GAC – CSG Bilateral

ICANN87 / Bali

Sunday 18 October 2026

Agenda

1. DNS Abuse: Practical mitigation steps (Mason Cole / Susan Chalmers)
2. Registration Data: Developing a workable model for accuracy and access / Supplemental SSAD (John McElwaine / Sushil Pal)
3. Review of Reviews: Structural Aspects (Osvaldo Novoa / Manal Ismail & Tracy Hackshaw)

DNS Abuse: Areas of GAC / CSG alignment

GAC		CSG
Associated domain check	**ALIGNED** (PDP under way)	Associated domain check
Bulk registration / API friction	**ALIGNED** (PDP under way)	Bulk registration / API friction
Investigating subdomains	(Not yet taken up by CSG)	
Public reporting of abuse stats	**ALIGNED**	Public reporting of abuse stats
Registration verification relationship to DNS abuse	**ALIGNED**	Proactive / timely risk-based validation (e.g., NIS2 and .US)
Transparency reporting obligations	**ALIGNED**	Transparency reporting obligations
	(Not yet taken up by GAC)	Mitigation of exact match domains

DNS Abuse: Broadening tools

- Targeted outcomes are making their way into gTLD and ccTLD policy / contracts
  - E.g., updated .US management contract contains many of the same provisions called for by community

  Examples:
  - **Measures to proactively prevent DNS Abuse**. Specifically…automated tools, monitoring systems, incentive programs, or early-warning mechanisms that would effectively detect potential threats and preemptively safeguard [the TLD].
  - Registration data database with **accurate, verified, and validated contact information** for all usTLD registrations

DNS Abuse: Broadening tools

- Tools showing utility – e.g., Associated Domain Check:

OCTO Report (18 September) on Associated Domain (AD) Analysis:

1) Over half of all reported maliciously registered domains in generic top-level domains (gTLDs) were registered (or used) in combination with other domains
2) A subset of reported abuse can be detected earlier using some AD methods, compared to reliance on standard security feeds alone.
3) Previously unknown suspected abuse can often be identified via ‘expansion analysis’ based on AD methods.

…so the community created a policy to address the problem.

Additional DNS Abuse Tools: CSG Rationale

- **Transparency in reporting mitigation actions taken** (noted in GNSO issues report)
  - No clear measurement or transparency = lack of surety in abuse handling
  - No follow-up “report to reporter” = uncertainty, unnecessary additional reports

- **Mitigation of exact match domain registrations**
  - Financial / reputational / user & customer damage due to exact match domain registrations (e.g., namelogin.com)
  - Used for phishing, fraud and disinformation

Additional DNS Abuse Tools: CSG Rationale

- **Standardization of responses from registrars and registries** (noted in GNSO issues report)
    - Inconsistent or non-substantive responses and timing = inefficient mitigation and needless follow-up

Additional DNS Abuse Tools: CSG Rationale

- **Proactive / timely and risk-based validation** (noted in GNSO issues report)
  - The INFERMAL study results suggest that proactive or timely verification can reduce DNS abuse by a significant amount.
  - Syntactical and operational validation are “hollow” / subject to throwaway data.
  - ccTLDs that more stringently validate have lower instances of abuse.
  - Registrars already fully validate data to reduce fraud for certain areas of operations (e.g., auctions), so there's merit to the procedure.
  - Risk-based verification already being recommended by governments (see NIS2 Article 28 implementation guidelines and .US contract).
  - “Register first and ask questions later" falls short of community needs.

DNS Abuse: Next steps

- Which priorities would the GAC want to see the community pursue now that PDP1 recommendations are substantially complete and PDP2 is kicking off, and why?

- Will the GAC be providing advice in this regard?

- CSG and CPH are engaged informally on further steps
  - Best practices
  - Agreement on common data sets
  - Anticipation of and mitigation of event-driven abuse

Registration Data: Developing a workable model for accuracy and access

- Authentication and equitable access to Urgent Requests:
  - How the SSAD authentication framework can accommodate legitimate requestors beyond law enforcement, including:
    - governmental and intergovernmental authorities
    - cybersecurity actors
    - IP counsel
    - brand-protection professionals
    - other trusted requestors
  - These requests should be handled without creating unnecessary barriers to the Urgent Request process. A particular issue is whether verification by trusted authorities (e.g., governmental bodies, bar authorities, or recognized professional organizations) should satisfy authentication requirements.

Registration Data: Developing a workable model for accuracy and access

- Effective access to underlying privacy/proxy registration data:
  - The GAC and CSG should seek common ground on ensuring that privacy/proxy services do not become an obstacle to legitimate investigations involving:
    - intellectual property infringement
    - fraud
    - phishing
    - counterfeiting
    - consumer protection
    - cybersecurity
    - law-enforcement matters
  - A central policy question is whether Recommendation 8.7.3 must require disclosure once the registrar has completed its review and determined that disclosure is legally permissible, while preserving applicable legal protections and the forthcoming PPSAI Consensus Policy framework.

Registration Data: Developing a workable model for accuracy and access

- Meaningful response standards, prioritization, and accountability:
  - Whether the proposed SSAD SLAs and response requirements will produce timely and useful outcomes for legitimate requestors. This could include preserving priority treatment for consumer-protection matters such as:
    - Phishing
    - Fraud
    - Malware
    - Harmful counterfeiting
  - Ensuring that Urgent and Standard Request SLAs cannot be circumvented through repeated requests for additional information
  - Requiring specific and understandable reasons for denials or recategorization
  - Providing effective reexamination, escalation, and compliance mechanisms when Contracted Parties do not meet SSAD requirements.

Review of Reviews

- An informal exchange of views on the current proposal, conscious of the GAC's recent input to the RoR draft report public comment as well as limitations that would apply to the GAC.

- CSG shares its respective views on next steps.

- CSG is supportive of the RoR effort and acknowledges the need to thoroughly reform ICANN's review framework

- Salient points: Early comprehensive Structural Review, need for Stability+Resiliency Review, Review Scoping Committee

Review of Reviews: Structural Aspects

- Need to happen first:
  - Long overdue
  - Much of the other efforts depends on the “structure”
- Duration: now 18 months: good!
- Cadence: can do better (more often than every 15 years)

THANK YOU!!