DNS Abuse Mitigation PDP

PDP Updates & NCSG Positioning

ICANN86 June 2026

Timeline

March - June 2026

Working group kicks off

The group has been meeting on a weekly basis since March 2026. We had 4x kickoff meetings in ICANN85 with 10x meetings since with deliberations on charter questions 1-7.

ICANN86

In-person Working Meetings

During ICANN86, we will have 4x in-person meetings. We will be discussing preliminary language for questions 1-7 shared by ICANN staff and to which all groups ahd to input by 8 June. We will also begin deliberations on questions 8 and 9 (on metrics to evaluate policy effectiveness and how registrars can demonstrate compliance, respectively.

2027-on

Milestones for 2026-on

The project plan aims for deliberations on the charter questions to be completed by November 2026. The draft would then be published in February 2027 with a deadline for public comment in May 2027, with the final report to be submitted to the GNSO Council by June 2027.

Priority Issues for the NCSG

Five Key Areas

Preliminary Recommendation 1: **Associated Domain Check (ADC) Trigger**
Preliminary Recommendation 3: **Defining a ‘reasonable investigation’**
Preliminary Recommendation 5: **Safeguards for ADCs**
Preliminary Recommendation 7: **Topics for consideration to GNSO Council**

Associated Domain Check (ADC) Trigger

What should trigger an ADC?

The WG has been discussing whether a single confirmed abusive domain is sufficient to trigger a full portfolio investigation. Currently, section 3.18.2 of the RAA reads, *"When Registrar has actionable evidence that a Registered Name sponsored by Registrar is being used for DNS Abuse, Registrar must promptly take the appropriate mitigation action(s) that are reasonably necessary to stop, or otherwise disrupt, the Registered Name from being used for DNS Abuse. Action(s) may vary depending on the circumstances, taking into account the cause and severity of the harm from the DNS Abuse and the possibility of associated collateral damage.*

The NCSG's position is that ADCs should be triggered by a combination of contextual signals, not just one reported instance of DNS abuse. This is to mitigate the risk of ADCs being used for profiling and surveillance.

Associated Domain Check (ADC) Trigger

Strawman Language	When a registrar has actionable evidence that a Registered Name is being used for DNS Abuse 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.
NCSG's Response	When a registrar has actionable evidence that a Registered Name is being used for DNS Abuse pursuant to Section 3.18.2 of the RAA, and has at least one credible indicator of coordinated activity that may be associated with the same abusive activity, actor, or campaign, the registrar must perform an Associated Domain Check (ADC). For the avoidance of doubt, this requirement does not extend to compromised

Defining a ‘Reasonable’ Investigation

How to define a ‘reasonable investigation’

The NCSG's position is that the investigation standard must be genuinely proportionate. It must be calibrated to the severity of the suspected abuse, portfolio size, and registrar business model.

Lnauge on data that "may” be used could be acceptable. Language on what data"should” be collected or the requirement to generate new data solely for the purpose of ADC and/or demonstrating compliance would not be acceptable.

Defining a ‘reasonable investigation’

Strawman Language

A reasonable investigation MUST be practical, narrowly-scoped, and proportionate based on the circumstances and consistent with Section 3.18.2. A reasonable investigation IS NOT a general audit of the registrant’s broader portfolio and MUST NOT require registrars to access or generate data that is not reasonably available to them at the time of review, recognizing that registrar capabilities, technical systems, and available data may differ across and within registrars.

Defining a ‘reasonable investigation’

NCSG’s Response

A reasonable investigation MUST be practical, narrowly-scoped, and proportionate based on the circumstances and consistent with Section 3.18.2. A reasonable investigation IS NOT a general audit of the registrant’s broader portfolio and MUST NOT require registrars to access or generate data that is not reasonably available to them at the time of review, recognizing that registrar capabilities, technical systems, and available data may differ across and within registrars.

A reasonable investigation should:

- **Be narrowly scoped**
- **Be targeted towards identifying whether the same registrant or account has other active domains that are also being used for similar abuse**
- **does NOT require registrars to access or generate data that is not reasonably available to them at the time of review.**

Safeguards for ADCs

What options are within the scope of the PDP?

The WG has acknowledged that ADC processes can harm legitimate registrants through wrongful suspensions and erroneous account-level actions. However, deliberations continue as to whether recourse is within the current PDP scope.

NCSG's position is that this cannot be left as a footnote, but at minimum, we contend that registrant recourse must be referred to the GNSO Council as a priority follow-up item. The integration of transparency and accountability mechanisms into the ADC PDP is another alternative pathway.

Safeguards for ADCs

Strawman Language	**An ADC MUST be conducted in compliance with applicable law, contractual requirements, and data privacy safeguards. A registrar MUST NOT be required to collect or generate new data solely for the purpose of ADC and/or demonstrating compliance, unless necessary and proportionate to establish sufficient and reliable evidence. Furthermore, nothing in this policy should be understood to prohibit a registrar from using data, tools, or services that it may lawfully use in the normal course of its operations to investigate DNS Abuse and conduct ADC.**
NCSG's Response	**An ADC MUST be conducted in compliance with applicable law, contractual requirements, and data privacy safeguards. A registrar MUST NOT be required to collect or generate new data solely for the purpose of ADC and/or demonstrating compliance, ~~unless necessary and proportionate~~ to establish sufficient and reliable evidence. Furthermore, nothing in this policy should be understood to prohibit a registrar from using data, tools, or services that it may lawfully use in the normal course of its operations to investigate DNS Abuse and conduct ADC.**

Topics for consideration to GNSO Council

Access to Remedy & Transparnecy/ Accountability

(1) Access to Remedy: A broader, community-wide discussion is needed to develop a baseline standard for registrant access to recourse and remedy mechanisms. The WG raised concerns that including such a mechanism(s) in the ADC PDP would lead to a fragmented, piecemeal process. NCSG's recommendation is to put this forward to the GNSO Council as a topic of relevance to broader DNS abuse mitigation efforts.

(2) Transparency & Accountability Measures: Minimum standards of transparency when it comes to mitigation action(s) is needed. A broader discussion regarding minimum requirements for transaprency reporting on domain suspensions and notification(s) to registrants is also needed.

Topics for consideration to GNSO Council

Strawman Language

During its deliberations, the WG came across topics that were out of scope for this PDP but should be considered by the GNSO Council when considering the follow-up PDPs or next steps on DNS Abuse. Therefore, the WG recommends to GNSO Council to consider further policy work and or next steps as noted in the Final Issue Report on the following two issues that related to broader DNS Abuse Mitigation rather than ADC:

- Limited Transparency in DNS Abuse Mitigation Actions taken (Issue C1 in Final Issue Report)
- Lack of Standard Dispute/Recourse Mechanism for Registrants for mitigation actions taken in response to DNS Abuse (Issue C3 in Final Issue Report)

NCSG's Response

- DNS abuse mitigation safeguards, such as transparency reporting requirements and accountability measures