# Human Rights in ICANN: How We Do It

Authentication · Authorization · DNS Abuse — an HRIA perspective

NCSG — Joint Meeting with SSAC

# What We Will Cover

20 min overview · 60 min discussion

1. **How HRIA developed inside ICANN**
   CCWP-HR, NCSG, ICANN Bylaws, PDP requirement

2. **The Rapid HRIA method**
   Inspired by BSR — applied to GAC communiques and policy

3. **Case study: Law enforcement authentication**
   SSAD Urgent Requests — what went wrong in practice, and what HRIA requires

4. **Case study: DNS Abuse — Associated Domain Checks**
   Guilt by association, privacy, due process

5. **Why this is relevant to SSAC**
   Security advisories carry human rights stakes too

# How HRIA Developed Inside ICANN

Built by NCSG and the community — not mandated from above

**2016+**

### CCWP-HR established

Cross-Community Working Party on ICANN & Human Rights — first formal community space linking ICANN policy to human rights obligations in the Bylaws

**~2019**

### ICANN Org first HRIA

ICANN published its first organizational human rights impact assessment

**ICANN 81-82**

### NCSG HRIA working sessions

NCSG organized the first practical tabletop HRIA exercises at ICANN meetings — scenarios from real registrant risks (Sudan media, activist sites, protest sites)

**2024**

### NCSG Rapid HRIA on GAC communique

NCSG published the first rapid HRIA on a GAC communique — on law enforcement confidentiality of WHOIS requests

**2026**

### PDP HRIA requirement & LE report

New PDPs required to include HRIA at charter stage.

# What is a Human Rights Impact Assessment?

NCSG has been developing and applying this methodology within ICANN

## The BSR definition

*"A human rights assessment identifies and prioritizes actual and potential adverse human rights impacts and makes recommendations for appropriate action to address those impacts."*

**Key distinction:**

An HRIA assesses risks to people — not risks to companies or organizations. This is the inversion that matters.

We apply this to GAC communiques, PDP proposals, and policy amendments — periodically and systematically, not just at charter stage. Can apply it to SSAC documents too :)

## General HRIA process

1. **Identify rights at risk**

   Map which human rights may be impacted by the policy or action

2. **Affected communities**

   Who is most vulnerable? Consultation with impacted groups

3. **Stakeholder engagement**

   Bring in affected parties — including those without a seat at the table

4. **Remedies & mitigation**

   Concrete recommendations for avoiding or reducing harm

# The Rapid HRIA Method

Adapted from BSR — applied to fast-moving ICANN policy decisions

We apply this to GAC communiques, PDP proposals, and policy amendments — periodically and systematically.

1

### Rightsholders

Who is affected? Registrants, esp. vulnerable communities: journalists, activists, political opposition, LGBTQI groups, minority religious communities

2

### Severity

What harms are possible? Prosecution · surveillance · unlawful arrest · imprisonment · house raids · cruel punishment

3

### Long-term implications

Chilling effect on domain names for free expression? Incentive for inaccurate data? Erosion of trust?

4

### Peer practice

What do comparable institutions do? e.g., RIPE NCC publishes transparency reports on LE data requests — ICANN should not offer less accountability

5

### Mitigation

What should the policy do to prevent or reduce harm? What remedies are needed?

# Rapid HRIA in Action: GAC Cancun Communique

NCSG / Digital Medusa applied the Rapid HRIA framework to a real GAC recommendation

**GAC Cancun 2023:**
*"...identify and advance solutions for confidentiality of law enforcement requests so as not to preclude participation by law enforcement requesters when measuring usage of the WHOIS Disclosure System."*

| | |
|---|---|
| **Rightsholders:** | Domain name registrants — especially LGBTQI groups, political opposition, minority religious communities, journalists |
| **Severity:** | Prosecution · surveillance · unlawful arrest · imprisonment · illegal house raids · cruel punishment |
| **Long-term:** | Chilling effect on use of domain names for free expression; incentive for inaccurate registration data |
| **Peer practice:** | RIPE NCC publishes transparency reports on LE requests — ICANN should not offer less accountability, not more secrecy |
| **Conclusion:** | **ICANN should NOT grant law enforcement the option to seek disclosure confidentially — transparency is itself a safeguard** |

Case Study 1

# Authentication & Authorization

SSAD Urgent Requests

# What Went Wrong: Authentication Failures in Practice

Three documented cases from NCSG's law enforcement research — why HRIA matters before systems are built

**2021**

## Forged emergency requests — Apple, Meta, Discord

A cybercrime group obtained private user data from Apple, Meta, and Discord by submitting forged emergency disclosure requests impersonating law enforcement. No court order was needed — the emergency channel bypassed standard legal thresholds entirely. Data was disclosed before the fraud was detected.

*HRIA lesson: Authentication of identity is not the same as legitimacy of the request. Emergency pathways that skip judicial oversight are structurally vulnerable to abuse.*

**2024–25**

## Fraudulent account in Google LERS portal

A fraudulent account was created inside Google's Law Enforcement Request System (LERS) by impersonating a government entity. Google stated the account was disabled before data was accessed, but the incident exposed a core vulnerability: a compromised identity inside a centralized portal can bypass all downstream safeguards.

*HRIA lesson: Centralized authentication portals are high-value targets. The more they streamline access, the more dangerous a single compromised credential becomes.*

**Ongoing**

## Kodex and commercial authentication intermediaries

Commercial platforms like Kodex authenticate law enforcement identities globally — but only verify who is requesting, not whether the request is lawful, proportionate, or consistent with human rights. Reports note these mechanisms are not immune to vulnerability. Authentication is outsourced; human rights assessment is not.

*HRIA lesson: Verification of identity does not substitute for assessment of legislative mandate, proportionality, or necessity. These are separate questions requiring separate answers.*

# Authentication

The HRIA lens reveals what identity verification alone misses

**Current framing**

## Identity verification only

Is this person who they claim to be?

A DUG membership check, or an identity provider confirming agency affiliation.

**NCSG framing (consistent with Steve Crocker)**

## Verification + Legislative mandate

**1. Is this agency who it claims to be?**

**2. Does this agency have a legal basis under its domestic law to access?**

An agency can be authenticated as a police force and still be acting without judicial authorization, or targeting political dissidents.

*The registrant is never a party to this process and will never know a request was made. The HRIA question is not 'Is this a real law enforcement agency?' — it is 'Does this request, from this country, against this registrant, meet proportionality and necessity standards?'*

# Authorization: Necessity, Legitimacy & Proportionality

The three-question legal test — plus NCSG's operational checklist for registrars

**Legitimacy**

### Is the purpose legitimate?

Does the requesting authority have a lawful mandate under its domestic law? Is the stated objective a recognized ground for restricting privacy rights (e.g. crime prevention, national security)?

**Necessity**

### Is this the least invasive means?

Have other investigative paths been exhausted? Infrastructure data should be a last resort — not a first request. Necessity is not only a legal standard; it is a human rights test.

**Proportionality**

### Is the intrusion proportionate to the aim?

Is the scope of data requested matched to the severity and specificity of the investigation? Does the harm to the registrant's rights outweigh the benefit to the stated purpose?

**Operational checklist — NCSG recommends registrars also ask:**

- **Active conflict or crisis in the requesting country?**
  Ongoing conflict or suspension of rule of law changes the risk calculus
- **Country freedom ranking?**
  Freedom House, RSF press freedom index — proxy for systemic risk
- **Sensitive or vulnerable registrant?**
  Journalism, political opposition, LGBTQI groups, minority religious groups, human rights defenders
- **Judicial authorization provided?**
  Or only an administrative/emergency request? Is the claimed urgency substantiated?

Case Study 2

# DNS Abuse Mitigation & Associated Domain Checks

PDP 1 — ICANN 2026 — What HRIA sees that the charter did not ask

# Associated Domain Checks: What HRIA Reveals

PDP 1 — DNSAM Working Group, launched January 2026 — NCSG is an active participant

## What ADC does

When one domain in a registrant's portfolio is confirmed malicious, the registrar must examine ALL other domains held by the same registrant.

Rationale: abuse clusters — bad actors spread infrastructure to resist takedown.

NCSG position: Done right, ADC is a useful mitigation tool. Done wrong, it becomes a registrant surveillance mechanism based on guilt by association.

## HRIA risk register

- **Guilt by association**

  One abusive domain triggers investigation of entire portfolio — including legitimate domains of journalists, activists, NGOs

- **Portfolio exposure**

  Registrant's full domain holdings become visible — a surveillance footprint created by policy design

- **Account-level takedown**

  Registrars may take the whole account down rather than domain-by-domain — no proportionality constraint in current draft

- **No due process**

  Registrant not notified; no mechanism to challenge suspension; appeal rights undefined in the PDP

# The HRIA Tabletop: Scenarios from ICANN 81 & 82

NCSG organized these sessions — real situations, no hypotheticals

ICANN 81

### Human rights activist site compromised

An activist's website is used as a phishing vector by an adversary. A technically correct abuse suspension would simultaneously silence the activist. No current ICANN mechanism distinguishes the victim registrant from the abuser.

ICANN 81

### Protest site also engaged in phishing

A site engaged in both legitimate political speech and active phishing. ADC logic: one confirmed abuse domain triggers investigation of entire portfolio. An HRIA asks: what process protects the political speech while addressing the abuse?

ICANN 82

### Sudan independent media

Multiple independent media platforms became inaccessible due to DNS-related actions during conflict. A technically justified action collapsed access to information. No transparency, no recourse for affected users.

# Why This Is Relevant to SSAC

Security advisories carry human rights stakes — even when not framed that way

### Technical mechanisms have human rights implications

Authentication systems, abuse reporting pathways, data access protocols — the HRIA question is not just 'does it work?' but 'who is harmed if misused?'

### Abuse tools can be weaponized

Technically valid mechanisms have been used against journalists and dissidents. An HRIA lens asks not just whether a request is well-formed, but whether its purpose is legitimate.

### SSAC advisories shape PDP deliberations

When SSAC advises on a new mechanism, that advice lands in GNSO policy work. An HRIA flag in an SSAC advisory gives the policy community the signal it needs early.

### We are not asking SSAC to become a human rights body

We are asking: could future advisories note when a security mechanism carries human rights risk alongside technical risk?

# The Ask — and Questions for Discussion

1. Authentication for LE Urgent Requests must include mandate verification — not just identity verification

2. Authorization requires assessment of legitimacy, necessity, and proportionality — not just a legal instrument check

3. ADC policy must include proportionality constraints and due process — association is not confirmation of abuse

4. SSAC advisories could flag human rights risk factors alongside technical ones, consistent with ICANN Bylaws