Public Comment Summary Report

Registration Data Request Service (RDRS) Policy Alignment Analysis

Open for Submissions Date:
Thursday, 30 October 2025

Closed for Submissions Date:
Tuesday, 15 December 2025

Summary Report Due Date:
Tuesday, 20 January 2026 (extended from Friday, 09 January 2026)

Category: Policy

Requester: ICANN Board

ICANN organization contact(s):
lisa.carter@icann.org

Open Proceeding Link:

https://www.icann.org/en/public-comment/proceeding/registration-data-request-service-rdrs-policy-alignment-analysis-30-10-2025

Outcome:

The ICANN organization appreciates the comments submitted by the community on the RDRS Policy Alignment Analysis. ICANN org received 13 submissions which generally support the goals and direction of the RDRS Policy Alignment Analysis, particularly the intent to improve consistency, predictability, and transparency in registration data disclosure processes. However, support was frequently paired with requests for clarification, limitation, or future policy work before broader adoption or expansion.

The common themes of overall feedback include:

- Governance and policy alignment clarity
- Voluntary vs. mandatory registrar participation
- Law enforcement or government access
- Liability and legal risk
- Cost, resourcing, and operational burden
- Scope limitations and future expansion concerns.

Privacy compliance, law-enforcement access, and request response timing concerns, including urgent requests were the most prevalent themes.

Section 1: What We Received Input On

ICANN org published the RDRS Policy Alignment Analysis in October 2025 at the request of the ICANN Board of Directors to collect community input and generate community discussion on the proposed options for aligning the RDRS-related policy gaps identified in the paper. It also was meant to help inform discussions between the ICANN Board and the Generic Names Supporting Organization (GNSO) as they assess the work of the Privacy and Proxy Services Accreditation Issues (PPSAI) IRT and Registration Data Policy IRT, and begin to discuss the consensus policy recommendations for a System for Standardized Access/Disclosure.

Section 2: Submissions

Organizations and Groups:

Name	Submitted by	Initials
Business Constituency	Mason Cole, Steve Crocker and Steve DelBianco	BC
Coalition for Online Accountability	David Hughes	COA
Department of Information and Communications Technology, Government of Papua New Guinea	Jessy Dika Sekere	PNG
Governmental Advisory Committee	Fabien Betremieux	GAC
Intellectual Property Constituency	Margaret Milam	IPC
International Trademark Association	Lori Schulman	INTA
Internet Society Mexico Chapter (ISOC México)	Eunice Alejandra Perez Coello	ISCO (Mexico)
Noncommercial Stakeholder Group	Farzaneh Badii	NCSG
Registrars Stakeholder Group	Zoe Bonython	RrSG
Registries Stakeholder Group	N/A	RySG
Stiftung Digitale Chancen	Torsten Krause	SDC
Tucows	Sarah Wyld	N/A

Individuals:

Name	Affiliation (if provided)	Initials
Remy Nweke - DigitalSENSE Africa (ITREALMS Media)	Remy Nweke	RN

Section 3: Summary of Submissions

Commenters broadly recognize the value of RDRS as a mechanism to improve the handling of registration data disclosure requests and generally support efforts to align the system with existing policy frameworks. At the same time, several submissions consistently caution against treating RDRS as a substitute for formal policy development or allowing operational implementation to resolve open policy questions, and emphasize the importance of transparency, clearly defined limits, and protection against unintended legal or procedural consequences.

There is strong consensus that alignment efforts must remain grounded in data protection and privacy obligations, respect the multistakeholder process, and proceed at a pace that allows for informed community input. Several commenters emphasized the importance of transparency around ICANN org's proposed roadmap, the limitations of voluntary registrar participation, and the potential operational impacts on contracted parties. Submissions most consistently requested clarification of:

- **RDRS's long-term status** and whether registrar participation would remain voluntary versus becoming a mandatory long-term solution.
- **Clear boundaries on scope and expansion** to avoid expanding beyond current use cases or data types without formal policy development.
- **Defined treatment of law enforcement and government access** calling for policy direction on how law enforcement authentication, prioritization, or differentiated access would be handled.
- **Transparency and reporting commitments** for metrics, reporting obligations, and publication of outcomes.
- **Risk, liability, and compliance clarity for contracted parties** due to concerns that unresolved liability exposure or inconsistent legal interpretations could affect participation.

Overall, the submissions reflect cautious support paired with a clear expectation that next steps be deliberate, well-scoped, and explicitly tied to established policy mechanisms. Commenters also provided feedback on the structure and format of the RDRS Alignment Analysis.

Section 4: Analysis of Submissions

Analysis of overall feedback grouped by theme:

Public Comment Theme	Theme Analysis	Representative/Organization Referencing the Theme
Data protection / GDPR alignment	Concerns that RDRS alignment must not create disclosure expectations inconsistent with GDPR and other data protection policies and procedures, especially when those laws differ from one	BC, COA, GAC, INTA, IPC, NCSG, PNG, RN, RrSG, SDC

	country or region to another.	
Law enforcement access and authentication	General support for having predictability for legitimate requestors, paired with caution about protecting privacy and ensuring global accessibility and applicability -- including avoiding the need for new policy development (GAC); recognition that additional policy work may be required to adequately address the complexities of law enforcement authentication processes (Tucows); concerns about other non-LEA authenticated users submitting urgent requests (RySG and Tucows); the view that the authentication system must meet the needs of all parties before the mechanism is implemented; the importance of avoiding system complexity (IPC); and that the need for robust safeguards, transparency and accountability mechanisms (NCSG).	BC, COA, INTA, IPC, NCSG, PNG, RN, RrSG, RySG, SDC, Tucows, ISOC
Timeline and pace of work	Concerns that alignment work could move faster than multi stakeholder consensus or PDP capacity allows.	BC, COA, GAC, INTA, IPC, PNG, RN, RrSG, RySG, SDC
Resourcing and operational burden	Contracted parties highlighted cost, staffing, and technical burden associated with expanded expectations. Others generally noted that resourcing and operational burden should be carefully considered during	COA, IPC, PNG, RN, RrSG, RySG, SDC,Tucows

	this next phase, given original SSAD recommendation concerns.	
Voluntary participation vs. mandatory participation for registrars and ccTLDs	Questions raised about whether voluntary participation can deliver consistent, predictable outcomes. Most support mandatory registrar participation and voluntary ccTLD. However, Tucows, RrSG, and NCSG participation do not support making registrar participation mandatory. Tucows and RrSG also do not support voluntary participation for ccTLDs.	BC, COA, IPC, PNG, RN, RrSG, RySG
Accuracy and quality of data	Emphasis that disclosure effectiveness depends on data quality and registrar practices.	BC, IPC, PNG, RN
Scope creep / mission concerns	Concerns that alignment efforts could implicitly expand ICANN's role.	IPC, RrSG, RySG, NCSG

ICANN org also notes the following feedback on the proposed enhancements and options for policy alignment in the RDRS Policy Alignment Analysis.

Mandatory Registrar Participation in RDRS:

Comments generally regard mandatory registrar participation as a policy-level determination, not an operational refinement. While some acknowledged that voluntary participation may limit effectiveness and consistency, commenters cautioned against imposing mandatory participation through alignment or implementation activities alone. A common theme in the comments was that any move toward mandatory participation would require formal policy development and community consensus. Several commenters do not support mandatory registrar participation (RrSG, Tucows, NCSG). Others question the effectiveness of a voluntary model (IPC, BC, GAC) and support further policy development for mandatory contracted party participation. IPC specifically supports mandatory participation of registrars and registry operators.

API for Registrars and Requestors:

Commenters generally viewed the use of APIs for registrars and requestors as a potentially beneficial technical enhancement, particularly if it improves efficiency, consistency, and usability of the RDRS (BC, COA, GAC, INTA, IPC, PNG, RN, RrSG, RySG).

At the same time, commenters stress that APIs should remain neutral technical tools and not introduce new rights, obligations, or disclosure expectations. Concerns were raised about security, operational control, and the risk that APIs could unintentionally standardize or privilege certain disclosure outcomes without policy guidance (RrSG, RySG).

Overall, the comments reflect openness to APIs, based on careful scoping, transparency, and safeguards to ensure that policy questions are not resolved implicitly through technical design and do not expand disclosure expectations.

Phased Federated Authentication

Authentication improvements were generally acknowledged as valuable for improving trust and efficiency in disclosure request handling. However, submitters expressed divergent views on the idea of beginning federated authentication with law enforcement requestors. Several commenters (IPC, RrSG, RySG, and COA) cautioned that prioritizing law enforcement in a phased authentication approach could be interpreted as conferring special status or implicitly resolving policy questions regarding access, absent community agreement. Others noted that such sequencing raises policy-sensitive questions related to fairness, jurisdictional variation, and ICANN's role (NCSG).

While some submitters recognized potential practical benefits in starting with a well-defined requester group, several commenters indicated caution, with calls for clarity, transparency, and appropriate policy recommendations before adopting a law-enforcement-first approach.

Service Level Agreements (SLAs) for Substantive Responses on an Agreed Timeline

Comments broadly supported the goal of timely and predictable handling of disclosure requests. However, some expressed significant concern about establishing enforceable SLAs that would require registrars to provide substantive responses within fixed timelines and highlighted variability in legal obligations, request complexity, and jurisdictional requirements, cautioning that rigid timelines could create legal risk or unintended consequences (RrSG, RySG, IPC). Many framed SLAs as policy obligations rather than operational improvements, suggesting that such requirements should not be imposed through alignment or implementation work alone (COA, SDC). The GAC requested further information on the elements of the SLAs from the ICANN Board.

Requests for Underlying Customer Data for Domains Using Affiliated Privacy and Proxy Services

Comments are generally supportive of the policy work needed to address requests for access to underlying customer data for domains registered through affiliated privacy and proxy services (COA, BC, GAC, INTA, IPC) and recognize the complex and sensitive nature of the work. The NCSG emphasized privacy protections, while the RrSG expressed concerns regarding contractual arrangements, and legal exposure for registrars, but noted the interests of legitimate requestors in accessing accurate data.

The RrSG submission also noted that existing privacy and proxy frameworks were designed to balance competing interests, and cautioned against altering those balances through RDRS alignment activities, as well as highlighting the unresolved policy questions, particularly around authority, due process, and compliance with data protection laws.

Country Code Top-Level Domain Participation:

Comments broadly recognized that ccTLDs operate within distinct governance, contractual, and legal frameworks, and reflected a shared understanding that ICANN does not have the same authority over ccTLDs as it does over gTLD registrars or registries. As a result, voluntary participation for ccTLDs was generally viewed as appropriate and expected (BC, COA, GAC, IPC, INTA, PNG, RN). Commenters did raise some concerns with maintaining a voluntary model for ccTLDs and emphasized respect for national laws, jurisdictional diversity, and the autonomy of ccTLD operators (RySG, RrSG). Tucows and RrSG also noted they do not support voluntary ccTLD participation without full consideration of the key questions provided in the RrSG submission, and highlight operational complexities that may require policy development work, as well as potential user confusion due to uneven ccTLD participation.

Additional Comments:

The NCSG expressed concern that the Alignment Analysis makes no mention of an RDRS human rights impact assessment, as discussed during ICANN84, or upholding data protection rights, and called on ICANN to reiterate its human rights commitment per section 1.2(b)(viii) of ICANN's Bylaws through integration of human rights protection mechanisms for registrants as an integral step in enhancing RDRS or successor system.

The RrSG and Tucows expressed significant concern regarding lack of consideration given to cost recovery billing for RDRS, indicating billing functionality as a crucial component of any long-term system, and urged the ICANN Board to confirm that any long-term system made mandatory for registrars prioritizes implementing billing functionality.

Tucows requested the SSAD Operational Design Assessment (ODA) be updated with the data that has now been gathered, as noted in their Public Comment on the RDRS Standing Committee Report.

The COA recommended that ICANN consider "introducing an Authorized Requestor (aka Trusted Requestor or Trusted Flagger) framework for vetted and verified entities with a proven track record of lawful reporting of abuse or infringement." Authorized requestors would then receive expedited or priority handling for disclosure requests for nonpublic registration data via RDRS thereby assisting the registrar review processes, and also enhancing responsiveness to legitimate requests while upholding privacy and due process safeguards.

INTA advocated for mandatory disclosure of underlying privacy and proxy customer data when justified by well-founded IP rights violation claims, referencing the PPSAI Final Report Annex B framework, which INTA considers valid under current regulations. INTA recommended reconvening the PPSAI Implementation Review Team to integrate these recommendations into existing policies and RDRS, with further policy development if needed. INTA submitted their comments via letter to ICANN after providing Public Comments. The letter is attached to this summary for reference and review purposes.

Section 5: Next Steps

All comments will be analyzed by ICANN org, the ICANN Board, and GNSO Council to ensure the community's feedback and concerns are considered during consultation discussions on next steps for the System for Standardized Access/Disclosure policy recommendations and aligning RDRS-related policies and other relevant procedures.

December 14, 2025

Submitted via ICANN Public Comment Portal

Re: Registration Data Request System (RDRS) Policy Alignment Analysis

The International Trademark Association (INTA) thanks ICANN for the opportunity to provide comments to the RDRS Policy Alignment Analysis referenced above. INTA is on record for having deep concerns about the efficacy of the RDRS system and we are pleased that the ICANN community is exercising serious efforts towards its improvement. INTA's principal issue with RDRS is that it was not designed with both requestors and registrars needs in mind. For example, the interface is burdensome and confusing to someone who is not familiar with ICANN policy and responses are mostly unsupported and unpredictable. While INTA proposed a rethink of the entire system, rather than incremental improvements to the RDRS pilot, we respect the ICANN Board's decision to continue the pilot. With regard to the suggested improvements, we submit the following on behalf of our members.

Mandatory Registrar Participation in RDRS

The RDRS pilot currently operates on a voluntary basis for registrars, resulting in low usage and inconsistent experiences. INTA strongly supports making participation mandatory for all ICANN-accredited registrars to ensure a reliable, centralized request system, mirroring assumptions in existing EPDP Phase 2 policies. Achieving this requires adopting a Consensus Policy, and INTA urges the GNSO Council to incorporate mandatory adoption into policy work, either by amending current recommendations or initiating a new expedited policy development process.

Inclusion of Privacy/Proxy Customer Data

A significant gap exists concerning the disclosure of underlying customer data for domains registered via privacy or proxy services, which currently are not obligated to participate or disclose data under RDRS. Since about 30% of domains use such services, this gap limits RDRS's scope and effectiveness. INTA advocates for mandatory disclosure of underlying data when justified by well-founded IP rights violation claims, referencing the PPSAI Final Report Annex B framework, which remains valid under current regulations. INTA recommends reconvening the PPSAI Implementation Review Team to integrate these recommendations into existing policies and RDRS, with further policy development if needed.

Response Timeline and Service Level Agreements for Urgent Requests

Currently, the Registration Data Policy mandates responses to disclosure requests within 30 calendar days but lacks expedited timelines for urgent requests such as threats to life or critical infrastructure attacks. INTA and other stakeholders view this absence of binding rapid response timelines as a serious concern. The document notes the need for a faster response mechanism for urgent cases, although a specific recommended path is pending.

Accreditation and Authentication of Requestors

The RDRS pilot lacks formal accreditation or identity verification for requestors, which hinders automation, causes caution or delays among registrars, and creates inefficiencies for requestors who must repeatedly prove legitimacy. INTA supports introducing a streamlined accreditation system, starting with law enforcement, and moving then to IP and cybersecurity professionals to improve trust and efficiency while avoiding costly full implementations. This phased approach could be achieved through implementation guidance and incremental enhancements rather than new policy processes.

Standardization of Request Handling and Transparency of Responses

Operational inconsistencies during the RDRS pilot have led to varied and sometimes inadequate responses to requests, including vague refusals and misalignment with EPDP Phase 2 recommendations, such as denying requests solely based on intellectual property infringement claims. As a matter of efficacy, requestors must receive either the requested data or a clear, comprehensible rationale for refusal, as required by the Registration Data Policy, effective since August 2025. To be clear, the uniform template rationales currently contained within the RDRS are inadequate (for example, where the only rationale for rejection was, “More Info Required”) and should be revised to require clear, consistent, and actionable explanations of the basis for refusal and/or requirements for requestor responses. ICANN Compliance is obligated to enforce these obligations, and INTA recommends enhancing implementation notes and adopting relevant EPDP Phase 2 recommendations to improve standardization and transparency.

API Integration and System Efficiency

The current RDRS web portal is manual and cumbersome for high-volume users. INTA supports rapid development of Application Programming Interfaces (APIs) to allow automated request submission and response retrieval, facilitating integration with existing workflows and systems. This improvement does not require new consensus policy and can reduce transaction costs while encouraging participation. INTA recommends prioritizing API development as part of ongoing RDRS maintenance and evolution.

Optional Participation for ccTLDs

While Country Code Top Level Domains (ccTLDs) are not bound by Generic Top Level Domain (gTLD) policies, there is community interest in allowing voluntary ccTLD participation in RDRS to provide a unified system for requestors handling multiple TLDs. INTA supports this voluntary expansion and recognizes it cannot be mandated due to sovereign policies governing ccTLDs.

INTA encourages continued dialogue and designing the RDRS successor system to accommodate ccTLD integration with minimal adjustments.

General Comments

The underlying notion that the sole intended purpose of the RDRS is to facilitate communication between requestors and registrars is fundamentally flawed. The system is more than about basic communication. It should be a sophisticated and efficient means for requestors to clearly communicate all relevant information to establish a legitimate basis for data disclosure from data controllers. It is essential that the system lawfully discloses the requested data or provides a clear, reasoned, and actionable explanation for refusal to disclose requested data when the registrar has determined that the privacy interests of the data subject outweigh all other legitimate interests.

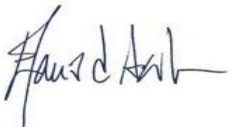
For those who view the RDRS merely as means for communication, the below RDRS Usage Metrics serve as compelling evidence that it fails to facilitate even simple or clear communication. [See metrics infographic on Slide 36 of the Key Insights from the 2-year RDRS Pilot Program presented during ICANN prep week on October 14, 2025.] While some of the deficiencies of the RDRS may be addressed by the improvements currently under consideration in the Alignment Analysis, many deficiencies remain unaddressed.

For example, mandatory registrar participation is intended to address the myriad requests where the "Domain [is] Not Supported." And inclusion of privacy and proxy services is intended to address the numerous requests where the "Data [is] Publicly Available." However, for the RDRS or any other system to be effective, these metrics should show only two or three paths (not dozens of them), namely either "Approved" or "Denied," because privacy interests outweigh requestor interests. To achieve this, many additional improvements are required to cover all facets of the system. As demonstrated in the reference above, all paths represent problems with the RDRS that need to be addresses as soon as possible. For example, rather than leaving requestors in the dark, INTA recommends that ICANN require disclosure in instances where "Domain was Transferred," or where certain "Other Corrective Action Required" (such as when an abusive domain is disabled). Furthermore, the existence of a privacy or proxy service does not justify blanket rejection on the basis that "R[egistrar] Cannot Disclose Due to Law," or a blanked subpoena requirement policy. Finally, if the RDRS request instructions and template are written in clear, plain English then there should be no rejections on the basis that "More Info [is] Required."

Indeed, certain registrars have shared that their own in-house data access systems yield a higher quality of disclosure requests. INTA suspects that the reason may be as simple as the plain English instructions for those in-house access systems, as distinct from the RDRS, which requires expertise in both ICANN policy and data privacy law to navigate. Improvements to the RDRS instructions and request template have been discussed throughout the pilot with continuous input from INTA members. However, INTA is unaware of any meaningful progress on implementation to date.

Thank you for consideration of our input. INTA continues to support the multistakeholder model and urges ICANN to incorporate recommendations from experts within the community to continuously improve its systems to ensure a stable, secure, and unified global Internet. If you have any questions or concerns, please contact Lori Schulman, Senior Director, Internet Policy at lschulman@inta.org

Sincerely,



Etienne Sanz de Acedo
INTA Chief Executive Officer
Esanzdeacedo@inta.org

About INTA

INTA is a global association of brand owners and professionals dedicated to supporting trademarks and complementary intellectual property (IP) to foster consumer trust, economic growth, and innovation, and committed to building a better society through brands. Members include nearly 6,500 organizations, representing more than 34,350 individuals (trademark owners, professionals, and academics) from 185 countries, who benefit from the Association's global trademark resources, policy development, education and training, and international network.