

Drafting Human Rights-Respecting Board Resolutions

A Constructive Proposal from the Noncommercial Stakeholder Group

Re: The October 2025 Resolution on RDRS and Law Enforcement Authentication

ICANN85 – Mumbai, March 2026

Purpose of This Document

NCSG has consistently asked the ICANN Board to consider human rights when drafting its resolutions. The Board’s February 2026 response to our December 2025 letter acknowledged shared expectations for safeguards, transparency, and accountability in the context of law enforcement authentication. This document takes that shared commitment and makes it operational.

We are not asking for human rights language in every Board resolution. But when a resolution directly concerns law enforcement access to people’s personal data, the resolution itself should reflect that this is a human rights issue. Authentication of law enforcement for the purpose of requesting access to registrants’ personal information engages privacy, due process, freedom of expression, and protection from arbitrary interference. A resolution that treats this exclusively as an operational matter sends a signal that human rights are an afterthought, not a design requirement.

This document presents the Board’s original October 2025 resolution alongside a proposed revision that integrates rights safeguards with the operational objectives. The goal is to demonstrate that these objectives are complementary, not competing, and to offer the Board a practical template for future resolutions that engage human rights concerns.

Reading Guide

[NEW] New clauses added by NCSG to address rights, safeguards, and accountability

[AMENDED] Existing clauses modified to integrate rights considerations

Unmarked clauses are retained from the original resolution without change

What Is Missing

The resolution as adopted addresses operational continuity, system usage, registrar engagement, and policy alignment. These are legitimate and necessary considerations. However, the resolution is silent on the following:

- The rights and interests of registrants and end users, who are the data subjects whose personal information the RDRS facilitates access to. They do not appear as affected stakeholders in the resolution or its rationale.
- Safeguards for the law enforcement authentication mechanism. Resolution 2025.10.30.16 encourages collaboration with the GAC PSWG on authentication, but contains no requirement that the resulting mechanism include oversight, misuse prevention, transparency, or redress.
- Systemic accountability. Section 10 of the Registration Data Policy governs how individual registrars handle individual requests. It does not address system-level accountability: who audits the mechanism, how aggregate patterns of use are monitored, what reporting is required, or how the mechanism is evaluated over time.
- ICANN's own bylaw commitment to respect internationally recognized human rights. A resolution directing work on law enforcement access to personal data is a textbook case where this commitment should be operationalized, not merely assumed.
- Transparency obligations. There is no requirement for aggregate public reporting on the volume, origin, type, or disposition of requests processed through the RDRS or any future authentication-enabled system.

The Board's February 2026 response to NCSG stated that Section 10 of the Registration Data Policy and the GNSO Standing Committee's consensus address these concerns. They do not. Section 10 governs micro-level request handling by individual registrars. It does not constitute systemic governance of the authentication framework. And the Standing Committee's consensus was on a procedural recommendation to explore authentication—not an endorsement of a resolution that frames the matter in exclusively operational terms.

NCSG’s Proposed Human Rights-Respecting Resolution

Below is the complete resolution with NCSG’s proposed additions and amendments. All original clauses are preserved. New and amended clauses are highlighted. The additions do not alter the operational objectives of the resolution; they complement them by ensuring the framework is rights-respecting, accountable, and transparent.

Whereas Clauses

Whereas, the ICANN Board noted in its resolution that the metrics from system usage and observation of trends would inform future discussions with the GNSO Council about the RDRS and decisions regarding the future of outstanding policy recommendations from the Expedited Policy Development Procedure on the Temporary Specification Phase 2 for a System for Standardized Access/Disclosure (SSAD).

Whereas, on 28 November 2023, the ICANN organization launched the renamed Registration Data Request Service (RDRS) for requestors and for voluntary registrar participation.

Whereas, since launch, the ICANN organization has published monthly usage metrics, quarterly satisfaction survey results from both requestors and participating registrars, and has discussed and documented enhancements to the service with the GNSO Standing Committee on RDRS.

Whereas, the GNSO Standing Committee has completed its Findings Report on the RDRS and recommended that the service continue to operate while further GNSO policy work proceeds.

Whereas, the pilot period is scheduled to end in November 2025.

[NEW] Whereas, the RDRS and any successor system or authentication mechanism facilitates third-party access to nonpublic registration data, including personal information of domain name registrants who are the data subjects directly affected by such disclosure.

[NEW] Whereas, ICANN’s Bylaws, Article 1, Section 1.2(b)(viii), commit ICANN to carrying out its activities in a manner consistent with relevant principles of international law and international conventions and with applicable local law, and with due regard for the public interest, including the rights of registrants and end users.

[NEW] Whereas, the Framework of Interpretation for Human Rights, adopted by the ICANN Board, provides that ICANN will respect internationally recognized human rights as required by applicable law and, in particular, recognizes that privacy and data protection are fundamental rights engaged by registration data disclosure.

[NEW] Whereas, authentication of law enforcement agencies for the purpose of accessing personal registration data engages fundamental rights including privacy, due process, and protection from arbitrary interference, and that the design and governance of such mechanisms should reflect these considerations.

[NEW] Whereas, the NCSG and other community groups have consistently emphasized that any authentication or accreditation mechanism must be accompanied by safeguards, transparency, accountability, and meaningful consideration of registrant and end-user rights, and that such considerations are integral to—not separate from—the operational design of the system.

Resolved Clauses

Resolved (2025.10.30.13), the ICANN Board directs the ICANN President and CEO, or his designee(s), to continue operations of the RDRS for a period of up to two years, until December 2027, while the community continues its deliberations regarding the future of the service and related policy recommendations.

Resolved (2025.10.30.14), the ICANN Board directs the ICANN President and CEO, or his designee(s), to continue to engage with the GNSO Council and the GNSO Standing Committee on any further enhancements to the service during this period.

Resolved (2025.10.30.15), the ICANN Board directs the ICANN President and CEO, or his designee(s), to encourage continued comprehensive RDRS usage by data requestors and by ICANN-accredited registrars.

[AMENDED] Resolved (2025.10.30.16), the ICANN Board encourages the ICANN President and CEO, or his designee(s), to continue to collaborate with the GAC PSWG on possible law enforcement authentication mechanisms, and directs that the development of any such mechanism shall incorporate safeguards including: clear and publicly disclosed criteria for authentication eligibility; mechanisms for the prevention, detection, and remediation of misuse; independent oversight or periodic review of the mechanism's operation.

[NEW] Resolved (2025.10.30.16a), the ICANN Board directs the ICANN President and CEO, or his designee(s), to ensure that the RDRS and any successor system or authentication mechanism includes aggregate transparency reporting obligations, including periodic public disclosure of the volume, categories of requestors, geographic distribution, and disposition of requests processed, in a manner that enables community oversight without compromising the integrity of individual investigations.

[NEW] Resolved (2025.10.30.16b), the ICANN Board recognizes that registrants and end users are central stakeholders affected by the operation of the RDRS and any future authentication mechanism, and directs the ICANN President and CEO, or his designee(s), to ensure that any assessment of community impact associated with these systems explicitly addresses the effects on registrant rights and interests, including privacy and data protection.

[NEW] Resolved (2025.10.30.16c), the ICANN Board affirms that the continued operation of the RDRS and the development of law enforcement authentication mechanisms shall be conducted in a manner consistent with ICANN's commitment under its Bylaws and the Framework of Interpretation for Human Rights to respect internationally recognized human rights, and directs that this commitment shall be reflected in the design, governance, and evaluation of these systems.

[NEW] Resolved (2025.10.30.18a), the ICANN Board directs the ICANN President and CEO, or his designee(s), to include, in any future report to the Board on the operation of the RDRS or the development of authentication mechanisms, an assessment of whether the safeguards, transparency, and accountability provisions directed by this resolution have been implemented and are functioning effectively.

Part IV: Explanatory Notes

The following explains the rationale behind each proposed addition.

New Whereas Clauses

The five new whereas clauses establish the normative foundation that is absent from the original resolution. They do three things. First, they name registrants and end users as the data subjects affected by the RDRS. Second, they anchor the resolution in ICANN's existing legal commitments—the Bylaws and the Framework of Interpretation for Human Rights—rather than introducing new obligations. Third, they recognize that authentication of law enforcement for access to personal data is inherently a human rights matter, so that the resolved clauses can direct action accordingly.

Importantly, these clauses do not create new rights or obligations outside ICANN's existing framework. They make explicit what is already implicit in ICANN's Bylaws. The question is not whether ICANN has these commitments, but whether its resolutions reflect them when it matters most.

Amended Resolution 2025.10.30.16

The original clause encourages collaboration with the GAC PSWG on authentication mechanisms. The amendment retains this direction and adds a requirement that the mechanism include specific, enumerated safeguards: eligibility criteria, misuse prevention, independent oversight, and registrant redress. These are not abstract principles; they are concrete design requirements that any credible authentication system should include. The Board's own February 2026 response stated it shares NCSG's expectations for safeguards. This clause operationalizes that shared expectation.

New Resolution 2025.10.30.16a (Transparency)

This clause addresses the systemic accountability gap that Section 10 of the Registration Data Policy does not cover. Section 10 governs how individual registrars handle individual requests. It says nothing about aggregate transparency—how many requests are made, by whom, from where, and with what outcomes. Without this information, neither the Board nor the community can assess whether the system is functioning as intended or whether patterns of misuse are emerging. The clause includes a proportionality safeguard: reporting should enable oversight without compromising individual investigations.

New Resolution 2025.10.30.16b (Registrant Impact)

This clause addresses the most fundamental omission in the original resolution: the absence of registrants and end users from the community impact assessment. The Board's rationale discussed operational continuity, registrar satisfaction, resource needs, and system usage—but not the people whose data flows through the system. This clause does not limit the Board's operational discretion; it requires that when the Board assesses community impact, it explicitly considers the effects on the people most directly affected.

New Resolution 2025.10.30.16c (Human Rights Consistency)

This clause connects the resolution to ICANN's existing Bylaws commitment and the Board-adopted Framework of Interpretation for Human Rights. It does not impose new obligations; it ensures that existing commitments are reflected in the resolution directing operational work. If ICANN's commitment to respect internationally recognized human rights means anything, it should appear in resolutions that direct work on law enforcement access to personal data.

New Resolution 2025.10.30.18a (Periodic Review)

This clause creates a feedback loop. Safeguards, transparency, and accountability provisions are only meaningful if they are monitored. Directing that future reports to the Board include an assessment of whether these provisions have been implemented and are functioning effectively ensures that the commitments in this resolution are not a one-time gesture but an ongoing governance requirement.

Conclusion: A Template, Not an Exception

NCSG offers this proposal in a constructive spirit. Our purpose is not to relitigate the October 2025 resolution, but to demonstrate what a human rights-respecting resolution looks like in practice. We believe this model can serve as a template for future Board resolutions that engage registrant rights—not as a requirement for every resolution, but as a standard practice when the subject matter demands it.

Law enforcement authentication for access to people’s personal data is precisely the kind of issue where ICANN’s Bylaws commitment to respect internationally recognized human rights should be visible in the Board’s own directives. Making that commitment visible does not slow down operational work. It strengthens it, by ensuring the mechanism is designed to be accountable and trustworthy from the outset.

NCSG respectfully asks the Board to consider this proposal and to work with us on developing a standing approach to human rights-respecting resolutions that the Board can draw on whenever its actions directly engage the rights of registrants and end users.

The Original Board Resolution (30 October 2025)

Below is the operative text of the Board’s resolution as adopted at the Regular Meeting of 30 October 2025, concerning the continuation of the Registration Data Request Service.

Whereas Clauses

Whereas, the ICANN Board noted in its resolution that the metrics from system usage and observation of trends would inform future discussions with the GNSO Council about the RDRS and decisions regarding the future of outstanding policy recommendations from the Expedited Policy Development Procedure on the Temporary Specification Phase 2 for a System for Standardized Access/Disclosure (SSAD).

Whereas, on 28 November 2023, the ICANN organization launched the renamed Registration Data Request Service (RDRS) for requestors and for voluntary registrar participation.

Whereas, since launch, the ICANN organization has published monthly usage metrics, quarterly satisfaction survey results from both requestors and participating registrars, and has discussed and documented enhancements to the service with the GNSO Standing Committee on RDRS.

Whereas, the GNSO Standing Committee has completed its Findings Report on the RDRS and recommended that the service continue to operate while further GNSO policy work proceeds.

Whereas, the pilot period is scheduled to end in November 2025.

Resolved Clauses

Resolved (2025.10.30.13), the ICANN Board directs the ICANN President and CEO, or his designee(s), to continue operations of the RDRS for a period of up to two years, until December 2027, while the community continues its deliberations regarding the future of the service and related policy recommendations.

Resolved (2025.10.30.14), the ICANN Board directs the ICANN President and CEO, or his designee(s), to continue to engage with the GNSO Council and the GNSO Standing Committee on any further enhancements to the service during this period.

Resolved (2025.10.30.15), the ICANN Board directs the ICANN President and CEO, or his designee(s), to encourage continued comprehensive RDRS usage by data requestors and by ICANN-accredited registrars.

Resolved (2025.10.30.16), the ICANN Board encourages the ICANN President and CEO, or his designee(s), to continue to collaborate with the GAC PSWG on possible law enforcement authentication mechanisms.

Resolved (2025.10.30.17), the ICANN Board urges the GNSO Council to ensure that future policy work on the System for Standardized Access/Disclosure (SSAD) recommendations is aligned with policies related to requests for underlying registration data for domains registered under privacy and proxy services, an enforceable timeline for urgent requests, and other relevant procedures.

Resolved (2025.10.30.18), the ICANN Board urges the GNSO Council to consider the RDRS Policy Alignment Analysis, published concurrently with this resolution, in its future consultation with the ICANN Board on the EPDP Phase 2 policy recommendations.

