



87

ANNUAL  
GENERAL  
MEETING



## SAC135: SSAC Comments on the Initial Report of the GNSO DNS Abuse Mitigation Policy Development Process 1

Rod Rasmussen

SSAC Member Biographies and Disclosures of Interest as of 13 July 2026

20 October 2026

# Three takeaways from SAC135



## *The SSAC supports the baseline*

The preliminary recommendations are workable and proportionate



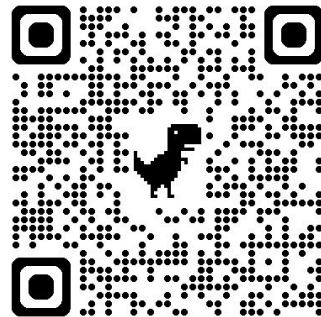
## *Association comes from combined signals*

And an association is not a finding of abuse



## *Measure compliance and effect separately*

Capture the baseline before the policy takes effect



## Where the SSAC Stands

The SSAC supports the preliminary recommendations as a ***workable and proportionate*** baseline

### PR1 ADC Trigger



Tied to the existing actionable-evidence standard

### PR2 to 4 Investigation and Association



The right frame; reflects where the data sits

### PR5 Safeguards



Doesn't narrow what registrars already do well

### PR6 Timeline



A contextual standard beats a fixed deadline

### PR7 Measuring Effectiveness



Supported, with input

See Part 3

### PR8 Demonstrating Compliance



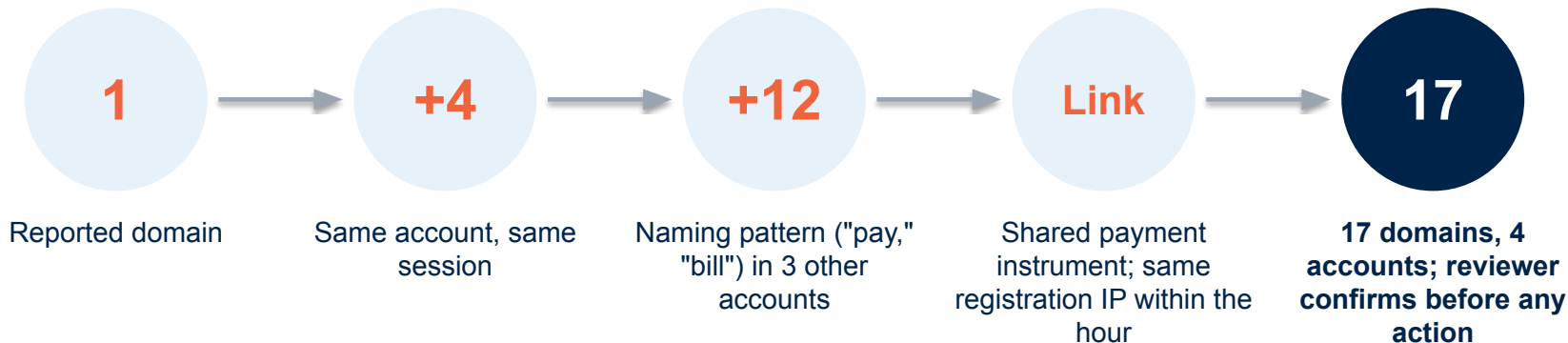
Supported, with one clarification

See Part 3

PR titles from the Initial Report (18 August 2026). SSAC rationale: SAC135 §2, pp.4 to 5.

## How Association Works in Practice

### One phishing report on a toll-road operator led to 17 domains across 4 accounts



Running total: **1 → 5 → 17 domains**

Unavailable in this case: browser fingerprint (the registrar does not collect it).

## “Is it being done?” and “Is it working?” need different measures

**PR7 purposes:** (1) consistent minimum baseline for ADCs (2) compliance can be assessed and enforced (3) timely identification and disruption of DNS Abuse campaigns



### Is it being done?

Implementation and compliance (purposes 1 and 2)

#### Measured directly

- Share of registrars with a documented ADC process
- Number of ADCs reported or audited
- Associated domains identified per trigger
- Proportion of identified domains actioned



### Is it working?

Effect on abuse (purpose 3)

#### No counterfactual

- Cannot be measured against what would have happened without the policy
- Answering it requires input beyond ICANN org and registrars

→ SAC135 Recommendation 1

## Records should show three things a reviewer can check, without replaying the investigation



**Timestamps (PR8):** time of trigger, ADC initiated, ADC completed

### Compliance can verify through three routes



Complaints



Proactive monitoring



Scheduled audits

***“A general assertion that a check was performed is not sufficient.”***

→ **SAC125 Recommendation 5**

# Three takeaways from SAC135



## *The SSAC supports the baseline*

The preliminary recommendations are workable and proportionate



## *Association comes from combined signals*

And an association is not a finding of abuse



## *Measure compliance and effect separately*

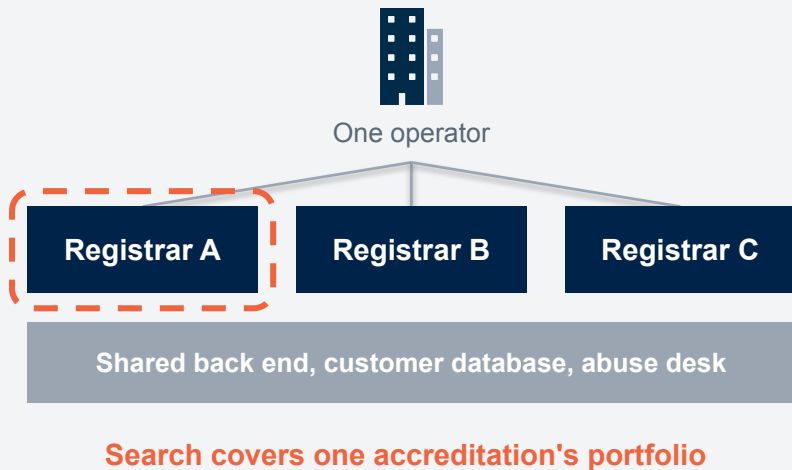
Capture the baseline before the policy takes effect



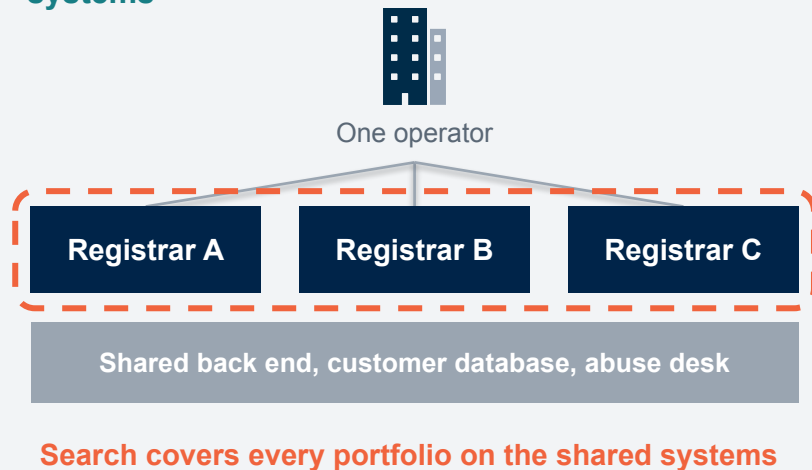
# Backup Slides

# Where affiliated registrars share systems, the check should span them

## One accreditation only



## SSAC: across Affiliated Registrars on shared systems



**Not proposed:** coordination between unaffiliated registrars.

## How Association Works in Practice

No single signal finds the campaign; each added signal narrows the set



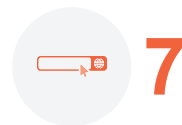
Operational  
elements



Domain  
implementation  
characteristics



Temporal  
elements at  
registration time



Name-based  
characteristics



Submitted or  
industry  
information

Broad, inexpensive signal

Narrow with stronger  
signals

Candidate set

***“An association does not itself constitute a finding of abuse.”***

SAC135 §3, p.6

SAC135 Table 1

## What a registrar can check depends on who holds the data



*A registrar may rely on a reseller to conduct investigation steps; it remains responsible under RAA 3.12.*

### Baseline: every registrar

- Account relationship
- Registration timing
- Nameservers

*Data a registrar reliably holds*

### Better practice: registrars with richer data

- Payment detail information
- Session cookies and browser fingerprint
- Registrant IP address at registration

*Rated medium availability in Table 1*

### A falling ADC count may mean a registrar is doing more, not less



#### Fewer ADCs

The registrar may be screening malicious batches at registration. Those domains never produce a trigger, so they never produce an ADC.



#### More observed malicious registrations

A short-term rise does not by itself show the policy is failing. A fall does not by itself show it is working.

**Abusers adapt:** batches may become smaller, more dispersed across accounts and registrars, and better disguised.

**Better question: has the policy made the DNS harder to abuse, and to do so at scale?**

## Capture baselines now, and count what the policy misses as well as its errors



### Baseline first

Capture baseline data before the policy takes effect



### Count, then normalize

Report absolute numbers of maliciously registered domains; normalize comparisons across registrars by domains under management



### Track errors and misses

False positives: benign domains actioned. False negatives: associated domains not identified, or identified without action.



### Publish for study

Aggregated ADC data in a machine-readable schema, to the extent ICANN org lawfully can

→ SAC135 Recommendations 2 to 4

## Two issues the SSAC asks the Final Report to list for the GNSO Council



### Registrant recourse

An ADC turns one report into action on many domains. 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 unaffiliated 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.”***

## Preliminary Recommendation 7

### Recommendation 1

#### ***Assess separately***

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

#### ***Baseline first***

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.

## Preliminary Recommendation 7

### Recommendation 3

#### ***Publish aggregated data***

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

#### ***Independent research***

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.

## Preliminary Recommendation 8

### Recommendation 5

#### ***Keep records distinct***

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.

# Table 1, candidate association signals (1 of 2)

| #                                            | Candidate signal                                                   | Availability | Difficulty | Automatable | Independence | Reliability |
|----------------------------------------------|--------------------------------------------------------------------|--------------|------------|-------------|--------------|-------------|
| <b>Operational elements</b>                  |                                                                    |              |            |             |              |             |
| 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      |
| <b>Domain implementation characteristics</b> |                                                                    |              |            |             |              |             |
| 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         |

Shading shows rating level only (darker = high, white = low); for difficulty, high means more effort.

## Table 1, candidate association signals (2 of 2)

| #                                             | Candidate signal                                                    | Availability | Difficulty | Automatable | Independence | Reliability |
|-----------------------------------------------|---------------------------------------------------------------------|--------------|------------|-------------|--------------|-------------|
| <b>Temporal elements at registration time</b> |                                                                     |              |            |             |              |             |
| 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      |
| <b>Name-based characteristics</b>             |                                                                     |              |            |             |              |             |
| 22                                            | Repeated patterns in domain string                                  | high         | low        | yes         | medium       | medium      |
| 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      |
| <b>Submitted or industry information</b>      |                                                                     |              |            |             |              |             |
| 29                                            | Evidenced third-party reports with campaign information             | medium       | medium     | no          | high         | medium      |

**Ratings describe the general case across the registrar ecosystem, not every environment.** They support discussion of which signals are worth considering and how they combine; they do not adjudicate any individual registrar's circumstances.

Shading shows rating level only (darker = high, white = low).

# How each signal is rated

## Availability

low / medium / high

How readily the registrar already holds or can access the data underlying the signal, without new collection

## Difficulty

low / medium / high

The operational effort required to evaluate the signal once the data is in hand

## Automatable

yes / no

Whether a registrar could realistically detect the signal through an automated process rather than manual review

## Independence

low / medium / high

How well the signal identifies associated domains when used on its own

## Reliability

low / medium / high

How likely a match on the signal reflects association rather than coincidence

**Independence corresponds to recall; reliability to precision.** An effective candidate set captures the most associated domains with the fewest unrelated ones. Achieving both typically requires combining signals.

# More illustrative user stories

## Malware command-and-control report

Illustrative §3.7.2

Researcher supplies the domain generation algorithm. Next 30 days of output matches 9 names. Creation date and nameservers remove 2 registered years earlier by unrelated registrants.

7 domains

**Unavailable:** Reseller account; registrar relies on the reseller to identify the end customer (IG3.1).

## A naming pattern string distance does not catch

Illustrative §3.7.3

String distance finds nothing. A fixed brand prefix finds 11; 6 add a deceptive term. 9 of the 11 fall within a four-day window; 8 of those share nameservers.

8 domains,  
3 accounts

**Unavailable:** Payment detail information; the registrar receives only an approval result.

## A reseller account

Illustrative §3.7.4

Account holder is the reseller. 14 domains on the same nameservers; 6 in the same two-day window with a repeated string pattern. Reseller confirms one end-customer account.

6 domains

**Unavailable:** Registrant contact data, payment details, registration IP (held by the reseller).

## A broad first cut narrowed by a shared certificate

Illustrative §3.7.5

240 domains resolve to the same hosting provider: too broad. 19 appear on the trigger domain's TLS certificate. 12 were registered the same week and share a registration IP.

12 domains

**Unavailable:** Session cookie and browser fingerprint (not collected).

# SSAC rationale by preliminary recommendation

| Preliminary recommendation | SSAC rationale                                                                                                                                                                                      |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PR1 and IG1.1              | Trigger tied to actionable evidence under RAA 3.18.2, from the registrar or any reporter. "Is being used" covers dormant, intermittent, or offline abuse. Excluding compromised domains is correct. |
| PR2 to 4, IG3.1, IG4.1     | MUST/MAY structure, limit to reasonably accessible information, and the three groups of factors are the right frame. Reseller treatment reflects where the data sits.                               |
| PR5 and IG5.1              | Compliance with applicable law, without prohibiting lawful data, tools, or services, is the right approach. Over-association cautions correspond to the reliability treatment in SAC135 §3.         |
| PR6 and IG6.1              | Contextual promptness aligned with the RAA and the ICANN Advisory is preferable to a fixed period. Campaigns vary in velocity; fixed periods tend to become a floor.                                |
| PR7                        | A two-year review is the right interval; starting from data ICANN org and registrars hold is sound but not sufficient. Compliance and effect on abuse need different treatment (SAC135 §4).         |
| PR8                        | Internal process description on request and no prescribed format are both correct; the listed data points are right. One clarification on how records are organized (SAC135 §5).                    |