

SAC135

SSAC Comments on the Initial Report of the GNSO DNS Abuse Mitigation Policy Development Process 1

Preface

This is a public comment to the ICANN community from the ICANN Security and Stability Advisory Committee (SSAC) in response to a call for comments on the Initial Report of the GNSO DNS Abuse Mitigation Policy Development Process 1 Working Group.

The SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), technical administration matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to other parties, and the advice offered here should be evaluated on its merits. SSAC members participate as individuals, not as representatives of their employers or other organizations. SSAC consensus on a document occurs when the listed authors agree on the content and recommendations with no final objections from the remainder of the SSAC, with the exception of any withdrawals included at the end of the document.

Table of Contents

Preface.....	2
Table of Contents.....	3
1 Introduction.....	4
2 General Comments.....	4
3 Candidate Association Signals for Identifying Domains Related to a Trigger Domain.....	5
3.1 Availability of Signal Data.....	6
3.2 Understanding the Signal Ratings.....	7
3.3 Signal Attributes.....	7
3.4 Signal Categories.....	8
3.5 Candidate Association Signals by Category.....	9
3.6 Applying the Candidate Signals.....	11
3.7 Illustrative User Stories.....	12
4 Measuring Policy Effectiveness (Preliminary Recommendation 7).....	13
4.1 Two Distinct Questions.....	13
4.2 Input to the IRT on Indicators and Baselines.....	15
5 Demonstrating Compliance (Preliminary Recommendation 8).....	17
5.1 What the Records Need to Separate.....	17
5.2 How Compliance Can Use the Records.....	18
6 Matters Outside the Scope of the PDP.....	18
7 Recommendations.....	19
8 Acknowledgments, Disclosures of Interest, and Withdrawals.....	19
8.1 Acknowledgments.....	20
8.2 Disclosures of Interest.....	20
8.3 Withdrawals.....	20
Appendix A: Candidate Signal Glossary.....	21

1 Introduction

The Generic Names Supporting Organization (GNSO) Domain Name System (DNS) Abuse Mitigation Policy Development Process 1 (DNSAM PDP 1) Working Group published its Initial Report on 18 August 2026 for public comment. The Initial Report contains preliminary recommendations and implementation guidance that would require registrars to conduct an Associated Domain Check (ADC) when they have actionable evidence that a Registered Name is being used for DNS Abuse. The Security and Stability Advisory Committee (SSAC) welcomes this opportunity to provide input and thanks the Working Group for its work in developing this report.

The SSAC supports the preliminary recommendations and implementation guidance as a workable and proportionate baseline for conducting ADCs. In this comment, the SSAC provides supplementary rationale for its support, technical input on how a registrar determines that domains are associated, and specific recommendations on the measurement of the policy's effectiveness and the demonstration of compliance. The SSAC offers the technical input as material for implementation guidance and for the Implementation Review Team (IRT).

This report is not a checklist of required checks, a legal analysis of privacy, or a position on mitigation. What a registrar does with the domains an ADC identifies remains governed by Section 3.18.2 of the Registrar Accreditation Agreement (RAA) and applicable law.

2 General Comments

The SSAC supports the preliminary recommendations, which establish a workable and proportionate baseline for conducting ADCs. This section documents the SSAC's rationale for its responses to the guided public comment submission form. It states briefly why the SSAC supports each preliminary recommendation and implementation guidance item; detailed input follows in Sections 3 through 5.

Preliminary Recommendation 1 and Implementation Guidance 1.1. The trigger is tied to the existing standard of actionable evidence under RAA 3.18.2. The rationale confirms that the evidence may come from the registrar's own detection or from any external reporter. Implementation Guidance 1.1 confirms that "is being used" is not limited to abuse observable at the time of review. This matters because malicious registrations are often dormant, intermittent, or already offline when a well-evidenced report¹ arrives. The exclusion of compromised domains is correct. Pivoting on the registrant of a compromised domain surfaces that registrant's legitimate holdings rather than a portfolio of malicious registrations.

Preliminary Recommendations 2 through 4 and Implementation Guidance 3.1 and 4.1. The MUST and MAY structure, the limitation to information reasonably accessible to the registrar, and

¹ A report containing actionable evidence as defined in the ICANN Advisory on Compliance With DNS Abuse Obligations and referenced in the Initial Report's glossary.

the three groups of factors in Implementation Guidance 4.1 are the right frame for the material in Section 3 of this report. The treatment of resellers in Implementation Guidance 3.1 reflects where the data sits. The party holding a given signal is whichever entity operates the relevant system or holds the end-customer relationship.

Preliminary Recommendation 5 and Implementation Guidance 5.1. The preliminary recommendation requires compliance with applicable law and confirms that the policy does not prohibit a registrar from using data, tools, or services it may lawfully use. This is the right approach. Registrars that already investigate abuse effectively should not read the policy as narrowing what they do. The over-association cautions in Implementation Guidance 5.1 correspond to the reliability treatment in Section 3.

Preliminary Recommendation 6 and Implementation Guidance 6.1. A contextual standard of promptness aligned with the existing RAA obligation and the ICANN Advisory is preferable to a fixed period for ADCs. Campaigns vary in velocity. A single deadline would be too long for some cases and too short for others. Fixed periods also tend to become a floor in practice.

Preliminary Recommendation 7. A review after two years is the right interval, and deriving data points from information already held by ICANN org and registrars is a sound starting point. However, it is not sufficient on its own. The three listed purposes raise two distinct questions: (1) whether the policy has been implemented and complied with, and (2) whether it has changed abuse. (1) can be measured directly. (2) cannot be measured against a counterfactual, and answering it requires input beyond ICANN org and registrars. Section 4 explains why the two require different treatment and offers input to the IRT on indicators and baselines.

Preliminary Recommendation 8. The requirement for an internal process description available to ICANN on request, and the decision not to prescribe a documentation format, are both correct. The listed data points are the right ones. Section 5 offers one clarification on how those records should be organized.

3 Candidate Association Signals for Identifying Domains Related to a Trigger Domain

The Initial Report proposes policy language governing registrar obligations once an ADC has been triggered by actionable evidence of DNS Abuse. The SSAC's input below is intended as additional implementation guidance to support that work. It identifies candidate signals a registrar could consider when determining whether other domains under its management are associated with the trigger domain.

Table 1 assesses each signal from the registrar's perspective, reflecting the data a registrar holds or can reasonably access in the ordinary course of business. Few of these signals are sufficient on their own. They are most effective in combination, with each additional matching signal narrowing the

set of candidate domains and reducing false positives. Associations identified through these signals are scoping outcomes only. An association does not itself constitute a finding of abuse. Any subsequent action against an identified domain is governed by existing policy on DNS Abuse mitigation, which is outside the scope of this guidance.

Table 1 does not assess privacy concerns per signal. Whether a given data element is private, or whether its use is restricted, is a legal determination that depends on the applicable jurisdiction and regulatory regime, and that analysis is outside the SSAC's remit.

As a general observation, most of the signals in the table rely on data the registrar already holds or observes in the ordinary course of business. Data protection regimes commonly permit processing of such data for fraud prevention and security purposes; under the General Data Protection Regulation, for example, fraud prevention is recognized as a legitimate interest. This is an observation about the general shape of the landscape, not a legal conclusion, and it does not relieve any registrar of the obligation to assess its own footing.

Some signals nonetheless warrant particular care. Signals that involve collecting or correlating user-level data across accounts, such as browser fingerprints or session cookies, may carry additional obligations depending on applicable laws, including disclosure of the practice in the registrar's terms of service. Registrars should be aware that the use of individual elements in this table may be affected by the privacy laws applicable to them, and should evaluate that question within their own legal context.

3.1 Availability of Signal Data

The signals in Table 1 are described in terms of the party that holds the data. Which party that is depends on which entity operates the relevant system or holds the end-customer relationship. Some signals may be held by or visible to a reseller but not to the registrar. Where all registrations from a reseller sit in a single account between the registrar and the reseller, the reseller holds the individual customer accounts and the registrar does not. Payment data is another example. A reseller may own or manage the system it uses to take payment from registrants. In that case the registrar does not hold payment information. Alternatively, the registrar may provide the payment processing system the reseller uses, and then it does. A web agency with many clients' domains under management is a further case. There, registrant, payment, IP address, and other signals are not available to the registrar or to the reseller. Other arrangements exist with the same effect.

Two consequences follow for the Initial Report. First, the reseller provisions of Implementation Guidance 3.1 reflect where the data sits. A registrar may rely on a reseller to conduct investigation steps while remaining responsible under RAA 3.12. Second, implementation guidance should distinguish a baseline from better practice. The baseline is what every registrar can do with data it reliably holds, such as the account relationship, registration timing, and nameservers. Better practice is what a registrar with richer data can do. Table 1 is organized to support that distinction.

Domain re-registration, sometimes called drop-catching, was not treated as a separate trigger signal. Re-registered names were considered alongside newly registered names in developing the table. The detection signals are common to both.

The rationale on Preliminary Recommendations 2 through 4 states that the policy requires an ADC only within a registrar's portfolio and does not require cross-registrar checks or coordination. The SSAC does not propose coordination between unaffiliated registrars. That would raise data-sharing questions beyond the scope of this PDP. However, a single entity commonly holds several registrar accreditations that share a back end, a customer database, and an abuse desk. Where that is the case, a check confined to the portfolio of one accreditation would be an artificially narrow reading of information reasonably accessible to the registrar in the normal course of its operations. It would leave untouched associated domains that the same operator can already see. The SSAC suggests the Working Group clarify this point. Where Affiliated Registrars (RAA 1.4) within an Applicable Registrar Family (RAA 1.5) operate on shared systems and the data is accessible, the ADC should extend across those portfolios.

3.2 Understanding the Signal Ratings

The ratings in Table 1 describe the general case across the registrar ecosystem, not every environment. Availability, difficulty, and reliability vary with a registrar's business model, sales channels, and technical setup. Edge cases exist for nearly every cell. A signal rated low availability may be readily accessible to a particular registrar. A signal rated high availability may be out of reach in some reseller or white-label models. The ratings are intended to support discussion of which signals are worth considering and how they combine. They do not adjudicate any individual registrar's circumstances.

3.3 Signal Attributes

Each signal in Table 1 is assessed against five attributes: availability, difficulty, whether it can be automated, independence, and reliability. The definitions below describe what each attribute measures and how its scale should be read.

Availability (low / medium / high): How readily the registrar already holds or can access the data underlying the signal, without new collection. Low means the data is often unavailable to the registrar, for example device data in some reseller models. Medium means it is held by some registrars or in some channels but not consistently. High means the registrar reliably holds it as a matter of course, for example account holder identity.

Difficulty (low / medium / high): The operational effort required to evaluate the signal once the data is in hand. Low means a lookup or comparison. Medium means some processing, correlation, or judgment is required. High means the signal is labor-intensive or technically involved to apply reliably.

Automatable (yes / no): Whether a registrar could realistically detect the signal through an automated process rather than manual review. Yes means it can be scripted or run programmatically across the registrar's domains. No means it currently requires human assessment.

Independence (low / medium / high): How well the signal identifies associated domains when used on its own. Low independence, for example the same registration IP address, which can be shared across many unrelated registrants behind a reseller, VPN, or proxy, captures few of the associated domains by itself and is meaningful mainly in combination with other signals. High independence means the signal, applied alone, captures most of the domains actually associated with the trigger domain.

Reliability (low / medium / high): How likely a match on the signal reflects association rather than coincidence. Low reliability means a match frequently links unrelated domains and may yield many false positives. High reliability means a match rarely links unrelated domains.

Independence and reliability are complementary. Independence describes how many of the associated domains a signal captures. Reliability describes how much unrelated material it introduces alongside them. In information retrieval terms, they correspond to recall and precision. A signal can be high on one and low on the other. An effective candidate set maximizes the associated domains captured and minimizes the unrelated domains included. Achieving both typically requires combining signals.

3.4 Signal Categories

Operational elements are drawn from the registrar's account, session, and payment systems. The same account holder is the strongest single signal because an account set up for fraudulent purposes typically contains only registrations from the same activity. The two limiting cases are a compromised account, where an attacker's registrations sit alongside a legitimate registrant's, and an aggregator account held by a reseller, web agency, or similar party for many unrelated end customers. Payment signals are strong where the registrar holds the underlying instrument details and weaker where it receives only an approval result from a processor. Session and fingerprint signals are strong where held but are the signals most likely to carry additional data protection obligations.

Domain implementation characteristics are observed from the registration record and from the DNS. Three rows that can look alike are kept separate because they draw on different data. Same nameservers (row 15) is a value the registrar records at registration. Common destination (row 13) is where the domain resolves or redirects, which may differ from the DNS delegation where forwarding is used. Shared DNS record artifacts (row 17) are values in records other than the delegation, such as an SPF policy, MX host, or SOA MNAME, which are observed by lookup. Nameservers and DNS artifacts are rated low on reliability because large providers assign the same values to many unrelated customers and SOA values are often left at a default. A shared certificate (row 16) rates high on independence because a certificate valid for several domains links them

directly, but medium on reliability because content delivery networks and hosting providers can request a single certificate covering unrelated domains.

Temporal elements are readily available to every registrar and are easy to evaluate, but few are reliable on their own because legitimate registrants register domains at the same times as abusers. A bounded timespan around the trigger domain's creation date is a useful filter in combination with other signals. The group originally included registrations made shortly after a zone file snapshot; that row was removed because the SSAC had no evidence of the technique in use. The reference to events in row 21 was added because registrations around a news event, natural disaster, or holiday include both legitimate and malicious names, which is the situation in which care against over-association is most needed.

Name-based characteristics are the signals registrars most often use already, because reports of a campaign tend to arrive with a visible naming pattern. Two techniques are named because they are common and relatively distinctive. Top-level domain (TLD) stuffing (row 23) places a TLD string and a hyphen at the start or end of a second-level label so that a subdomain reads as though it belongs to another domain; few legitimate registrations begin with a string such as "com-". TLD hopping (row 24) registers the same label across many TLDs; brand owners do this too, so it is rated medium. Several signals in this group, such as homoglyph substitution and deceptive terms, are stronger for detecting a suspicious registration than for linking a domain to a trigger domain. That distinction is discussed in Section 3.6.

Submitted or industry information covers what the registrar learns from others. A well-evidenced report that describes the campaign, including the naming pattern, infrastructure, or generation algorithm, is one of the most useful inputs to an ADC and is the mechanism by which an ADC removes the need for a reporter to file a separate report for each domain. It is rated as not automatable because it requires a person to read the report and translate it into a search. It also requires care because a described pattern, such as a domain generation algorithm, can also match legitimate domains.

3.5 Candidate Association Signals by Category

Table 1 groups the candidate signals into the five categories described in Section 3.4: operational elements, domain implementation characteristics, temporal elements at registration time, name-based characteristics, and submitted or industry information. Definitions of each signal are in the glossary (see Appendix A).

TABLE 1: Candidate association signals for identifying domains related to a trigger domain

#	Candidate signal	Availability	Difficulty	Automatable	Independence	Reliability
Operational elements						
1	Same account holder	high	low	yes	high	high
2	Same registrant IP address at registration time	medium	low	yes	low	low
3	Non-traditional payment method (e.g., gift card, cryptocurrency)	medium	low	yes	medium	medium
4	Same payment detail information (e.g., credential, account number)	medium	low	yes	high	high
5	Cookies (session) on customer's browser	medium	medium	no	medium	high
6	Browser fingerprint of customer	medium	medium	no	high	high
7	Same affiliate channel	high	low	yes	medium	low
8	Bulk/API key	high	medium	yes	medium	medium
9	Address field mismatch across account data elements	high	low	yes	medium	low
10	Geographical parity across access sessions	low	high	no	low	medium
Domain implementation characteristics						
11	Same unique identifier in contact/account data	high	medium	yes	high	high
12	Similar patterns across registration elements	low	high	no	low	low
13	Common destination	medium	medium	yes	low	medium
14	Discordance between destination geoIP and account data	medium	medium	yes	low	low
15	Same nameservers	high	low	yes	medium	low
16	Same certificate (Common Name / Subject Alternative Name)	high	low	yes	high	medium
17	Shared DNS record artifacts (TXT/SPF, MX, SOA/MNAME)	high	low	yes	medium	low
Temporal elements at registration time						
18	Registered within the same bounded timespan	high	low	yes	low	medium
19	Registered with a regular temporal pattern	high	high	yes	low	low
20	Aberrant temporal registration patterns	high	medium	yes	medium	low
21	Burst or batch registrations prior to weekends, holidays, or events	high	medium	yes	medium	medium
Name-based characteristics						
22	Repeated patterns in domain string	high	low	yes	medium	medium

#	Candidate signal	Availability	Difficulty	Automatable	Independence	Reliability
23	TLD stuffing (starting or ending a domain name with "TLD-")	high	low	yes	medium	high
24	TLD hopping (same string across multiple TLDs)	medium	low	yes	medium	medium
25	Spoofing a well-known brand name	high	medium	yes	medium	medium
26	Use of deceptive terms (e.g., login, secure)	high	low	yes	medium	medium
27	Small string distance between domain names (Levenshtein or similar)	high	low	yes	medium	medium
28	Character homoglyph swapping (e.g., zero "0" for letter "O")	high	high	yes	medium	medium
Submitted or industry information						
29	Evidenced third-party reports with campaign information	medium	medium	no	high	medium

3.6 Applying the Candidate Signals

The most practical approach is to add signals one at a time. The goal is a candidate set that captures as many associated domains as possible and includes as few unrelated domains as possible. A typical sequence starts with a broad and inexpensive signal, such as string similarity to the trigger domain or membership of the same account. It then narrows the set with signals that carry more weight, such as nameservers, creation date, or a shared payment instrument. Each added signal removes unrelated domains. Where the set becomes too narrow, a signal can be relaxed. The sequence can be applied across all domains under management or limited to the domains of the same account holder. Where the account holder is known, starting from that space is preferable. The full portfolio of a large registrar is expensive to search and produces more unrelated matches.

A registrar's records of past campaigns are also a signal. Patterns that the registrar has itself identified, or that recur across reports it has received, are as useful as those listed in Table 1.

Some name-based signals are stronger for identifying a suspicious registration than for linking a domain to a trigger domain. Homoglyph substitution, deceptive terms, and brand spoofing describe what a malicious name looks like. They narrow a search space. They do not by themselves establish that two domains belong to the same campaign or actor. Signals such as the same account, the same payment instrument, the same certificate, or registration within the same window do establish that link. An investigator can use the first kind to define the space to search and the second kind to establish association within it.

Table 1 reflects techniques observed in use at the time of writing. Abuse techniques change. The more effective registrars become at detecting association through a particular signal, the more actors will work to avoid it. Implementation guidance should therefore be written so that the set of indicators can be refreshed without reopening the policy. ICANN org may wish to consider whether

an existing function could periodically publish observed campaign characteristics for registrars to draw on. This would be consistent with the third factor in Implementation Guidance 4.1.

3.7 Illustrative User Stories

Each story follows the same form: the trigger domain and the source of the evidence; the first pivot; the signals used to narrow the set; the resulting candidate set; and what a reviewer then assesses for each domain before any action. Each ends with the rows of Table 1 used and those that were unavailable.

3.7.1 A phishing report with a naming pattern

A registrar receives a well-evidenced report that a domain is hosting a phishing page impersonating a toll road operator. The reporter notes that it has seen several similar domains, all containing the operator's name and a word such as "pay" or "bill". The registrar begins with the account that holds the reported domain (row 1) and finds four more domains registered in the same session (row 18). It then searches its portfolio for the naming pattern (rows 22, 25, 26) and finds a further twelve domains across three other accounts. Two of the three accounts share a payment instrument with the first (row 4); the third was created from the same registration IP address within the same hour (rows 2, 18). The candidate set is seventeen domains in four accounts. A reviewer confirms that each resolves to the same hosting provider (row 13) before any action. Unavailable in this case: browser fingerprint (row 6), which the registrar does not collect.

3.7.2 Malware command-and-control report

A security researcher reports that a domain is a command-and-control server for a malware family and provides the domain generation algorithm the malware uses, including the seed and the TLDs it targets. The registrar generates the algorithm's output for the next thirty days (row 29) and matches it against its portfolio, finding nine registered names. Because the algorithm can produce strings that coincide with legitimate names, the registrar checks each match against creation date (row 18) and nameservers (row 15). Seven of the nine were registered within two days of each other and delegated to the same nameservers; two were registered years earlier by unrelated registrants and are removed from the set. The candidate set is seven domains. Unavailable in this case: the account is a reseller account (row 1 aggregated), so the registrar relies on the reseller to identify the end customer under Implementation Guidance 3.1.

3.7.3 A naming pattern that string distance does not catch

A registrar receives a report that a domain impersonating a bank's login page is hosting credential phishing. The registrar first searches its portfolio for names within a small string distance of the trigger domain (row 27) and finds nothing, because the campaign's names vary in length and in the terms appended after the brand string. Searching instead on the leading label as a fixed prefix (row 22) returns eleven domains that begin with the same brand string and hyphen, six of which combine it with a deceptive term such as login, verify, or alert (row 26). The registrar narrows the set by

creation date and finds that nine of the eleven were registered within a four-day window (row 18), and that eight of those nine are delegated to the same nameservers (row 15). The candidate set is eight domains across three accounts. A reviewer confirms the phishing content on each before any action. Unavailable in this case: payment detail information (row 4), because the registrar receives only an approval result from its processor.

3.7.4 A reseller account where the registrar pivots on what it holds

A registrar receives a well-evidenced report that a domain sponsored through one of its resellers is distributing malware. The domain sits in a single aggregated account held by the reseller, so the account holder signal (row 1) identifies the reseller rather than the end customer. The registrar pivots on the data it does hold. It finds fourteen domains in the reseller's account delegated to the same nameservers (row 15), of which six were registered within the same two-day window as the trigger domain (row 18) and share a repeated string pattern of a word followed by four digits (row 22). The candidate set is six domains. Under Implementation Guidance 3.1 the registrar asks the reseller to confirm whether the six sit in one end-customer account, and the reseller confirms that they do. A reviewer assesses each domain against the reported malware evidence before any action. Unavailable in this case: registrant contact data, payment detail information, and registration IP address (rows 11, 4, 2), all of which the reseller holds rather than the registrar.

3.7.5 A broad first cut narrowed by a shared certificate

A registrar identifies through its own monitoring that a domain is being used in a payment fraud campaign. The trigger domain is the only registration in its account, so the registrar starts from the hosting arrangement instead. Two hundred and forty domains under its management resolve to the same hosting provider (row 13), which is too broad a set to act on because the provider serves many unrelated customers. The registrar retrieves the Transport Layer Security (TLS) certificate for the trigger domain and finds nineteen of the 240 named in its Subject Alternative Names (row 16). Because hosting providers issue certificates covering unrelated customer domains, the registrar checks the nineteen against creation date and finds twelve registered within the same week (row 18), all of which also share a registration IP address (row 2). The candidate set is twelve domains. A reviewer assesses each for evidence of the fraud campaign before any action. Unavailable in this case: session cookie and browser fingerprint data (rows 5, 6), which this registrar does not collect.

4 Measuring Policy Effectiveness (Preliminary Recommendation 7)

4.1 Two Distinct Questions

The SSAC supports a review of the policy's effectiveness after two years and supports the direction that the IRT identify a limited set of aggregated data points, derived where feasible from information already available to ICANN org and registrars. Preliminary Recommendation 7 lists three purposes for the policy:

1. establishing a consistent minimum baseline across registrars for conducting ADCs when the policy obligation is triggered;
2. ensuring that compliance with the ADC obligations can be assessed and enforced; and
3. contributing to the timely identification and disruption of DNS Abuse campaigns.

These purposes raise two distinct questions, and each is assessed differently:

- **Implementation and compliance:** whether registrars are conducting ADCs and meeting the obligation. This covers the first two purposes.
- **Effect on abuse:** whether the practice of conducting ADCs has changed the incidence or character of DNS Abuse. This covers the third purpose.

The review should assess the two questions separately. The first question can be measured directly. The second cannot. Implementation and compliance can be measured from ICANN Contractual Compliance's own activity and from the records registrars keep under Preliminary Recommendation 8. Examples are the share of registrars with a documented ADC process, the number of ADCs reported or audited, the number of associated domains identified per triggering domain, and the proportion of identified domains on which action was taken.

The effect of the policy on abuse cannot be measured against a counterfactual. A policy that makes associated registrations easier to find will change how abusers register. Batches may become smaller, more dispersed across accounts and registrars, and better disguised. A short-term rise in observed malicious registrations does not by itself show the policy is failing. A fall does not by itself show it is working. The more useful question is whether the policy has made the DNS harder to abuse, and to do so at scale. The rationale on Preliminary Recommendation 7 acknowledges this. Answering the second question therefore requires input from beyond ICANN org and registrars, which Section 4.2 addresses.

Registrar behavior will also change. A registrar that conducts ADCs learns which patterns indicate a malicious batch, and applying that learning at registration is the natural next step. Domains screened out that way never produce a trigger and never produce an ADC. The registrar is preventing the abuse the policy was written to address, and its ADC count falls as a result. A registrar with a low ADC count may therefore be doing more, not less.

The SSAC suggests the following text for future implementation guidance developed under Preliminary Recommendation 7:

The review should assess separately (a) whether the policy has been implemented and is being complied with, using indicators derived from ICANN Contractual Compliance activity and records maintained under Preliminary Recommendation 8, and (b) whether the practice of conducting ADCs is contributing to the identification and disruption of DNS Abuse campaigns, recognizing that changes in aggregate abuse levels cannot be attributed to this policy alone and may reflect changes in abuser behavior in response to it.

Recommendation 1: Implementation guidance developed for Preliminary Recommendation 7 should specify that the review separately assess:

- i. whether the policy has been implemented and is being complied with; and
- ii. whether the practice of conducting ADCs is contributing to the identification and disruption of DNS Abuse campaigns, recognizing that changes in aggregate abuse levels cannot be attributed to this policy alone.

4.2 Input to the IRT on Indicators and Baselines

The rationale on Preliminary Recommendation 7 states that the Working Group expects the IRT to identify the relevant data points and to establish baseline data for future measurement, and that the review should not rely solely on aggregate abuse-volume statistics. The SSAC agrees on both points. The following is offered as input to that work, and the SSAC is willing to develop any of these further.

- Baseline data should be captured before the policy takes effect. Existing ICANN abuse reporting, such as Domain Metrica, can supply registrar-level rates of malicious registrations. Reporting should include the absolute number of maliciously registered domains, not rates alone. Any comparison across registrars should normalize that number by domains under management.
- One outcome indicator is the balance over time between abuse carried out through maliciously registered domains and abuse carried out through compromised domains or other techniques that do not involve registration. A shift away from malicious registration is consistent with the policy achieving its purpose, even if total abuse does not fall.
- A screening test is available to Compliance without technical tooling. Compare the number of maliciously registered domains a registrar actioned in a period with the number of ADCs it reports for the same period. A registrar reporting few or no ADCs against a notable number of actioned malicious registrations is a candidate for closer examination. Upstream prevention is one explanation for that pattern and should be ruled out before any conclusion is drawn.
- Where a complaint alleges that an ADC was not performed, Compliance can request the reporter's evidence and the registrar's ADC record for the same case and compare them. The registrar works with richer data than an external reporter. Where the reporter's submission is accurate, the set the registrar identifies should therefore usually be a superset of what the reporter found. A shortfall may instead mean the reporter over-identified, so that explanation should be ruled out before concluding the check was not performed or not performed adequately.
- False positives should be tracked. Here that means benign domains actioned following an ADC. They are the principal cost of the policy to registrants and the principal concern raised during the PDP.
- Some data are useful because they are reported to ICANN and available to Compliance in its own work. Other data are suitable for publication in aggregate. The IRT should identify

which indicators belong in each group rather than assume that every data point collected is a data point published.

- ICANN org should publish aggregated ADC data to the extent it lawfully can, so that associated-domain reporting and registrar response can be studied independently and systematically. A registrar's records are scoped to its own ADCs, and a Compliance case file is scoped to a single complaint. Independent study is the only vehicle for examining ADC practice at industry scale. Aggregated data could better enable assessment of the policy's effect on abuse.
- The two-year review should account for false negatives, not only false positives. Here that means associated domains that an ADC did not identify, or identified without any action taken. No registrar can see what it failed to find, and a reporter who submits evidence learns nothing about what followed. Independent study of the aggregated data is therefore the only route to detecting misses at scale. Without it the review sees the cost of over-association but not the cost of under-association.
- The indicators developed for this review should be reusable as subsequent DNS Abuse policies are implemented. The ICANN Board has expressed interest in how the effectiveness of DNS Abuse policy interventions can be assessed over time.

Measurement of any kind is constrained by the absence of a standard format and evidentiary baseline for abuse reports submitted to registrars. Reporters, registrars, and Compliance each work with different definitions of sufficient evidence. The outcome of a report is difficult to track from submission to resolution. The SSAC described these conditions in SAC115, which found that inconsistent reporting standards extend victimization and leave reporters without a feedback loop on the reports they submit.²

Recommendation 2: The baseline data described in the rationale on Preliminary Recommendation 7 should be captured before the policy takes effect. It should include the absolute number of maliciously registered domains. Any comparison across registrars, at baseline or at review, should also be normalized by domains under management.

Recommendation 3: Implementation guidance developed for Preliminary Recommendation 7 should specify that ICANN org publish aggregated ADC data in a documented, machine-readable schema that supports independent study of ADC reporting and registrar response, to the extent it lawfully can.

Recommendation 4: Implementation guidance developed for Preliminary Recommendation 7 should specify that the scope of the two-year review include methodologically sound independent research on ADC reporting and registrar response in its assessment of the policy's effect on abuse.

² See SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS, <https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-115-en.pdf>

5 Demonstrating Compliance (Preliminary Recommendation 8)

5.1 What the Records Need to Separate

The SSAC supports Preliminary Recommendation 8, including the requirement for an internal process description available to ICANN on request and the decision not to prescribe a documentation format. The data points listed in the recommendation are the correct ones.

The SSAC offers one clarification for the IRT. The records a registrar maintains should allow a reviewer to distinguish three things:

1. the evidence and reasoning for classifying the trigger domain as maliciously registered;
2. the basis on which each associated domain was connected to the trigger domain (e.g., signals); and
3. the evidence and reasoning for any action taken on each associated domain.

Item 2 is a record of the association, not a reconstruction of the investigation. A registrar identifies associated domains by working through a series of pivots, and the sequence is not fixed in advance. A signal may return a broad candidate set, and a registrar may run several signals before narrowing that set to the domains it treats as associated. Recording every step of every investigation is not what this requires, and Preliminary Recommendation 5 does not require a registrar to generate data it does not otherwise hold. What the record should show is how each domain in the final set was connected to the trigger domain.

In the SSAC's view the best approach is to record the specific signals that made each connection. The SSAC recognizes that registrars operate different systems, and that a registrar may be able to demonstrate the basis and reasoning for an association by other means. A general assertion that a check was performed is not sufficient. Read together with the internal process description that Preliminary Recommendation 8 already requires, this allows a reviewer to see that a check was performed and on what basis, without requiring the registrar to document the path it took to get there.

A registrar should be able to answer four questions about any domain it actioned as the result of an ADC. Take `trigger.example` as the trigger domain and `associated.example` as a domain the check identified and the registrar actioned.

1. What was the evidence that `trigger.example` was maliciously registered and what was the reasoning?
2. What signals connected `associated.example` to `trigger.example`?
3. What was the evidence that `associated.example` was itself maliciously registered and what was the reasoning?
4. When did each of these steps occur?

The first and third are already required under RAA 3.18.2. The second is what this policy adds. The fourth is required by Preliminary Recommendation 8, which records the time of the trigger and the times the ADC was initiated and completed. These timestamps will provide the only systematic view of registrar response times under the policy. In aggregate they are an input to the review in Section 4.

Recommendation 5: Implementation guidance developed for Preliminary Recommendation 8 should specify that records preserve the distinction between:

- i. the evidence for the trigger domain;
- ii. the basis on which each associated domain was connected to it; and
- iii. the evidence for action on each associated domain.

5.2 How Compliance Can Use the Records

Compliance can verify that ADCs are being performed by three routes: complaints, proactive monitoring, and scheduled audits. In each case it needs the same information from the registrar. First, the trigger: the report or internal finding, its source, the evidence, and the timestamp. Second, the timestamp and the resulting set of domains. Third, the outcome: how many domains in the set were found to be maliciously registered, how many were actioned, and how many were subsequently reversed.

For a complaint alleging that an ADC was not performed, the comparison described in Section 4.2 applies. Where the reporter's submission is accurate, the registrar's set should be a superset of the reporter's. For proactive monitoring, the screening ratio of actioned malicious registrations to reported ADCs identifies registrars for closer examination. Neither route requires Compliance to reproduce the registrar's technical analysis.

6 Matters Outside the Scope of the PDP

The Working Group has identified several issues during its work that fall outside its charter. The SSAC supports listing these in the Final Report so that the GNSO Council can consider them in sequencing future work. The SSAC asks that the following be included.

Registrant recourse. The Working Group has treated remedies for registrants adversely affected by mitigation as outside the scope of this PDP. The SSAC agrees. A domain can be wrongly suspended with or without an ADC, and the gap is in the RAA rather than in this policy. There is nonetheless a security and stability reason to record it. An ADC allows a registrar to turn one report into action on many domains. That is the purpose of the policy. It also multiplies the consequence of an error in the association step. There is no ICANN policy mechanism through which a registrant whose domain was wrongly actioned can seek review.

Sharing findings across registrars. An ADC may surface indicators that point to associated domains at other, unaffiliated registrars. The PDP did not address whether or how such findings can lawfully be shared. The SSAC notes the question without proposing an answer.

7 Recommendations

Recommendation 1: Implementation guidance developed for Preliminary Recommendation 7 should specify that the review separately assess:

- i. whether the policy has been implemented and is being complied with; and
- ii. whether the practice of conducting ADCs is contributing to the identification and disruption of DNS Abuse campaigns, recognizing that changes in aggregate abuse levels cannot be attributed to this policy alone.

Recommendation 2: The baseline data described in the rationale on Preliminary Recommendation 7 should be captured before the policy takes effect. It should include the absolute number of maliciously registered domains. Any comparison across registrars, at baseline or at review, should also be normalized by domains under management.

Recommendation 3: Implementation guidance developed for Preliminary Recommendation 7 should specify that ICANN org publish aggregated ADC data in a documented, machine-readable schema that supports independent study of ADC reporting and registrar response, to the extent it lawfully can.

Recommendation 4: Implementation guidance developed for Preliminary Recommendation 7 should specify that the scope of the two-year review include methodologically sound independent research on ADC reporting and registrar response in its assessment of the policy's effect on abuse.

Recommendation 5: Implementation guidance developed for Preliminary Recommendation 8 should specify that records preserve the distinction between:

- i. the evidence for the trigger domain;
- ii. the basis on which each associated domain was connected to it; and
- iii. the evidence for action on each associated domain.

8 Acknowledgments, Disclosures of Interest, and Withdrawals

In the interest of transparency, these sections provide the reader with information about aspects of the SSAC process. The Acknowledgments section lists the SSAC members, outside experts, and ICANN staff who co-authored or contributed directly to this particular document or who provided reviews. The Disclosures of Interest section points to the biographies of all SSAC members, which disclose any interests that might represent a conflict—real, apparent, or potential—with a member's participation in the preparation of this comment. The Withdrawals section identifies individuals

who have recused themselves from the discussion of the topic with which this comment is concerned. Except for members listed in the Withdrawals section, this document has the consensus approval of all of the members of SSAC.

8.1 Acknowledgments

The committee wishes to thank the following SSAC members and ICANN staff for their time, contributions, and review in producing this comment.

SSAC Members

Greg Aaron
Benedict Addis
Gautam Akiwate (SSAC representative to DNSAM PDP 1, Alternate)
Gabriel Andrews
Jeff Bedser
Nabil Benamar
Hadia Elminiawi
Jothan Frakes (SSAC representative to DNSAM PDP 1, Participant)
James Galvin (ICANN Board Liaison to DNSAM PDP 1)
Robert Guerra
Layal Jebran
Warren Kumari
Sourena Maroofi
Rod Rasmussen (SSAC representative to DNSAM PDP 1, Member)
Raffaele Sommese
Matthew Thomas (SSAC representative to DNSAM PDP 1, Member)
Rick Wilhelm

ICANN Staff

Daniel Gluck
Michael Monarrez-Puckett
Carlos Reyes
Danielle Rutherford (Editor)
Kathy Schnitt

8.2 Disclosures of Interest

SSAC member biographical information and Disclosures of Interest at the time of publication are available at: <https://www.icann.org/en/ssac/members/archive/13-07-2026>.

8.3 Withdrawals

There were no withdrawals.

Appendix A: Candidate Signal Glossary

This appendix defines each candidate signal listed in Table 1. Entries are alphabetical. Where a signal is easily confused with another, the entry notes the distinction and the row in Table 1 to which it relates.

Aberrant temporal registration patterns: Registration activity at times anomalous for the registrar's customer base, for example offsets suggesting registrations during the peak hours of a different region from the one the account data claims.

Address field mismatch across account data elements: Inconsistency across account data elements such as billing address, registrant contact, and IP geodata. Example: registrant contact in one location, card billing address in another, and registration geoIP in a third region.

Browser fingerprint of customer: The registering party's browser presents the same fingerprint across registrations. Kept separate from cookies because fingerprinting can be performed in several ways, whereas a session cookie is a single identifier.

Bulk/API key: Registrations made using the same bulk registration or API credential.

Burst or batch registrations prior to weekends, holidays, or events: Spikes or batches of registration activity immediately ahead of weekends, extended holidays, or events.

Character homoglyph swapping: A recognizable term with characters replaced by others that look similar or identical, such as a lower-case L, the number one, and an upper-case I, or the digit zero for the letter O.

Common destination: Domains pointing at the same destination infrastructure, such as the same hosting provider, IP address, ASN, path, redirect, or host.

Cookies (session) on customer's browser: The same session cookie observed on the registering party's browser across different registrations.

Discordance between destination geoIP and account data: The registration data claims one region but the domain resolves somewhere inconsistent with it, for example a domain registered as a bank in one country resolving to an unrelated jurisdiction.

Evidenced third-party reports with campaign information: A report from an abuse reporter, law enforcement, or other third party that describes characteristics of the campaign beyond the reported domain.

Geographical parity across access sessions: Consistency, or lack of it, between account and registration data and the geoIP of access sessions. Distinct from row 9, which looks at how the registration is set up, and from row 13, which looks at the destination.

Non-traditional payment method: The registration was paid for using a payment type outside the ordinary card and invoicing methods, such as cryptocurrency, prepaid or gift cards, or similar instruments. This captures the payment type only. Availability is uneven because a payment processor does not always surface enough detail to distinguish a gift card from a standard card. Legitimate registrants use these methods as a matter of preference, so the signal is a place to look rather than an indicator on its own. A reusable identifier tied to a specific instrument, such as a card bank identification number (BIN) or a cryptocurrency wallet address, falls under same payment detail information.

Registered within the same bounded timespan: Registered within a defined window around the creation date of the trigger domain.

Registered with a regular temporal pattern: Registrations recurring on a schedule, for example at the same time each week.

Repeated patterns in domain string: Similar patterns across registrations, such as a fixed string followed by random numbers or strings, the same strings in a different order, or the use of separators with the same or similar strings.

Same account holder: Evidence that the same entity holds the account or accounts across the registrations. Where an account has been set up for fraudulent purposes, the registrations in it are typically all part of the same activity, which is why the signal rates high on independence and reliability. The exception is a compromised account, where an attacker's registrations sit alongside unrelated legitimate ones and both ratings should be discounted. Aggregator accounts are the other limiting case: resellers, web agencies, and in some instances law firms hold large numbers of domains for unrelated end customers under one account, which lowers reliability. The signal is retained as a separate entry because other signals can surface associated domains held under different account holders, so the same account cannot be assumed as the search space for every other signal.

Same affiliate channel: Registrations arriving through the same marketing or acquisition path, such as a shared promotion code, campaign identifier, affiliate link, or dedicated registration URL. Registrars generally hold this data for marketing attribution. It narrows the set of domains for review but does not separate bad actors from legitimate registrants responding to the same offer. Individually issued codes are stronger than broadly shared ones. Distinct from row 8, which reflects the registration credential rather than the arrival path.

Same certificate (Object Name / Subject Alternative Name): Domains sharing a TLS certificate, whether through the same common name or by appearing together in the certificate's Subject Alternative Names. Any domain the certificate is valid for counts. Shared certificates can produce false positives, because content delivery networks and hosting providers can request a single certificate covering unrelated domains.

Same nameservers: Domains delegated to the same nameservers. Most useful where the provider issues distinct nameserver pairs per customer; less useful where a large provider assigns the same pair to many unrelated customers.

Same payment detail information: The same underlying payment details behind the transaction, such as card number, account number, wallet, or billing information. Payment type can be derived from these details. A match is a strong signal because it ties registrations to a single paying party, subject to the case of stolen or otherwise compromised payment credentials. Availability is uneven because the registrar may receive only an approval result from its processor. Details include the BIN, the leading digits of a card number identifying the issuing institution and card product. A BIN match is weaker than a full instrument match, since it groups every card from the same issuer and product, but is informative where a batch of registrations resolves to an unusual or prepaid issuer.

Same registrant IP address at registration time: The IP address used by the registering party at the time of registration. Not the IP address of the resulting website, which is covered under common destination.

Same unique identifier in contact/account data: The same unique identifier appears across contact or account data, such as an email address, phone number, or full address. A bare registrant name is not a unique identifier.

Shared DNS record artifacts (TXT/SPF, MX, SOA/MNAME): Domains sharing distinctive values in DNS records other than the delegation itself, such as the same verification token or SPF policy in a TXT record, the same MX hosts, or the same SOA MNAME. Distinct from same nameservers, which the registrar records at registration; these values are observed by lookup. Lookups are limited in practice to the apex and common labels such as www, since the registrar cannot enumerate the zone. Reliability is limited by defaults and shared infrastructure. A match is a trigger for review rather than a determination on its own.

Similar patterns across registration elements: Patterned variation across registration elements rather than exact matches, for example g123@ and g234@ at the same mail provider, or 123 Main Street and 234 Main Street. Distinguished from row 11, which requires the same identifier.

Spoofing a well-known brand name: A domain string containing or resembling a brand name to which the registrant has no evident connection.

TLD hopping: The trigger domain's label registered under other TLDs. Example: for trigger.example, look for the label "trigger" registered under other TLDs.

TLD stuffing: Beginning or ending a second-level label with an existing TLD string followed or preceded by a hyphen, so that a subdomain reads as though it belongs to another domain. Example: a link to icann.org-board.example, where a user may not notice the hyphen in place of a slash.

Use of deceptive terms: A familiar term, such as a popular website, brand, event, or other string, combined with a term such as login, secure, tickets, or donations. Examples: popularsite-login.example, concertevent-tickets.example, disaster-donations.example.