ICANN 84 ANNUAL GENERAL MEETING

# GAC Meeting with the NCSG

09:00-10:00 UTC

29 October 2025

# Agenda

1. **Welcome and Introductions** (Nicolas Caballero, GAC Chair and Rafik Dammak, NCSG Chair)

2. **HRIA and GAC Communique**
   Discuss several points about conducting HRIA and the substance of the communiqué
3. **RDRS, urgent requests/registrant data requests**
   Discuss at a high level the 24hr turnaround, how disclosure to law enforcement should be done and the need for safeguards from NCSG's perspective
4. **DNS abuse mitigation**
   Explaining points supported by NCSG and those not supported
5. **ICANN Reviews / Review of Reviews**

6. **Closing Remarks**
   (Nicolas Caballero, GAC Chair and Rafik Dammak, NCSG Chair)

# Human Rights Impact Assessment (HRIA) and GAC Communique

Farzaneh Badii, Digital Medusa

# HRIA and GAC Communique

NCSG's second Human Rights Impact Assessment (HRIA) on GAC Communiqué at ICANN83.

Finds GAC advice prioritizes enforcement over privacy, due process, and remedy.

**Private data disclosure to law enforcement:** supports disclosure of personal data to law enforcement without emphasizing enough on safeguards for the registrants.

**Urgent Requests:** Supports 24-hour disclosure, ignoring necessity and proportionality.

**Accuracy:** Supports faster verification risks. This method might be the less harmful but still human rights impact should be considered. And accuracy should never be equated with identification. End users rights are at stake as well if they cannot access website because of stringent accuracy requirements

**DNS Abuse:** Enforcement-heavy approach may cause overreach and "guilt by association." remedy and due process should be considered by GAC.

Overall: Communiqué lacks rights-based framing

# Registration Data Request Service (RDRS), Urgent Requests / Registrant Data Requests

Farzaneh Badii, Digital Medusa

# RDRS, Urgent Requests/Registrant Data Request

## RDRS and Law-Enforcement Authentication

- **Authentication ≠ Accountability:** While authentication ensures the requester is who they claim to be, it does **not** ensure that the request itself is lawful, proportionate, or rights-compatible.
- **Technical validation must not replace legal thresholds:** Merely verifying law-enforcement credentials does not meet requirements for **necessity, proportionality, or due process** under international human-rights standards.
- **Global diversity of legal regimes:** Many jurisdictions lack independent oversight or judicial authorization for data access—global rollout of RDRS without safeguards risks **normalizing unaccountable disclosure practices.**
- **Authentication of law enforcement should be through transparent processes that can be vetted with especial protocols in place**

# RDRS, Urgent Requests/Registrant Data Request

## Human-Rights Due Diligence

- Fundamental-rights assessment should precede disclosure: Registrars should conduct case-by-case Human Rights Impact Assessments (HRIAs) when requests pose risks to privacy, expression, or security of individuals.
- **Adopt “necessity and proportionality” tests:** Before disclosure, registrars should evaluate whether the request meets international norms under the UDHR and ICCPR (Articles 12, 17, 19, 2(3)).
- **Context-sensitive risk assessment:** Special scrutiny is needed when requests raise flags for end user or domain name registrant security, freedom of expression
- **Insist on Institutionalizing safeguards:** Develop internal procedures for escalation, independent review, and documentation of high-risk disclosure decisions.

# DNS Abuse Mitigation

Michaela Nakayama Shapiro, ARTICLE 19
Farzaneh Badiei, Digital Medusa

# DNS Abuse Mitigation: Guiding Principles

- **Legality, Legitimacy & Proportionality and Necessity:** Mitigation must be tethered to clear legal bases, serve a legitimate public interest, and be proportionate in scope.
- **Transparency & Accountability:** Stakeholders must be informed of processes, decisions, and justifications for action
- **Granularity in Mitigation:** Rather than wholesale domain suspensions, registrars should explore less drastic interventions—like contacting registrants or hosting providers—when appropriate).
- **Technical Evidence-Based Actions:** Mitigation should rely on specific, verifiable evidence. Avoid over-reliance on presumed patterns or indicators alone.
- **Preservation of Anonymity:** Anonymity remains essential for at-risk communities and activists. DNS Abuse mitigation mechanisms must respect privacy and anonymity.
- **Access to Appeals and Redress:** Affected registrants should be offered clear, accessible mechanisms to challenge mitigation decisions and/or actions.

# DNS Abuse Mitigation: Feedback on Preliminary Report

- **Diversifying sources cited**: The CCWP-HR and NCSG members have developed tools for conducting HRIAs for PDPs and have undertaken a collective HRIA on DNS Abuse mitigation during ICANN. These resources could have provided additional and much-needed information to ground this report, but were not cited.

- **Post-registration Identity Checks:** the NCSG reiterates its position that the requirement for "data accuracy" when it comes to registrant data only encompasses contactability, not identity verification

- **Lack of Standard Dispute/Recourse Mechanism for Registrants**: The NCSG is very concerned that this gap was not listed as a priority item. Such a PDP would go far in terms of operationalizing/respecting ICANN's human rights commitment per ICANN's bylaws. Regardless of the specific issue to be prioritized for a PDP, the outcome of any PDP must include clear due process elements.

- **Recommendations for 'proactive monitoring' must be undertaken with the utmost care:** Even where technically possible, the constant monitoring of all registrants' domain-related activities amounts to a staggering system of surveillance Such techniques should also only be undertaken with clear safeguards.

# DNS Abuse Mitigation: Upcoming PDP

***The NCSG Supports***

I. Narrowly targeted PDP(s)
II. Gathering further opinions from stakeholders during upcoming ICANN meetings
III. Clear timelines and milestones for any potential PDP(s)

***On the two issues proposes, the NCSG has the following feedback***

**IV. Unrestricted API Access for Domain Name Registration for New Customers**

We appreciate the logic that by taking action at this stage of the domain lifecycle, we could prevent DNS abuse further down the line. However, the charter question for this PDP neglects to account for undue burden that such barriers to accessing APIs could pose to new registrants. The charter should therefore also include a question about how to find this balance.

**V. Associated-Domain Checks**

When investigating actionable DNS abuse, registrars may need to examine other domains associated with the same registrant data to disrupt broader abuse networks. However, such inspections must be conducted with strict safeguards to avoid undue surveillance of legitimate registrants. An HRIA must also be conducted for any solutions to ensure that the risk to privacy and anonymity of registrants is not compromised and that this does not pose an undue burden on smaller registrants.

# ICANN Reviews

Manju Chen, NCSG

# ICANN Reviews / Reviews of Reviews

## Background

- The Board passed a resolution effective on 5 September 2025 to approve the Charter as presented to the Board on 25 August 2025.
- The GNSO representatives on the Review of Reviews Cross Community Group are Sophie Hey (CPH) and Osvaldo Novoa (NCPH).
- The reviews and their past outcomes to be evaluated include:
  - Periodic review of ICANN structure and operations (section 4.4),
  - Annual Review (section 4.5) and
  - Specific Reviews (section 4.6); and
  - Previously conducted Reviews; and
  - Reviews that have previously been formally recommended.

# ICANN Reviews / Review of Reviews

## NCSG position

- Look forward to review and comment on the “Purpose of the Review’ that the CCG has been working on.
- Remain concerned about the novelty of the process – should be the community’s collected effort to closely monitor and ensure the RoR remains a once-and-never incident.
- Expect substantial and actionable recommendations from the CCG.

# Agenda

1. **Welcome and Introductions** (Nicolas Caballero, GAC Chair and Rafik Dammak, NCSG Chair)

2. **HRIA and GAC Communique**
   Discuss several points about conducting HRIA and the substance of the communiqué
3. **RDRS, urgent requests/registrant data requests**
   Discuss at a high level the 24hr turnaround, how disclosure to law enforcement should be done and the need for safeguards from NCSG's perspective
4. **DNS abuse mitigation**
   Explaining points supported by NCSG and those not supported
5. **ICANN Reviews / Review of Reviews**

6. **Closing Remarks**
   (Nicolas Caballero, GAC Chair and Rafik Dammak, NCSG Chair)