

ICANN | GAC

Governmental Advisory Committee

Status	Final
Distribution	Public
Date	28 September 2026

Governmental Advisory Committee Comments on the Initial Report of the DNS Abuse Mitigation PDP1 Working Group on Associated Domain Checks (ADC)

These GAC comments are proposed in response to the [ICANN Public Comment proceeding](#) on “Initial Report of the DNS Abuse Mitigation PDP1 Working Group on Associated Domain Checks (ADC)” opened on 18 August 2026 and closing on 28 September 2026.

While input is requested (and will be provided) through a specific “guided input form”, for ease of reading, and reference, this document includes the text of the Preliminary Recommendations in the DNS Abuse PDP1 [Initial Report](#). For each of these, each community group is asked to indicate its level of support as well as its reasoning where applicable. 5 choices are offered:

- *Support Recommendation as written*
- *Support Recommendation intent with wording change*
- *Significant change required: changing intent and wording*
- *Do not support Recommendation: Recommendation should be deleted*
- *Other*

Table of contents

		Level of GAC Support
Summary of GAC Submission	3	
GAC Input in the “Guided Submission Form”	4	
Recommendation 1: Associated Domain Check Trigger	4	
Preliminary Recommendation 1	4	(Support as written)
Preliminary Implementation Guidance 1.1	4	(Support as written)
Rationale on Preliminary Recommendation 1 and Preliminary Implementation Guidance 1.1	5	(No comment)
Recommendation 2: Associated Domain Check Investigation	5	
Preliminary Recommendation 2	5	(Support as written)
Recommendation 3: Reasonable Investigation	6	
Preliminary Recommendation 3	6	(Support as written)
Preliminary Implementation Guidance 3.1	6	(Support as written)
Recommendation 4: Determining “Association”	7	
Preliminary Recommendation 4	7	(Support as written)
Preliminary Implementation Guidance 4.1	7	(Support as written)
Rationale on Preliminary Recommendations 2–4	8	(No comment)
Recommendation 5: Safeguards for ADC Investigations	9	
Preliminary Recommendation 5	9	(Support as written)
Preliminary Implementation Guidance 5.1	9	(Wording change)
Rationale on Preliminary Recommendation 5 and Preliminary Implementation Guidance 5.1	10	(No Comment)
Recommendation 6: Timeline for ADC	11	
Preliminary Recommendation 6	11	(Support as written)
Preliminary Implementation Guidance 6.1	11	(Support as written)
Rationale on Preliminary Recommendation 6 and Preliminary Implementation Guidance 6.1	11	(No Comment)
Recommendation 7: Measuring ADC Policy Effectiveness	12	
Preliminary Recommendation 7	12	(Support as written)
Rationale on Preliminary Recommendation 7	12	(No Comment)
Recommendation 8: Demonstrating Compliance	13	
Preliminary Recommendation 8	13	(Wording change)
Rationale on Preliminary Recommendation 8	14	(No Comment)
Expected Impact of Recommendations (Section 3 of PDP1 Initial Report)	15	
HRIA Analysis for DNSAM PDP 1	15	(No Comment)
GPI Checklist	15	(No Comment)
Consideration of Data Privacy Issues	15	(No Comment)
Consensus Policies	15	(No Comment)
Other Comments	16	

Summary of GAC Submission

The GAC welcomes the clarity of Recommendation 1 on the ADC trigger and strongly supports its Preliminary Implementation Guidance. In particular, it agrees that “is being used for DNS Abuse” should not be limited to abuse occurring at the exact time of review. Registrars should be able to rely on evidence of current, recent, intermittent, recurring, or otherwise well-evidenced abuse, including where a domain is no longer active or the activity has ceased. This is a sensible approach, as malicious actors often use domain names only briefly or intermittently.

Regarding Recommendation 5: Safeguards for ADC investigations, and especially Preliminary Implementation Guidance 5.1, the GAC is concerned that referencing a “need to protect Registered Name Holders and registrars” could hinder effective investigations. It is important to ensure that legitimate Registered Name Holders are not subject to unnecessary or disproportionate internal registrar investigations under the ADC policy.

However, this concern must be balanced against the clear public policy need for ICANN-accredited registrars to investigate domains used by cybercriminals to conduct large-scale phishing campaigns and other types of DNS Abuse. In this regard, the GAC’s Human Rights and International Law Working Group urges the PDP working group to always keep in mind the impact of inaction or ineffective registrar investigations on the end user’s right to property, their rights to privacy and personal data protection, and their right to obtain justice.

Finally, the GAC notes the flexibility given to registrars in how they chose to implement the ADC policy, but expects ICANN Compliance to ensure consistent application under Recommendation 8: Demonstrating Compliance. The GAC also welcomes a review after two years, as proposed in Recommendation 7, to assess its effectiveness.

The GAC appreciates the opportunity to share its perspective on the Initial Report and looks forward to the finalisation of the document, the adoption of this policy, and its swift implementation prior to the addition of new gTLDs to the Internet’s Domain Name System

GAC Input in the “Guided Submission Form”

Recommendation 1: Associated Domain Check Trigger

Preliminary Recommendation 1

When a registrar has actionable evidence that a Registered Name is being used for DNS Abuse as defined in 3.18.1 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 domain names.

Level of GAC Support: **Support Recommendation as written**

GAC Rationale: The GAC appreciates the clarity of recommendation 1 on the ADC trigger.

Preliminary Implementation Guidance 1.1

When reviewing actionable evidence for the purpose of ADC, the phrase “is being used for DNS Abuse” is not limited to DNS Abuse that is occurring at the time of review. Registrars may rely on actionable evidence of current, recent, intermittent, recurring, or otherwise well-evidenced DNS Abuse, including where the Registered Name is no longer active or the abusive activity has ceased. Abuse reports submitted to a registrar should include sufficient information and evidence to support the reported allegation of DNS Abuse pertaining to the same abuse scheme and/or abusive actor, where relevant. Where the reported abuse is intermittent, recurring, or otherwise not continuously observable, the report should include evidence clearly demonstrating the pattern of abusive activity.

Furthermore, the WG further considered, as noted in the Charter, that an ADC is most appropriately required where the registrar has sufficient indicators to reasonably determine that the Registered Name has been registered for the purpose of conducting DNS Abuse, rather than where a legitimate domain is being primarily used for purposes other than DNS Abuse and would fall under the category of compromised domains. A Compromised Domain means a domain name that was registered for legitimate purposes but is subsequently exploited, or controlled by an unauthorized party to conduct DNS Abuse without the knowledge, authorization, or participation of the registrant and/or when an otherwise legitimate or benign domain name is used as a vector for DNS Abuse without the knowledge or consent of the registrant

Level of GAC Support: **Support Recommendation as written**

GAC Rationale:

The GAC strongly supports Rec 1 Preliminary Implementation Guidance which indicates that “*when reviewing actionable evidence for the purpose of ADC, the phrase “is being used for DNS Abuse” is not limited to DNS Abuse that is occurring at the time of review. Registrars may rely on actionable evidence of current, recent, intermittent, recurring, or otherwise well-evidenced DNS Abuse, including where the Registered Name is no longer active or the abusive activity has ceased*”. This approach is very sensible considering that malicious actors often weaponise domain names for a short amount of time or on an intermittent basis.

Rationale on Preliminary Recommendation 1 and Preliminary Implementation Guidance 1.1

The WG considered that the trigger for an ADC should remain tied to Section 3.18.2 of the RAA and to the registrar having actionable evidence of DNS Abuse. The trigger avoids potentially onerous demands on registrars, which could arise from an overly broad or speculative trigger, such as relying on an unsubstantiated report of DNS Abuse or a prediction of future abuse behavior. The requirements under section 3.18.2 of the RAA do not establish limitations on where the actionable evidence is acquired. What this means, in a practical sense, is that the registrar can identify the actionable evidence through its own analysis or the registrar can be informed by a report from any external reporter, both may constitute valid sources of actionable evidence under the RAA.

Actionable evidence as defined in the ICANN Advisory on Compliance With DNS Abuse Obligations means that the information that is readily available to the registrar must be sufficient to enable the registrar to make a reasonable determination as to whether the Registered Name is being used for one or more forms of DNS Abuse. Registrars are encouraged to proactively monitor the Registered Names that they sponsor to identify potential DNS Abuse. A registrar's assessment of actionable evidence will vary depending on the circumstances of each case. Abuse reports submitted to a registrar should include sufficient information and evidence to support the reported allegation of DNS Abuse. Where the reported abuse is intermittent, recurring, or otherwise not continuously observable, the report should include evidence reasonably demonstrating the pattern of abusive activity.

The WG discussed whether the obligation to perform an ADC should be conditioned on the registrar having completed mitigation action in respect of the domain name that triggered the ADC. However, the WG concluded that an ADC is part of a proactive mitigation action to identify whether one or more associated domains have been registered for the purpose of conducting DNS Abuse. Hence, relative to the triggering domain name, an ADC can be performed prior to taking mitigation action; in parallel with mitigation action; or where the registrar has already taken or is in the process of taking appropriate mitigation action. The WG discussed that the trigger for ADC should not substantially delay prompt mitigation action on already existing obligations.

GAC Comments: None

Recommendation 2: Associated Domain Check Investigation

Preliminary Recommendation 2

A registrar **MUST** perform a reasonable investigation in order to determine whether or not associated domains are used for DNS Abuse as defined in 3.18.1 of the RAA.

Level of GAC Support: **Support Recommendation as written**

GAC Rationale: None

Recommendation 3: Reasonable Investigation

Preliminary Recommendation 3

A reasonable investigation by a registrar **MUST** consist of reviewing information reasonably accessible to the registrar in the normal course of its operations to determine whether associated domain names are being used for DNS Abuse as defined in 3.18.1 of the RAA. For the purposes of this Recommendation, information reasonably accessible to the registrar includes, but is not limited to, information ordinarily accessible to the registrar through its contractual obligations, technical systems, and abuse reports.

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 accessible to them, recognizing that registrar capabilities, technical systems, and available data may differ across and within registrars.

Registrars **MAY** conduct an ADC by 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.

Level of GAC Support: **Support Recommendation as written**

GAC Rationale: None

Preliminary Implementation Guidance 3.1

The categories of reasonably accessible information identified in Recommendation 3 establish the minimum baseline for a reasonable investigation. A reasonable investigation does not require consideration of every category in every case but should address those categories that are reasonably relevant under the circumstances. The Recommendation does not prescribe how registrars should review, prioritize, or weigh that information, recognizing that registrar capabilities, technical systems, business models, and the facts and circumstances of individual cases may differ.

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.
- Registrars will remain responsible for all relevant contractual obligations, as required by 3.12 of the RAA. This means the registrar is fully responsible for complying with all RAA requirements (including 3.18) even when it uses a Reseller

Level of GAC Support: **Support Recommendation as written**

GAC Rationale: None

Recommendation 4: Determining “Association”

Preliminary Recommendation 4

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

Level of GAC Support: **Support Recommendation as written**

GAC Rationale: None

Preliminary Implementation Guidance 4.1

When determining whether association exists, the indicators taken into consideration by the registrar **MAY** include, but are not limited to, the following factors as applicable and as available:

- domains within the same account, customer, Registered Name Holder, end customer, or other potential common connection point;
- 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; or
- 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.

Level of GAC Support: **Support Recommendation as written**

GAC Rationale: None

Rationale on Preliminary Recommendations 2–4

The WG recommends that registrars may use a range of technical, operational, or abuse intelligence signals, recognizing that different association indicators (e.g., account identifiers, infrastructure patterns, or registration activity signals) may be relevant depending on the circumstances, and that no single data point will be determinative in all cases. The policy should not prescribe a fixed or exhaustive sequence of investigation steps, but should allow registrars to apply a reasonable range of indicators and pattern recognition signals appropriate to the circumstances. This policy only requires ADC within a registrar portfolio and does not require cross-registrar checks/coordination. A reasonable investigation should remain distinct from mitigation, meaning registrars should assess available evidence first and determine proportionate next steps based on that assessment. The WG intends that ADCs remain evidence-driven and proportionate. The recommendation is not intended to require registrars to conduct portfolio-wide reviews as a matter of course. At the same time, the WG recognizes that the facts and circumstances of a particular case may justify a broader review. Accordingly, the recommendation neither mandates nor prohibits a more comprehensive investigation where such action is reasonable and proportionate under the circumstances. For the avoidance of doubt, a proportionate investigation is one that is reasonably tailored to the available evidence and the nature, scope, and severity of the reported DNS Abuse. The WG understands that proportionality may support reviewing a limited number of associated domains in some cases, while in other cases a broader review may be justified where the evidence indicates a larger coordinated abuse campaign, multiple related domains, or other factors suggesting that abuse extends beyond the reported domain name.

GAC Comments: No comment

Recommendation 5: Safeguards for ADC Investigations

Preliminary Recommendation 5

ADC MUST be conducted in compliance with applicable law(s) (including data privacy laws) and contractual requirements. 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.

Level of GAC Support: **Support Recommendation as written**

GAC Rationale: None

Preliminary Implementation Guidance 5.1

Registrars SHOULD apply “association” criteria for ADC in a reasonable and proportionate manner taking into consideration the following (non-exhaustive) criteria:

- 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;
- avoiding reliance on assumptions that all domains sharing only certain attributes are by default controlled by the same malicious 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 the 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;
- the potential impact on ~~legitimate domain name~~ Registered Name Holders.

In implementing this recommendation, registrars will not be required or expected to take any action in contravention of applicable law, including internationally recognized privacy principles, as appropriate. Implementation of this Policy should not be interpreted as requiring registrars to process more personal data than is reasonably necessary to perform an ADC, or otherwise to act in a manner that disproportionately impacts the fundamental rights of ~~legitimate~~ Registered Name Holders. The WG recommends that a registrar conducting an ADC SHOULD limit access to and correlation of data to what is reasonably accessible for the investigation, taking into account the purpose of the check and the nature of the evidence, ~~and the need to protect Registered Name Holders and registrars~~. The policy SHOULD avoid creating an overly prescriptive framework and instead rely on high-level safeguards (as noted above) that can operate across different jurisdictions, business models, and technical environments. Any approach to retention of investigation results SHOULD be consistent with applicable law and existing contractual obligations, rather than creating a separate, retention regime under this policy. However, proportionate and lawful sharing of relevant information SHOULD be permitted where necessary for effective abuse mitigation or compliance with applicable law or contractual obligations.

Level of GAC Support: **Support Implementation Guidance intent with wording change**

GAC Rationale:

With regards to Safeguards for ADC investigations and particularly Rec 5 Preliminary Implementation Guidance 5.1, the GAC highlights that the last part of the sentence “the WG recommends that a registrar conducting an ADC SHOULD limit access to and correlation of data to what is reasonably accessible for the investigation, taking into account the purpose of the check and the nature of the evidence, and the need to protect Registered Name Holders and registrars” is repetitive and could impede effective registrar investigations.

While the GAC understands the importance of protecting legitimate Registered Name Holders from unnecessary or overreaching investigations infringing their rights, the prevailing purpose of the PDP is to prevent DNS abuse by cybercriminals who maliciously register multiple domains to further their abusive schemes (such as large scale phishing attacks, which remain among the most common category of cybercrime reported to law enforcement

(https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf).

The GAC's Human Rights and International Law Working Group emphasizes that the rights of end users victimized by DNS abuse - their rights to property, privacy, personal data protection, and their right to obtain justice - must always be kept in mind when considering the ultimate goal of the ADC policy development process.

The GAC believes it important to balance such rights against the need to appropriately investigate domains weaponised by malicious actors. The GAC therefore suggests, as indicated above, to: a) add "legitimate" before Registered Name Holders and b) delete the following repetitive text: "and the need to protect Registered Name Holders and registrars," as relevant safeguards are already described in the foregoing sentences.

Rationale on Preliminary Recommendation 5 and Preliminary Implementation Guidance 5.1

WG members agreed that existing registrar contracts and laws already provide core safeguards. Furthermore, WG members said that ADCs must account for registrar agreements, GDPR, and country-specific laws. They proposed that registrars should access only data reasonably appropriate for DNS Abuse investigations and only for the investigation period. Some WG members said applicable law alone is insufficient because some jurisdictions lack strong privacy protections. Additionally, they clarified privacy concerns related to personal data, not technical checks like nameservers. WG members noted the policy should not discourage proactive investigations and recommend against adding new retention regimes beyond existing legal or contract requirements.

GAC Comments: No comment

Recommendation 6: Timeline for ADC

Preliminary Recommendation 6

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 domain names.

Level of GAC Support: **Support Recommendation as written**

GAC Rationale: None

Preliminary Implementation Guidance 6.1

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 Registered Name Holders; and
- operational realities and information available.

Level of GAC Support: **Support Recommendation as written**

GAC Rationale: None

Rationale on Preliminary Recommendation 6 and Preliminary Implementation Guidance 6.1

The WG recommends that registrars may use a range of technical, operational, or abuse intelligence signals, recognizing that different association indicators (e.g., account identifiers, infrastructure patterns, or registration activity signals) may be relevant depending on the circumstances, and that no single data point will be determinative in all cases. The policy should not prescribe a fixed or exhaustive sequence of investigation steps, but should allow registrars to apply a reasonable range of indicators and pattern recognition signals appropriate to the circumstances. This policy only requires ADC within a registrar portfolio and does not require cross-registrar checks/coordination. A reasonable investigation should remain distinct from mitigation, meaning registrars should assess available evidence first and determine proportionate next steps based on that assessment. The WG intends that ADCs remain evidence-driven and proportionate. The recommendation is not intended to require registrars to conduct portfolio-wide reviews as a matter of course. At the same time, the WG recognizes that the facts and circumstances of a particular case may justify a broader review. Accordingly, the recommendation neither mandates nor prohibits a more comprehensive investigation where such action is reasonable and proportionate under the circumstances. For the avoidance of doubt, a proportionate investigation is one that is reasonably tailored to the available evidence and the nature, scope, and severity of the reported DNS Abuse. The WG understands that proportionality may support reviewing a limited number of associated domains in some cases, while in other cases a broader review may be justified where the evidence indicates a larger coordinated abuse campaign, multiple related domains, or other factors suggesting that abuse extends beyond the reported domain name.

GAC Comments: No comment

Recommendation 7: Measuring ADC Policy Effectiveness

Preliminary Recommendation 7

Following implementation of the ADC policy, ICANN org should conduct a review of the policy's effectiveness after two years. The review should assess whether the policy is achieving its intended purpose and what, if anything, could be improved. The ICANN org review may consider both quantitative and qualitative indicators to measure whether the policy has achieved its below noted intent.

The policy's intended purpose, namely is to:

- establish a consistent minimum baseline across registrars for conducting ADCs when the policy obligation is triggered;
- ensure that compliance with the ADC obligations can be effectively assessed and enforced by ICANN Contractual Compliance and, where appropriate, can act when obligations are not met; and
- contribute to the timely identification and disruption of DNS Abuse campaigns, through the application of ADCs, recognizing that the policy is one of several measures intended to mitigate DNS Abuse.

To support the review, ICANN org should work with the IRT to identify a limited set of aggregated data points that enable ICANN org to assess whether the policy has achieved its intended outcomes. Such data points should, to the extent feasible, be derived from information available to ICANN Contractual Compliance, ICANN's Office of the CTO (OCTO), and a limited set of aggregated information maintained by registrars in the ordinary course of business.

Level of GAC Support: **Support Recommendation as written**

GAC Rationale:

The GAC welcomes a review of this policy after two years, as suggested by Rec 7 -- Measuring ADC policy effectiveness, in order to ensure the above expectations are met and that there is progress towards the overarching policy objective of "requiring registrars to proactively pivot to investigate domain names linked to malicious actors, particularly in cases of high-volume domain registrations used for DNS Abuse campaigns".

Rationale on Preliminary Recommendation 7

The WG discussed and noted that the review should recognize that DNS Abuse is dynamic and that direct causation between this policy and overall abuse levels may be difficult to establish. The review should therefore avoid relying solely on aggregate abuse-volume statistics and should instead assess the policy's practical effectiveness in improving ADC performance and compliance. The WG expects the IRT to work on the identification of the relevant data points to assess the indicators noted above, as well as the establishment of baseline data for future measurement. IRT to consider whether and how metrics on ADC metrics can be included in the regular DNS Abuse mitigation metrics already produced by ICANN.

GAC Comments: No comment

Recommendation 8: Demonstrating Compliance

Preliminary Recommendation 8

Registrars MUST be able to demonstrate compliance with the ADC requirements, through records and documentation maintained in the ordinary course of business, when the obligation is triggered by actionable evidence of DNS Abuse. Some of the data points that MAY be sufficient to show compliance include:

- The trigger and time of trigger of the ADC.
- Whether and when an ADC was conducted.
- What information was reviewed that was reasonably accessible ~~directly to~~ by the registrar or through its reseller at the time.
- Whether, and how many, associated domains were identified.
- What resulting action, if any, was taken in relation to associated domains.
- That the ADC process followed was reasonable and proportionate under the circumstances.

The policy MUST not prescribe a format for ~~documentation~~ documenting compliance. Registrars may maintain evidence in ~~varying~~ forms, provided the evidence is sufficient to demonstrate compliance with the ADC requirements.

A registrar MUST develop and maintain an internal process description for conducting ADCs. This internal process should describe the steps the registrar uses when an ADC is conducted and should take into account any applicable ADC advisory or implementation guidance. The internal process MUST be made available to ICANN upon request.

Level of GAC Support: **Support Recommendation intent with wording change**

GAC Rationale:

The GAC notes that the recommendations give considerable flexibility to registrars in implementing the policy according to their specific business models and back-end systems. Despite possible different implementation approaches at the registrars' level, the GAC expects that ICANN Compliance will be able to ensure a consistent application of this policy based upon the obligations laid down in Recommendation 8.

The wording change is proposed for streamlining and clarity purposes.

Rationale on Preliminary Recommendation 8

The WG intends for this recommendation to be demonstrable and auditable without requiring registrars to create extensive new recordkeeping systems solely for ADC purposes. The purpose of the recommendation is to enable verification that an ADC was conducted and that resulting decisions were supported by a reasonable investigation. The WG expectation is that registrars maintain sufficient records, generated in the ordinary course of business, to demonstrate compliance with the policy requirements. Recommendation 5 is intended to avoid creating a requirement for registrars to collect or generate new data solely for the purpose of conducting an ADC. Recommendation 8 recognizes that registrars **MUST** be able to demonstrate compliance with the policy through reasonable documentation, internal procedures, and records maintained in the ordinary course of business or developed as part of implementing these requirements.

The intent is to ensure that compliance can be demonstrated without creating unnecessary operational burdens for registrars, or resulting in unnecessary collection or processing of data relating to Registered Name Holders. Recommendation 8 and 5 recognize that registrars may need to establish internal procedures, workflows, and, where necessary, compliance records to demonstrate that ADC obligations have been met.

GAC Comments: No comment

Expected Impact of Recommendations (Section 3 of PDP1 Initial Report)

The WG conducted a scoped impact assessment during its deliberations as an opportunity to raise material risks and obvious conflicts through WG input. The scoped assessment was intended to help document and stabilize the current preliminary recommendation language and was not intended to replace the final comprehensive impact assessments. The WG completed its scoped impact assessment as captured in this document: [Scoped Impact Assessment DNSAM PDP 1](#).

Once the WG Preliminary Recommendations became more stable, the WG conducted its comprehensive impact assessments as summarized below and accessible [here](#).

[HRIA Analysis for DNSAM PDP 1](#)

The worksheet presents a detailed Human Rights Impact Assessment (HRIA) of the preliminary recommendations. It assesses potential effects on relevant human rights (primarily privacy, due process, freedom of expression, freedom of association) and concludes that the Preliminary Recommendations are expected to have limited adverse impacts because ADCs are restricted to investigations based on actionable evidence that a Registered Name is being used for DNS Abuse, must comply with applicable law and contractual requirements, and emphasize proportionality. Overall, the assessment finds that the recommendations appropriately balance DNS abuse mitigation with protection of registrant rights. Furthermore, it shows that In this context, the WG worked to develop more consistent baseline requirements and expectations across registrars, including with respect to proportionality, evidentiary standards, safeguards, operational considerations, and efforts to minimize false positives and collateral impacts on Registered Name Holders.

[GPI Checklist](#)

The worksheet assesses the Preliminary Recommendations against the Global Public Interest (GPI) framework. It considers whether the Preliminary Recommendations advance objectives such as DNS security and stability, benefit to the Internet community, and ICANN's technical coordination. The analysis concludes that the Preliminary Recommendations generally align with the GPI principles by strengthening DNS abuse mitigation while preserving operational flexibility for registrars and incorporating safeguards to avoid unnecessary burdens or overreach that could impact Registered Name Holders.

[Consideration of Data Privacy Issues](#)

The worksheet evaluates the Preliminary Recommendations from a data privacy policy perspective rather than providing a legal opinion. It examines whether ADCs require processing of personal data, whether such processing is necessary and proportionate, any potential associated privacy risks, and the safeguards available and discussed to mitigate those risks. The assessment concludes that privacy risks are low because the recommendations limit investigations to reasonably accessible information, discourage creation of new data solely for ADC, and require compliance with applicable laws.

[Consensus Policies](#)

The worksheet reviews existing ICANN Consensus Policies to determine whether and how the DNSAM PDP 1 Preliminary Recommendations would affect them. It catalogues current policies across areas such as registration data, transfers, expiration, registry services, and rights protection, and assesses the expected impact of the proposed recommendations. The overall conclusion is that the recommendations would have minimal to no impact on existing Consensus Policies, as they are expected to establish a new consensus policy governing ADCs rather than substantially modifying existing policy obligations.

GAC Comments: No comment

Other Comments

Part 1 - GAC comments on further work on Associated Domain Checks

The GAC acknowledges that additional topics were discussed by the Working Group during its deliberations which fell out of scope of the PDP Charter but which could increase the effectiveness of the ADC policy.

The GAC notes that cross-registrar information sharing on ADC results and the discovery of large-scale DNS abuse campaigns could significantly increase the speed and effectiveness of DNS abuse mitigation when, as very often occurs, those campaigns exploit domains registered across different registrars.

Beyond cross-registrars information sharing, and under lawful and specific conditions, it would be beneficial to also share useful information stemming from the registrars' Associated Domain Checks (i.e., on large scale DNS abuse campaign being conducted) with law enforcement authorities, CERTs and other relevant authorities and stakeholders, particularly from targeted countries.

The GAC encourages ICANN org and the community to explore avenues for strengthening collaboration to this effect.

Finally, the GAC acknowledges that compromised domains fall outside the scope of the current PDP. However, the GAC notes that, in many countries, the compromise of legitimate but poorly secured local websites is the dominant form of abuse. The GAC therefore encourages ICANN org and the community to begin discussions on how to address this issue, building on the exchanges and evidence gathered during this PDP.

Part 2 - Additional GAC considerations (applicable beyond ADC)

Beyond the specific work of this PDP, the GAC wishes to offer additional considerations on DNS abuse:

- **Capacity building on abuse reporting and language accessibility:** in many developing countries, particularly landlocked developing countries and least developed countries, DNS service providers are often located outside national jurisdictions. In such circumstances, and in the absence of strong institutional relationships with registrars and registries, the quality and credibility of the DNS abuse report submitted may be the only means of ensuring that reported abuse is addressed. It is therefore important for ICANN to invest in the development and publication of standardised, evidence-ready reporting templates, enabling smaller administrations to consistently meet the expectation of providing "sufficient information and evidence". In addition, providing guidance and templates in languages other than English would be especially beneficial in this context.
- **Adequacy of ICANN DNS abuse policies to different countries and jurisdictions:** as ICANN policies apply globally, it is important to assess whether they produce equivalent results across different countries and jurisdictions, particularly in those characterised by the absence of local DNS service providers and/or by a concentration of shared hosting and reseller models. The GAC invites ICANN org to monitor whether DNS Abuse reports originating from these jurisdictions receive the same timeliness and quality of response as reports submitted elsewhere, and whether the application of ICANN policies may inadvertently disadvantage legitimate domain name holders based in these countries.