

DNSAM PDP1 At-Large Questions

At-Large members of the DNS Abuse Mitigation PDP1 on Associated Domain Check want to engage CPWG in the policy work for this PDP by asking questions related to each recommendation.

All with the link to this document can comment and give their input.

A “At-Large copy” of the DNSAM PDP1 Preliminary Recommendations can be found [here](#).

Charter Question 1 - What triggers the requirement to investigate associated domain names?

Preliminary Recommendation 1: Associated Domain Check (ADC) Trigger

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.

What does this recommendation propose?

Under this recommendation, registrars would initiate an Associated Domain Check (ADC) where actionable evidence indicates that a domain name is being used for DNS Abuse pursuant to RAA 3.18.2

The approach is intended to facilitate earlier identification of additional domains potentially connected to the same abusive activity while maintaining an evidence-based threshold. The recommendation explicitly excludes legitimate domains that have been compromised by third parties.

Potential impact on end users

Potential Benefits	Potential Concerns
Earlier identification of domains potentially connected to the same abusive activity.	Investigations could be initiated based on insufficient or inconsistent evidence thresholds.
Ability to initiate ADC investigations before, during, or after mitigation activity.	Different interpretations of “actionable evidence” may result in inconsistent ADC initiation practices.

use of evidence-based thresholds before initiating ADC investigations..	Broad or speculative interpretation of abuse indicators could contribute to overly broad investigations.
.	Lack of consistent application across registrars may affect predictability of investigations.

Global Public Interest Framework / ALAC Considerations

Element	Observation
Security and Stability	The recommendation establishes a trigger for initiating ADCs when actionable evidence of DNS Abuse exists.
Protection of End Users	Earlier review of potentially related domains may assist in identifying broader abusive activity affecting users.
Proportionality	The recommendation ties ADC initiation to actionable evidence and excludes compromised domains.
Accountability	Registrars would determine whether available evidence is sufficient to initiate an ADC.
Minimization of Collateral Harm	Excluding compromised domains may help avoid unnecessary investigative impact on legitimate registrants.
Global Public Interest	The recommendation introduces an operational threshold for initiating ADC investigations related to DNS Abuse.

QUESTIONS FOR CPWG / ALAC DISCUSSION

1. Does the “actionable evidence” standard appear sufficiently robust to initiate an ADC?
2. Could earlier initiation of ADCs assist in identifying broader DNS Abuse activity affecting end users?
3. What do you consider the primary risk if an ADC is initiated based on insufficiently robust evidence?
 - Overly broad investigations
 - Investigations based on unreliable information
 - Disproportionate actions
 - Inconsistent interpretations among registrars
 - Loss of trust in the process

Charter Question 2 - What criteria should be used to define “association” between domains? What elements can be considered to establish such “association”?

Preliminary Recommendation 2: ADC investigation

A registrar MUST perform a “reasonable investigation” in order to determine whether or not “associated domains” are engaging in DNS Abuse per 3.18.2 of the RAA.

What does this recommendation propose?

Under the recommendation, registrars would be required to conduct a reasonable investigation to determine whether associated domains are engaged in DNS Abuse pursuant to RAA 3.18.2 and emphasizes that determinations regarding associated domains should be grounded in a reasonable investigative process supported by available evidence.

Impact on end users

Benefits	Concerns
Additional review of domains potentially connected to abusive activity.	Registrars may apply different interpretations of what constitutes a “reasonable investigation.
Greater emphasis on evidence-supported determinations regarding associated domains.	Investigations may rely on incomplete or insufficiently reliable information.
Potential identification of domains connected to the same abusive activity.	Weak investigative standards could contribute to unsupported association determinations.

Global Public Interest Framework / ALAC Considerations

Element	Observation
Security and Stability	Registrars would be required to conduct investigations regarding associated domains.
Protection of End Users	Investigations involving associated domains may assist in identifying related abusive activity.
Proportionality	The recommendation relies on a “reasonable investigation” standard rather than prescriptive investigative steps.
Accountability	Responsibility for investigative determinations would remain with the registrar.
Evidence-Based Approach	Investigative conclusions would be based on information available to the registrar.
Global Public Interest	The recommendation establishes an investigative obligation related to associated domains.

QUESTIONS FOR CPWG / ALAC DISCUSSION

1. Does the concept of a “reasonable investigation” appear sufficiently robust to support determinations regarding associated domains?
2. Could the recommendation improve identification of associated domains engaging in DNS Abuse affecting end users?
3. What do you consider the primary risk if investigations are conducted without sufficiently reliable information?
 - Weak or unsupported determinations
 - Inconsistent investigative approaches
 - Incorrect identification of related abusive activity
 - Loss of trust in investigative processes
 - Overly broad investigations
4. Does the recommendation provide sufficient guidance for determining whether domains are reasonably associated with abusive activity?

Charter Question 3 - Defining "investigation": What constitutes a "reasonable investigation" by a registrar? What investigation steps are required or recommended? Are the criteria for investigation proportionate and necessary? What is the impact of this investigation on domain name registrants?

Preliminary Recommendation 3: Reasonable investigation

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 of the RAA. A reasonable investigation MUST be practical and proportionate based on the circumstances and consistent with Section 3.18.2. 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.

The ADC MAY 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.

What does this recommendation propose?

The recommendation proposes that a “reasonable investigation” 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 pursuant to RAA 3.18.2.

The text also recognizes that investigative practices may differ depending on registrar capabilities, operational models, technical systems, and available information, and therefore allows flexibility in how reasonable investigations are conducted.

Impact on end users

Benefits	Concerns
More structured approaches for reviewing information related to potentially abusive activity.	Investigative practices may differ depending on registrar capabilities, systems, and available information.
Flexibility for investigations conducted under different operational environments.	Reliance only on reasonably available information could limit identification of certain abusive activity.
More proportionate investigative approaches may help reduce unnecessary impact on legitimate registrants.	Flexible investigative approaches may produce inconsistent investigative outcomes.

Global Public Interest Framework / ALAC Considerations

Element	Observation
Security and Stability	The recommendation describes how registrars would conduct reasonable investigations related to DNS Abuse activity.
Protection of End Users	Review of reasonably available information may assist in identifying domains connected to abusive activity.
Proportionality	Investigations are expected to remain practical and proportionate under the circumstances.
Accountability	Registrars would remain responsible for ensuring that investigations are conducted.
Evidence-Based Approach	The recommendation relies on information reasonably available during normal registrar operations.
Operational Feasibility	The recommendation recognizes differences in registrar systems, capabilities, and operational models.
Global Public Interest	The recommendation establishes a flexible investigative framework rather than a fixed investigative model.

QUESTIONS FOR CPWG / ALAC DISCUSSION

1. Does the recommendation provide a sufficiently clear concept of what constitutes a “reasonable investigation”?

2. What do you consider the primary concern if investigations rely only on information reasonably available to registrars?
 - Inconsistent investigative outcomes
 - Limited ability to identify abusive activity
 - Variations in registrar capabilities and available information
 - Insufficient evidence for reliable determinations
 - Reduced effectiveness of abuse mitigation
3. Does the recommendation provide sufficient flexibility for registrars to conduct investigations under different operational and technical circumstances?
4. Does the flexible and non-exhaustive investigative approach appear appropriate for supporting effective DNS Abuse investigations?

Charter Question 4 - What data access and privacy safeguards are necessary to protect both registrants and registrars during associated domain checks?

Preliminary Recommendation 4: Determining “Association”

To determine whether “association” exists, a registrar MUST take into consideration potential indicators such as the Registered Name Holder or account-related information and/or technical or coordinated activity/behavioral indicator, that is reasonably accessible to the registrar and most likely to yield useful and actionable information. When determining “association,” registrars may take into account what is reasonably available to the registrar; the specific elements considered in any given ADC, even within a single registrar, may vary depending upon the particular circumstances.

What does this recommendation propose?

The recommendation proposes that registrars determine whether “association” exists by considering indicators that are reasonably accessible to them and most likely to provide useful and actionable information regarding DNS Abuse activity. These indicators may include Registered Name Holder or account-related information, as well as technical, coordinated activity, or behavioral indicators. The Working Group also recognized that no single indicator is likely to be determinative in every circumstance and that registrars may need flexibility in assessing potential associations. The recommendation also clarifies that ADC investigations are limited to a registrar’s own portfolio and do not require cross-registrar coordination or checks. Registrars would assess the available information and determine appropriate next steps based on the circumstances of the investigation.

Impact on end users

Benefits	Concerns
----------	----------

Use of multiple indicators to assess whether domains may be associated with abusive activity.	Different indicators may produce inconsistent association determinations across registrars.
Recognition that no single indicator should determine association in all cases.	Reliance on weak or insufficient indicators could contribute to unsupported association conclusions.
Flexibility for registrars to assess technical, operational, or behavioral indicators depending on the circumstances.	Use of account-related or behavioral indicators may raise proportionality concerns in some investigations.

Global Public Interest Framework / ALAC Considerations

Element	Observation
Security and Stability	Registrars may consider multiple indicators when assessing potential associations between domains.
Protection of End Users	The use of technical, operational, or behavioral indicators may assist in identifying related abusive activity.
Proportionality	The recommendation allows registrars to rely on indicators reasonably accessible under the circumstances.
Accountability	Registrars would assess available information and determine appropriate investigative next steps.
Evidence-Based Approach	The recommendation does not rely on a single indicator for determining association.
Data Access and Privacy Considerations	The recommendation limits ADC investigations to information reasonably accessible to the registrar.
Operational Flexibility	The recommendation recognizes that investigative practices and available information may differ across registrars.
Global Public Interest	The recommendation establishes a framework for assessing associations between domains potentially connected to DNS Abuse activity.

QUESTIONS FOR CPWG / ALAC DISCUSSION

1. Does the recommendation provide an appropriate framework for determining whether domains are associated with abusive activity?
2. Could the proposed indicators assist registrars in identifying potentially related abusive activity?
3. What do you consider the primary concern when registrars rely on multiple indicators to determine association?

- Inconsistent determinations across registrars
 - Reliance on insufficient or weak indicators
 - Overly broad association determinations
 - Overreliance on account or behavioral indicators
 - Differences in registrar capabilities and available information
 - Reduced trust in investigative processes
4. Does the flexible and non-exhaustive approach provide sufficient flexibility for determining potential associations between domains?

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

Preliminary Recommendation 5: Safeguards for ADC investigations

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.

However, registrars MUST apply “association” criteria for ADC in a reasonable and proportionate manner taking into consideration the following:

- *the risk of over-association, including scenarios where domains may be linked through reseller models, privacy/proxy services, or shared data that does not reflect common control;*
- *avoid reliance on assumptions that all domains sharing attributes are by default controlled by the same bad actor;*
- *the importance of ensuring that association is based on indicators that are meaningful and actionable, rather than speculative;*
- *the importance of accessing data only when deemed necessary to perform the ADC;*
- *usage of minimum information reasonably available and necessary to determine whether domain names are associated and avoid collecting or processing additional data not needed for that purpose; and,*
- *the potential impact on domain name registrants.*

What does this recommendation propose?

The recommendation proposes that Associated Domain Checks (ADCs) MUST be conducted in compliance with applicable law, contractual requirements, and data

privacy safeguards. Registrars should not be required to collect or generate new data solely for ADC purposes unless necessary and proportionate to establish sufficient and reliable evidence.

The recommendation further states that registrars should apply association criteria in a reasonable and proportionate manner, taking into account risks of over-association, speculative determinations, unnecessary access to information, and potential impacts on domain name registrants. The recommendation also emphasizes limiting access, processing, sharing, and retention of information to what is reasonably appropriate, lawful, and necessary for DNS Abuse investigations.

Impact on end users

Benefits	Concerns
Additional safeguards regarding access, processing, and use of information during ADC investigations.	Safeguards may be implemented differently depending on applicable laws or registrar practices.
Emphasis on limiting collection or processing of information not necessary for investigations.	Existing legal frameworks may provide uneven privacy protections across jurisdictions.
Recognition of risks associated with unsupported or speculative association determinations.	Risks of over-association may remain where domains share infrastructure or services.
More proportionate access to information may help reduce unnecessary impact on registrants.	Different interpretations of what is “necessary” or “proportionate” may produce inconsistent practices.

Global Public Interest Framework / ALAC Considerations

Element	Observation
Security and Stability	The recommendation establishes safeguards applicable to ADC investigations.
Protection of End Users	ADC investigations would continue to be permitted while applying proportionality and privacy safeguards.
Proportionality	The recommendation emphasizes reasonable and necessary access to information.
Accountability	Registrars would remain responsible for applying association criteria appropriately.
Data Minimization	The recommendation discourages collection or processing of information not necessary for the investigation.
Privacy and Data Protection	ADC investigations are expected to comply with applicable law and contractual obligations.
Minimization of Collateral Harm	The recommendation recognizes risks associated with unsupported association determinations.

Operational Flexibility	Safeguards may operate differently across jurisdictions and registrar environments.
Global Public Interest	The recommendation introduces safeguards intended to limit unnecessary access to information during ADC investigations.

QUESTIONS FOR CPWG / ALAC DISCUSSION

1. Does the recommendation provide appropriate safeguards for registrants and registrars during ADC investigations?
2. What do you consider the primary concern regarding the use of association criteria during ADC investigations?
 - Over-association of unrelated domains
 - Reliance on insufficient or speculative indicators
 - Unnecessary access to or processing of information
 - Inconsistent safeguards across registrars or jurisdictions
 - Insufficient protection for registrants affected by ADC investigations
3. Do the proposed safeguards appear sufficient to address risks related to over-association, unnecessary data access, or disproportionate investigative practices?

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

Preliminary Recommendation 6: Timeline for ADC

A Registrar MUST initiate and conduct an ADC promptly following the trigger as defined in Preliminary Recommendation 1, taking into account the specific circumstances of each case. For the avoidance of doubt, this requirement does not extend to compromised domains.

What does this recommendation propose?

The recommendation proposes that registrars MUST initiate and conduct an Associated Domain Check (ADC) promptly following the trigger defined in Preliminary Recommendation 1, while taking into account the specific circumstances of each case. The recommendation explicitly excludes compromised domains from this requirement.

The recommendation further recognizes that what constitutes “prompt” action may depend on factors such as the severity and urgency of the DNS Abuse, the scale and complexity of the activity under review, the need to minimize collateral impact

on legitimate registrants, and operational realities and available information. The recommendation aligns the concept of “promptly” with existing RAA obligations rather than establishing fixed ADC-specific timelines.

Impact on end users

Benefits	Concerns
Prompt initiation of ADC investigations may support earlier review of potentially abusive activity.	Flexible interpretations of “promptly” may result in inconsistent timelines across registrars.
Consideration of operational realities may support more proportionate investigative timing.	Lack of fixed timelines may create uncertainty regarding expected investigative timing.
Consideration of collateral impact may help reduce unnecessary disruption affecting legitimate registrants	Operational limitations or lack of information may affect timeliness of investigations.

Global Public Interest Framework / ALAC Considerations

Element	Observation
Security and Stability	The recommendation requires ADC investigations to be initiated and conducted promptly.
Protection of End Users	Earlier initiation of investigations may assist in reviewing abusive activity affecting users.
Proportionality	Timing considerations include operational realities and potential collateral impact on legitimate registrants.
Accountability	Registrars would remain responsible for conducting ADCs promptly under the circumstances of each case.
Operational Flexibility	The recommendation recognizes that DNS Abuse cases may differ in urgency and complexity.
Minimization of Collateral Harm	The recommendation explicitly references minimizing impact on legitimate registrants.
Consistency of Implementation	Reliance on a contextual “promptly” standard may result in varying implementation practices.
Global Public Interest	The recommendation aligns ADC timing expectations with existing RAA obligations.

QUESTIONS FOR CPWG / ALAC DISCUSSION

1. Does the recommendation provide an appropriate framework for initiating and conducting ADC investigations promptly?
2. Could the recommendation improve timely identification and mitigation of DNS Abuse affecting end users?

3. What do you consider the primary concern regarding the use of a flexible “promptly” standard for ADC investigations?
 - Inconsistent timelines across registrars
 - Delays in abuse mitigation
 - Lack of clarity regarding expected response times
 - Operational limitations affecting investigations
 - Potential collateral impact on legitimate registrants
4. Does the flexible ‘promptly’ standard provide sufficient clarity regarding expected timing for ADC investigations?
5. Does aligning ADC timelines with existing RAA obligations appear appropriate rather than establishing fixed ADC-specific timelines?

Charter Question 7 - What specific requirements are necessary to implement this policy and what parts can be subject to best practices, or potentially left to the discretion of the contracted party?

Preliminary Recommendation 7: Topics for consideration to GNSO Council

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)

What does this recommendation propose?

The recommendation proposes that the GNSO Council consider future policy work or next steps regarding broader DNS Abuse mitigation issues identified by the Working Group as outside the scope of the current PDP. These topics include:

- limited transparency regarding DNS Abuse mitigation actions; and
- the lack of a standard dispute or recourse mechanism for registrants affected by DNS Abuse mitigation actions.

The recommendation further recognizes that these issues relate more broadly to DNS Abuse mitigation frameworks and enforcement outcomes rather than the narrower operational scope of Associated Domain Checks (ADCs). As a result, the Working Group concluded that these topics would be more appropriately

addressed through future policy development efforts or other next steps outside of this PDP.

Impact on end users

Benefits	Concerns
Identification of transparency and recourse issues for possible future policy consideration.	Transparency and recourse issues remain unresolved within the current PDP framework.
Opportunity for future discussions regarding mitigation transparency and registrant recourse mechanisms.	Future approaches to transparency or recourse may vary across contracted parties.
	The timing and scope of future policy work remain uncertain.

Global Public Interest Framework / ALAC Considerations

Element	Observation
Accountability	The recommendation identifies transparency and recourse as possible areas for future policy work.
Transparency	Limited transparency regarding DNS Abuse mitigation actions is identified as an issue outside the scope of this PDP.
Registrant Recourse Considerations	The recommendation recognizes the absence of standardized recourse mechanisms related to mitigation actions.
Protection of End Users	Future discussions regarding transparency or recourse mechanisms may affect how mitigation actions are experienced by users and registrants.
Operational Scope Clarity	The recommendation clarifies that these issues fall outside the operational scope of ADC investigations.
DNS Abuse Governance Considerations	The recommendation identifies broader DNS Abuse governance issues for possible future consideration.
Global Public Interest	The recommendation identifies issues that may be considered in future DNS Abuse policy work outside the scope of this PDP.

Questions for CPWG / ALAC Discussion

1. Does the recommendation appropriately identify transparency and recourse issues as topics for future policy consideration outside the scope of this PDP?
2. What do you consider the primary concern regarding issues identified for future DNS Abuse policy work?
 - Limited transparency regarding mitigation actions
 - Lack of standardized recourse mechanisms for registrants
 - Variability in future approaches across contracted parties

- Uncertainty regarding future policy development
 - Potential impact on trust and accountability
3. Should issues related to transparency and recourse be considered in future DNS Abuse policy work outside the scope of this PDP?