the collaboration document;
- review of preliminary recommendation language;
- development of NCSG responses to Charter Questions;
- identification of risks to legitimate registrants;
- advocacy around privacy and proportionality;
- contributions to the human rights and global public interest framing;
- engagement on remedies, recourse, transparency, and accountability;
- preparation for deliberations on implementation, metrics, and compliance.

Our participation has not been limited to objecting to problematic text. We have also been trying to offer workable alternatives that can preserve DNS Abuse mitigation objectives while preventing overreach.

The main policy line we are advancing is:
Associated Domain Checks should be targeted investigative tools for coordinated DNS Abuse. They should not become broad registrant surveillance, account-level profiling, or a mechanism for guilt by association.

Summary of NCSG positions by Charter Question

CQ1: Trigger for ADC
NCSG's concern is that a single-domain trigger may be too low if it automatically opens the door to broader portfolio review. An ADC should require credible and substantiated evidence of DNS Abuse, a clear connection to DNS Abuse categories within scope, reasonable indicators of coordinated malicious activity, objective and verifiable association criteria, and safeguards against content-based or out-of-scope complaints.

NCSG framing: An ADC should be triggered only where the registrar has actionable and substantiated evidence of DNS Abuse, within the DNS Abuse categories recognized in ICANN's contractual framework, and reasonable indicators that additional domains may be part of the same malicious registration pattern or coordinated abuse campaign.

CQ2: Association criteria
NCSG can support flexible association criteria, but flexibility must not become open-ended discretion to associate domains based on weak or speculative signals. Shared infrastructure, privacy/proxy services, resellers, hosting, or nameservers may affect many unrelated registrants.

NCSG framing: Association should be based on objective, verifiable, and reasonably available indicators. Shared infrastructure alone should not be treated as sufficient evidence of malicious association.

CQ3: Reasonable investigation
NCSG supports a proportionate and practical investigation standard. Registrars should not be required to conduct broad forensic investigations, continuous monitoring, proactive surveillance, or account-wide audits.

NCSG framing: An ADC is an investigative step, not an evidentiary finding. Association may guide review, but it must not substitute for evidence. No associated domain should be subject to mitigation unless the registrar independently determines that the specific domain is being used for DNS Abuse.

CQ4: Data access and privacy safeguards
NCSG's position is that ADCs should use only data lawfully available to the registrar and reasonably necessary for the specific DNS Abuse purpose. The process should avoid unnecessary data collection, retention, sharing, or repurposing for unrelated purposes.

NCSG framing: Data used for an ADC should be limited to what is lawfully available and reasonably necessary for assessing the specific DNS Abuse concern. Data reviewed during an ADC should not be used for unrelated commercial, enforcement, profiling, or monitoring purposes.

CQ5: Adverse impact and remedies
NCSG considers this one of the most important issues. ADC-related processes can harm legitimate registrants through wrongful suspension, account-level review, reputational harm, exposure of sensitive portfolios, disruption of email or services, and lack of review or correction mechanisms.

NCSG framing: Any ADC policy must recognize that legitimate registrants can be harmed by overbroad or erroneous checks. Where mitigation action is taken against an associated domain, registrars should document the basis for the action, provide notice where feasible, provide a reasonable review path, and reverse or correct unsupported or disproportionate action without undue delay.

CQ6: Timelines and thresholds
NCSG supports the existing "promptly" standard, with accountability, rather than rigid fixed deadlines. Fixed timelines may encourage rushed or automated decisions and increase false positives.

NCSG framing: Registrars should act promptly where there is actionable and substantiated evidence of DNS Abuse, but timelines should remain context-specific and proportionate. Fixed timelines should not require rushed or automated action.

CQ7: Policy requirements versus guidance
NCSG should avoid two extremes. We should not allow all safeguards to be downgraded into optional best practices, but we should also avoid overly prescriptive operational requirements.

NCSG framing: Core safeguards should be binding where necessary, including trigger threshold, evidence requirement, domain-specific assessment, data minimization, documentation, and recognition of the recourse gap. Operational examples and technical methods may be placed in guidance or best practices.

CQ8: Metrics
Metrics shape incentives. If the policy only measures ADCs performed or domains taken down, it may reward over-removal.

NCSG framing: Metrics should measure accuracy, proportionality, and registrant impact, not only takedown volume. A successful policy is one that disrupts DNS Abuse while minimizing wrongful harm to legitimate registrants.

CQ9: Compliance
Compliance should not be reduced to showing that domains were taken down. It should include whether registrars followed the required process, used appropriate evidence, documented reasoning, avoided overbroad action, and corrected mistakes.

NCSG framing: Registrars should be able to demonstrate not only that they acted against DNS Abuse, but that they acted accurately, proportionately, and with safeguards for legitimate registrants. Compliance evidence should rely as much as possible on documentation already generated through ordinary abuse-handling processes.

Human rights and data protection considerations

The human rights dimension is not separate from the technical policy. It is embedded in the design of the ADC obligation itself.
NCSG's human rights and data protection concerns include freedom of expression, freedom of association, privacy, due process, access to information, protection against arbitrary or disproportionate interference, risks to vulnerable users, and risks to civil society and public-interest actors.
A full portfolio investigation based on one domain can reveal sensitive relationships, campaign infrastructure, advocacy networks, issue-based domains, or regional organizing structures. In high-risk environments, this can create real danger for activists, journalists, minority groups, or human rights defenders.
Even where no domain is suspended, the process of investigation can be intrusive if it expands data access, sharing, profiling, or retention.
NCSG's position is that the human rights and data protection assessment should not be delayed until the end of the PDP. It should shape the recommendations as they are being drafted.

Key risks NCSG is tracking
NCSG continue tracking the following risks:

- ADCs being triggered by too low a threshold;
- one abusive domain leading to broad portfolio investigation;
- association being treated as proof of abuse;
- shared infrastructure causing false positives;
- content disputes being mischaracterized as DNS Abuse;
- compromised domains being treated as maliciously registered domains;
- broad account-level surveillance;
- excessive data collection or retention;
- overreliance on opaque third-party intelligence feeds;
- lack of notice to registrants;
- lack of meaningful remedy or review;
- fixed timelines causing rushed decisions;
- metrics that reward takedown volume rather than accuracy;
- compliance rules that ignore wrongful suspensions or registrant complaints;
- disproportionate burdens on small and regional registrars;
- inadequate assessment of human rights and data protection impacts.

Practical examples of adverse impact

We are asking NCSG members to help provide examples of legitimate registrant harm that could result from overbroad ADC obligations.
Examples may include:

- A journalist operating separate domains for investigations, source protection, regional reporting, and archival projects.

- A civil society organization registering multiple domains for advocacy campaigns, election monitoring, emergency response, or community outreach.
- An activist in a high-risk jurisdiction whose domain portfolio could reveal sensitive relationships or organizing structures.
- A small nonprofit using multiple domains for email, donations, outreach, and service delivery.
- A legitimate domain compromised by a third party, where the registrant is treated as suspicious despite being a victim.
- Unrelated registrants sharing hosting, nameservers, IP addresses, resellers, privacy/proxy services, or other common infrastructure.
- Researchers operating domains for testing, sinkholing, measurement, security training, or abuse research.
- A community group with limited technical capacity struggling to respond quickly to registrar notices or unclear review processes.

These examples can help NCSG demonstrate that registrant harm is foreseeable and should be addressed directly in the policy design.

What NCSG members can do now

We need community input, especially from members with experience in civil society operations, digital rights, cybersecurity, registrar practices, domain name management, online safety, and human rights.

Please consider contributing in the following ways:

1. Share examples of adverse impact

We especially need examples of how overbroad ADCs could harm legitimate registrants. These can be real, anonymized, hypothetical, or scenario-based.

2. Follow the ICANN86 sessions

There will be several DNS Abuse Mitigation PDP 1 sessions during ICANN86. Remote participation is available, and community attention will help ensure NCSG positions are well supported.

Summary of NCSG's position

NCSG supports effective DNS Abuse mitigation. However, any Associated Domain Check obligation must be carefully limited.
Our position is that:

- ADCs should be triggered only by substantiated DNS Abuse and credible indicators of coordinated activity.
- A single abusive domain should not automatically justify a full portfolio investigation.
- Association should be based on objective and verifiable criteria.
- Association alone should never be sufficient for suspension or mitigation.
- Each domain must be assessed individually.
- Compromised domains should not be treated as maliciously registered domains.
- Privacy and data minimization must be built into the policy.

- Registrars should not be required to conduct broad surveillance or law-enforcement-style investigations.
- Smaller and regional registrars should not face disproportionate burdens.
- Legitimate registrants must have safeguards and meaningful remedies.
- Timelines should be prompt but flexible, with documentation and accountability.
- Metrics should measure accuracy and harm prevention, not only takedown volume.
- Compliance should include evidence of process, proportionality, and correction of mistakes.

In short: we want DNS Abuse mitigation that is effective, but also accurate, proportionate, accountable, and rights-respecting.

Important documents and links:

DNS Abuse Mitigation PDP 1 Workspace:
https://icann-community.atlassian.net/wiki/spaces/DAMP1/overview
Collaboration Document:
https://docs.google.com/document/d/1GxM-Yrgv6sZPEYU8ikW4cRM5YqWsJuWGiQyO39pLqNE/edit?usp=sharing
Preliminary Recommendation Review Document:
https://docs.google.com/document/d/1udLt1o9rwCc4xNRsuw6B-5onjpI63VDA/edit?usp=sharing&ouid=115002119020327708482&rtpof=true&sd=true
Scoped Impact Assessment:
https://docs.google.com/document/d/18xVFX-IXfEgPnIj2UaXmwiXsWE8FY-Jo/edit?usp=sharing&ouid=115002119020327708482&rtpof=true&sd=true
Charter - DNS Abuse Mitigation PDP 1:
https://gnso.icann.org/sites/default/files/policy/2026/draft/charter-dns-abuse-pdp1-v3-15jan26-en.pdf
GNSO DNS Abuse Mitigation PDP 1 project page:
https://gnso.icann.org/en/group-activities/active/dns-abuse-mitigation-pdp-1
GNSO DNS Abuse Mitigation PDP 1 Observer Enrollment:
https://gnso.icann.org/sites/default/files/policy/2025/draft/icann-join-new-user-instructions-12nov25-en.pdf

Closing

This PDP remains ongoing, and the policy language is still developing. That means NCSG still has a meaningful opportunity to shape the outcome.
Our most urgent task is to ensure that the Initial Report reflects NCSG's concerns on trigger thresholds, domain-specific evidence, privacy safeguards, adverse impact, registrant remedies, flexible timelines, transparency, metrics, and compliance.

We encourage all NCSG members to review this update and share comments, examples, or proposed language. Even short inputs are useful, especially where they help illustrate real-world harm to legitimate registrants or improve the wording of safeguards.

Thank you to everyone who has contributed to this work so far. We will continue to keep the community informed as the WG progresses through the remaining Charter Questions and prepares for further discussions around ICANN86 and beyond.