Re-the October 2025 Resolution Concerning Law-Enforcement Authentication and Registrant Rights

Dear ICANN Board, December 1, 2025

Participation in ICANN's multistakeholder processes allows issues to be raised that would not easily surface in governmental or private-sector environments. The Noncommercial Stakeholder Group (NCSG) has consistently contributed to policy development and has engaged the ICANN Board for many years on matters affecting domain name registrants and end users. This context is important because the Board's recent resolution on law-enforcement authentication appears to overlook concerns that NCSG has repeatedly placed on the record.

The October 2025 resolution signals the Board's intent to accelerate and align work on systems that facilitate disclosure of non-public (private and sensitive) registration data. It encourages continued collaboration with the GAC Public Safety Working Group on law-enforcement authentication, and directs the GNSO Council to ensure that future SSAD-related work aligns with policies governing access to underlying data, privacy/proxy issues, and urgent disclosure timelines. NCSG has no objection to authentication or accreditation of law-enforcement agencies; properly authenticated requests can support accountable, auditable access to sensitive registrant data.

However, the Board's explanatory text focuses largely on operational continuity of the RDRS, registrar and requestor satisfaction, voluntary participation, and resource considerations. It cites the Standing Committee's Findings Report, usage metrics, ICANN org's resource needs, and the Policy Alignment Analysis, and highlights community concerns about losing access to the RDRS or integrating future authentication mechanisms.

What is absent, despite NCSG's long standing input in meetings with the Board, written correspondence, and contributions to the Standing Committee report, is recognition that any authentication or accreditation mechanism must be accompanied by safeguards, transparency, and accountability. While the resolution references LEA validation, it does not address oversight, prevention of misuse, public reporting, or redress. As a result, domain name registrants and Internet end users, the primary subjects of the data at issue, do not appear in the Board's assessment of community impact.

By omitting these considerations, the Board presents an incomplete picture of the policy implications. NCSG's public comment on the RDRS made this clear: "Where international LEAs are involved, the mechanisms used for verification, eligibility, and request handling must be transparently disclosed." Any evaluation of "community impact" should therefore explicitly include the effects on registrants and end users, whose rights and interests are directly shaped by these decisions.

NCSG respectfully requests that the Board revise its explanatory text to reflect the full policy implications of law-enforcement authentication. In particular, the text should acknowledge that authentication must be accompanied by safeguards, transparency, accountability, and meaningful consideration of registrant and end-user rights, and that this is not merely an operational matter.

We also urge the Board to recognise explicitly that registrants and end users are central stakeholders affected by these decisions, and to reflect this in its assessment of community impact. NCSG stands ready to support the Board in developing a rights-respecting and accountable framework for law-enforcement authentication.

Best regards,

Rafik Dammak
NCSG Chair
On behalf of the NCSG