DNS ABUSE MITIGATION PDP1
Working Group Meeting #13
26 May 2026

Agenda

1. Welcome	5min
2. PDP Updates	10min
4. Flash review prelim rec from CQ1- 4	30min
5. Refine Strawperson on CQ5 and CQ6	25min
6. Next Steps on Impact Assessment(s)	10min
7. AOB	5min

PDP Updates (3 updates)

Road to ICANN86

Road to ICANN86

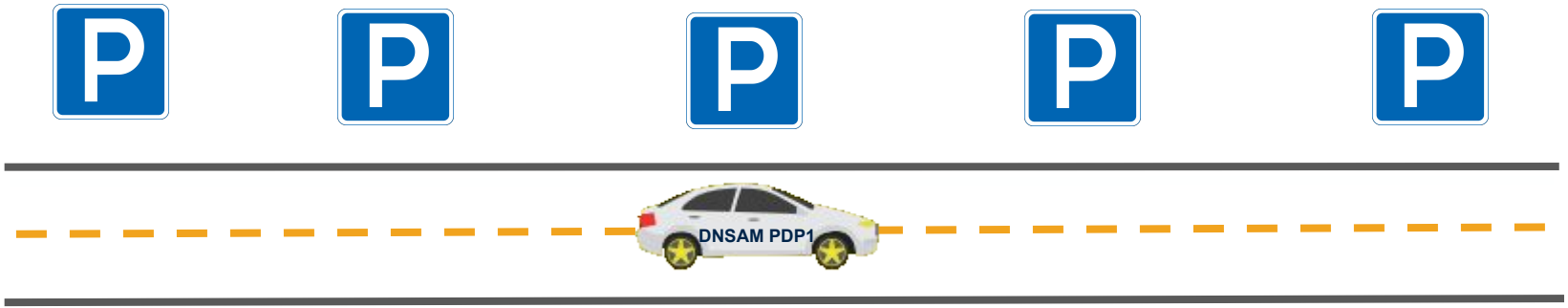
Week of 11 May
Deliberations on CQ5 and CQ6

Week of 18 May
Discuss Strawpersons CQ5 and 6

Week of 25 May
Review language on CQ1-6 as whole
IA next steps

Week of 1 June
Start Deliberations on CQ8-9
Prep for ICANN86

ICANN86
4 Working Sessions



Intro to Review Doc on Prelim Recommendations

New Review Document for CQ1-6

Based on CQ7 review, WG will be provided with a new review document where:

- Strawpeople language is categorized into:
  - Policy Recommendation
  - Rationale (WG explanation why they proposing this recommendation and the intention behind it)
  - Implementation Guidance (where relevant)
- Furthermore, LT with support from staff has reviewed and considered all comments in the CollabDoc and adjusted the language where necessary.
- The review document includes review tables:
  - Cannot Live With
  - Can Live with but with would prefer this change

New Review Document for CQ1-6

What does this mean for the WG:

- Review the updated language on CQ1-6 (to be provided based on todays discussion)
- Provide input in the dedicated table suggesting language WG member/SG/C CANNOT LIVE with and needs further discussion
- The CANNOT LIVE language will be added to the WG agenda to be discussed further

Language Review Best Practices

KEY PRINCIPLES

- The goal is for the WG to provide recommendations for new obligations on ADC so that they:
  - Can solve the issue as described in the Charter
  - Can receive Council support
  - Can be adopted by the Board
  - Can be implemented and enforced by ICANN org
- When reviewing the updated text, ask yourself:
  - Can my group live with this proposed recommendation/language?
  - If **NO**, provide **rationale and proposed alternate text**.

Language Review Best Practices

Reminder:

- Stay within scope - Check the Charter
- Goal is to provide Policy Recommendations. Not detailed implementation or contract language.
- Detailed Policy language will be developed in the IRT.

Language Review Best Practices

Draft language e.g. : The GNSO MUST add a new constituency - the pet constituency.

Helpful Comment:
Provide **rational and alternative language** to Text, the WG members CANNOT live with.

Draft language e.g.: The GNSO MUST add a new constituency - the pet constituency.

Less helpful comments:
Comment: I disagree.
Comment: ?
Comment: Please change.

ICANN DNS ABUSE ADVISORY CONSIDERATIONS RELEVANT FOR ADC

ICANN ADVISORY CONSIDERATIONS

After Actionable Evidence, Prompt Action Is Required: Upon obtaining actionable evidence, the registrar must *promptly* take *appropriate mitigation action(s)* that are reasonably necessary to stop, or otherwise disrupt, the Registered Name from being used for DNS Abuse. To determine the mitigation actions that are prompt and appropriate, the registrar will consider the specific circumstances of the case, which may include balancing the scope and intensity of the harm caused by the DNS Abuse against the possibility of associated collateral damage.

What Makes an Action Prompt: As noted above, the appropriate mitigation action to stop or disrupt an instance of DNS Abuse will vary depending on the specific circumstances. **Consequently, the appropriate amount of time to investigate and take action will also vary, making it impossible to prescribe a fixed amount of time for an action to be considered "prompt."** Instead, registrars must demonstrate an ongoing attentiveness to allegations of sponsored names being used for DNS Abuse. The attentiveness should be commensurate with the potential harm that DNS Abuse causes victims. Accordingly, in response to an inquiry by ICANN Contractual Compliance, registrars will be required to explain how the actions were prompt considering the specific circumstances. **ICANN Contractual Compliance will then review the explanation and the relevant circumstances to make a case-by-case determination as to whether the actions were reasonably prompt.**

Advisory Includes 2 Scenarios illustrating DNS Abuse Contract amendments including “prompt” action and “actionable evidence”.

Flash review prelim recommendation for CQ1-4

DNSAM PDP1

Prelim Recommendation 1:
When a registrar has actionable evidence that a Registered Name is being used for DNS Abuse and has determined, pursuant to Section 3.18.2 of the Registrar Accreditation Agreement (RAA), the registrar must perform an Associated Domain Check (ADC). For the avoidance of doubt, this requirement does not extend to compromised domains.

Main change based on WG input:

- Remove *definition* of “malicious domains”
- Add caveat that “compromised domains” are excluded from ADC

Based on CollabDocument Comments:

- The WG seems to agree with these changes

DNSAM PDP1

Prelim Recommendation 2:

To determine whether “association” exists, **a registrar MUST, at a minimum, review at least one Registered Name Holder or account-related indicator, or at least one technical or coordinated activity/behavioral indicator, that is reasonably accessible to the registrar and most likely to yield useful and actionable information. The ADC** can be conducted using a flexible, non-exhaustive set of criteria that allows registrars to identify domains that are reasonably linked to the same abusive activity, account, or actor. When determining “association”, registrars may take into account what is reasonably available to the registrar. and differences in registrar business models; the specific elements considered in any given ADC, even within a single registrar, may vary depending upon the particular circumstances.

Such association MAY include, but is not limited to, the following factors as applicable and as available:

- domains associated with the same account, customer, registrant, end customer, or other potential common connection points.
- domains exhibiting common patterns or indicators of coordinated activity, including naming conventions, shared infrastructure (e.g., nameservers), and/or campaign characteristics identified through internal analysis or external reporting.
- domains linked through information reasonably available to the registrar during its operations, including information derived from internal analysis and/or external reports that provide indicators of what to look for in a campaign.

DNSAM PDP1

Prelim Prelim Recommendation 3:

A “reasonable investigation” by a registrar MUST consist of reviewing information reasonably available to the registrar in the normal course of its operations to determine whether associated domain names are being used for DNS Abuse, per 3.18.2. A reasonable investigation MUST be practical and proportionate based on the circumstances and consistent with Section 3.18.2 of the RAA. A reasonable investigation MUST NOT require registrars to access or generate data that is not reasonably available to them, recognizing that registrar capabilities, technical systems, and available data may differ across and within registrars. **Notwithstanding for foregoing, registrars must undertake all means within its control, provided such actions are lawful and reasonable, to detect related or associated domains.**

Implementation guidance:

For the purposes of this policy, “reasonably available data” would include:

- **Data required to be collected or maintained under applicable ICANN agreements;**
- **Data otherwise held by the registrar and accessible through its technical systems; and**
- **Information received by the registrar in connection with an abuse report or investigation.**

Where a registrar operates through a reseller or similar business model:

- **A registrar may rely on a reseller to conduct ADC investigation steps using data reasonably available to the reseller.**
- **The registrar will remain responsible for ensuring that a reasonable investigation is conducted (as required in the RAA 3.12).**

DNSAM PDP1

Prelim Recommendation 4:

A registrar MUST review reasonably available data to it in order to satisfactorily determine whether or not associated domains are engaging in DNS Abuse per 3.18.2 of the RAA.

At a minimum, a registrar MUST:

- Review at least one reliable internal data point reasonably accessible to it to determine association; and
- Based on the results of that review, assess whether it is reasonable and appropriate to examine additional indicators, signals, or patterns to determine whether further domain names may be associated with the same actor or activity.

Where the initial review indicates a potential association of abusive activity, the registrar MUST take additional reasonable steps, using data and indicators available to it, to evaluate whether further abusive activity is present within the investigated portfolio. Where the initial review does not indicate such association, the registrar MAY determine that no further investigative steps are necessary, provided that this determination is reasonable and proportionate based on the information available.

DNSAM PDP1

Rec 2 and 3 main changes:

- Provide more context on minimum baseline criteria
- Consideration on what could be considered “reasonable available data”
- Consideration on reseller models

WG discussion:

- Does the WG agree with these changes (in green)?
- Should more language/changes be discussed?
- Are there any major concerns?

Continue discussion strawperson on CQ5 and CQ6

DNSAM PDP1 – CHARTER QUESTION 5

Charter Question 5: If the associated domain checks have an adverse impact on domain name registrants, are there corresponding remedies?

Response to Question:
ADCs MUST rely on applicable legal, contractual, and operational safeguards and MUST be implemented in a manner that is proportionate, evidence-based, and designed to minimize unintended impacts on legitimate registrants, taking reasonable measures to reduce the risk of false positives or erroneous associations. This is similar to the recommendations and responses made in CQ4 and 5.

The WG discussed and noted that existing procedures, contractual obligations, and legal frameworks provide safeguards relevant to conducting ADC. The WG noted that certain remedy-related issues, particularly those connected to mitigation actions such as suspension or takedown, to fall outside the scope of the current PDP and more appropriately addressed through future policy development efforts as noted in the Issue Report.

Pending discussion:

- **Impact Assessment - potential adverse impacts**
- **CQ/Rec to be updated once initial impact assessment is discussed (see next agenda item)**

DNSAM PDP1 – CHARTER QUESTION 6

Charter Question 6: What are appropriate timelines and thresholds for initiating and concluding the associated domain check?

The WG discussed that Registrar MUST initiate and conduct an ADC *promptly* following the trigger as recommended in CQ1 (meaning receipt or identification of actionable evidence of DNS Abuse), taking into account the specific circumstances of each case. For the avoidance of doubt, this requirement does not extend to compromised domains.

In determining what constitutes “prompt” initiation and completion of an ADC, relevant considerations MAY include:

- the severity and immediacy of the DNS Abuse;
- the scale and complexity of the abuse activity under review;
- the need to minimize collateral impact on legitimate registrants; and
- operational realities and information available.

Pending Discussion:

- **WG members asked to Consider 72hr timeline on ADC initiation?**
- **WG members asked to Consider 24hr to initiate ADC?**
- **WG members asked to Consider “prompt but no later than 72hrs”?**

Next Steps on Impact Assessment(s)

Scoped Impact Assessment

- The WG discussed Charter Questions 1–7, including questions that considered potential impacts on Human Rights (HR) and Data Protection (DP).
- As suggested by WG members, Staff and LT is using the WG discussions and input to prepare an scoped assessment of potential HR and DP impacts.
- This scoped assessment is intended to help document and stabilize the current preliminary recommendation language **and is not intended to replace the final comprehensive impact assessments.**
- Once all CQs have been reviewed and the recommendation language further stabilizes, the WG will conduct the final impact assessments.
- This approach was proposed by community members during ICANN85, and the PDP has sought to reflect and operationalize that input throughout its work.

Scoped Impact Assessment

The scoped model is a good idea because it:

- Reduces rework later
- Forces earlier identification of issues
- Keeps recommendations grounded while drafting

- Scoped Impact Assessment DOES NOT replace final impact assessments on ALL CQs and Recommendations.

Scoped Impact Assessment

- We will share scoped assessment with WG by Thursday next week.
- WG members are asked to review the scoped HR and DP assessments and identify any areas that may be missing, unclear, or inaccurately represented **before 8 June.**

Scoped Impact Assessment

Community Reference material for the considered questions and answers include DNSAM PDP1 WG discussion as well as:

- NCSG ICANN85 session on interim HRIA for DNSAM PDP1: https://icann85.sched.com/event/6cf1326584c1b6203f9c7458c1fd3836
- CPS Session on Data Protection Considerations for ADC: https://cpsummit2026.sched.com/event/2GbEx/data-protection-impact-assessment-on-an-associated-domain-check

Iterative Impact Assessment

Human Rights Questions Considered:

1. **Who is affected?**
    - Which groups or stakeholders could be impacted? Are any groups more affected than others?
2. **What action is being proposed and what is the objective?**
3. **Is the objective legitimate and consistent with ICANN's mission? Is the action necessary? is the action proportionate?**
4. **Who was consulted from the groups most affected by this action? What did they say?**
5. **For the rights below, would the proposed action have adverse impact. Are there any other rights not listed above that could be relevant given the specific nature of this action?** (If any right is affected, note how likely the harm is, how serious it would be, and whether it could be undone)
    A. right to privacy
    B. freedom of expression
    C. due process
    D. freedom of association
    E. non-discrimination

Iterative Impact Assessment

Data Protection Questions Considered:

1. What personal data is involved and who does it relate to?
2. What processing is proposed and for what purpose?
3. Is the processing necessary and limited to what is required?
4. What are the privacy risks and how severe are they?
5. What safeguards, controls and accountability mechanisms exist?

AOB

Next Steps

1. Staff to share with the WG the Review Doc with preliminary recommendations (updated based on today's discussion). WG Members to review prelim rec document above and identify any areas of “CANNOT LIVE WITH” before 8 June.

2. Staff to share scoped impact assessment (HR and DP) on current prelim language with WG when ready. WG members to review.

3. Identified areas of concerns/feedback/questions will be added and discussed during ICANN86 Working Sessions.