IPC Comment on the the Registration Data Request Service (RDRS) Policy Alignment Analysis

The Intellectual Property Constituency (IPC) appreciates the opportunity to comment on the Registration Data Request Service (RDRS) Policy Alignment Analysis paper (30 Oct 2025). The IPC strongly welcomes efforts to address the gaps identified in the analysis – including mandatory registrar participation, integration of privacy/proxy service data, clear timelines for urgent requests, accreditation of requestors, and system integration (API) – as well as additional gaps the IPC has observed during the RDRS pilot. We believe that closing these gaps is essential to the effectiveness of RDRS for requestors (including IP rights holders) and contracted parties alike.

1. Mandatory Registrar and Registry Participation in RDRS.

Issue: The RDRS pilot is currently voluntary for registrars, meaning many ICANN-accredited gTLD registrars chose not to participate. This optional participation has contributed to low usage by requestors and an uneven experience, as noted by the RDRS Standing Committee's findings. The Board's analysis emphasizes "mandatory registrar participation" as a key component for any long-term disclosure system. Without universal adoption by registrars, the utility of a centralized request system is severely limited – legitimate requestors may not bother using RDRS if large registrars or whole regions are absent. The IPC agrees that making RDRS (or its successor) mandatory for all contracted parties is foundational to its success.

IPC Position: The IPC strongly supports requiring all ICANN-accredited registrars and all registries to participate in the RDRS. This would mirror the assumption under the EPDP Phase 2 (SSAD) policy recommendations that all contracted parties must comply once the policy is in effect. IPC is concerned that the voluntary nature of the pilot depressed request volumes and skewed data, as fewer requestors used a system that didn't cover many registrars. The Standing Committee noted that optional registrar participation would likely reduce requestor participation and that broader participation would improve the system's value. In short, universal participation is needed to ensure legitimate access seekers have a single, reliable channel to reach any registrar and registry. Requiring registries to participate in the RDRS will support compliance with registry specific legal obligations, such as those under the EU NIS2 Directive's Article 28, ensure increased participation rates, and create standardization of disclosure processes that reduce friction and improve outcomes for requesters.

Recommended Path: To achieve mandatory participation, the EPDP Phase 2 Recommendation for a mandatory SSAD must be revised to apply to the RDRS,

since currently no policy obligates the use of RDRS with features that differ from the SSAD. The GNSO Council should act on the Board's invitation to address this gap. The IPC urges the Council to formally incorporate "RDRS mandatory adoption" into its policy work – preferably by amending the existing EPDP Phase 2 policy recommendations rather than initiating a focused policy development process (PDP/EPDP). ICANN Bylaws Annex A Section 9 provides a mechanism for the provision of a Board Statement (of the reasons why the Board considers that a recommendation is not in the best interests of the ICANN community or ICANN Org), Board-GNSO discussion, and development by Council of a Supplemental Recommendation. This was the process used successfully with respect to various "non-adopted" SubPro recommendations. Given that the ICANN Board specifically requested this analysis for community input, the IPC views this as a chance to use this Section 9 process to build consensus on a Supplemental Recommendation requiring that all gTLD registrars and registries use the standardized request system.

2. Inclusion of Privacy/Proxy Customer Data in RDRS

Issue: A significant policy gap exists regarding the disclosure of underlying customer data for domains registered via privacy or proxy services. Neither the current Registration Data Policy (Phase 1) nor the Privacy/Proxy Services Accreditation Issues (PPSAI) recommendations that the ICANN Board adopted in 2016 impose requirements for how privacy/proxy providers must respond to data requests under the RDRS. During the RDRS pilot, many requests involving proxy-protected domains could not be resolved through RDRS because the underlying data is held by privacy/proxy providers that are not obligated to participate or because there is no obligation for the registrars or registrar-affiliated privacy/proxy service providers to disclose underlying customer data behind the privacy/proxy data. This gap is critical. The WHOIS Disclosure System Design Paper noted that roughly 30% of registered domains use privacy/proxy services, meaning nearly one-third of queries could be essentially "out of scope" for RDRS unless this is addressed. This glaring misalignment needs to be fixed, as bad actors often hide behind privacy/proxy services, and IP owners or law enforcement need a streamlined way to secure that underlying information.

IPC Position: The IPC strongly supports requiring disclosure of underlying customer data for registrations using privacy or proxy services where the disclosure request is otherwise determined to warrant disclosure, and the use of a centralized request system (i.e. the RDRS or its successor) for this purpose. At a minimum, the IPC strongly supports mandatory disclosure of underlying customer data in response to requests based on well-founded assertions of IP rights violations by the registrant that meet the criteria set forth in the PPSAI Final Report Annex B. As a reminder, this disclosure framework was previously adopted by the Board when the PPSAI PDP recommendations were adopted as Consensus Policy and remains a valid disclosure framework under current applicable privacy regulations including GDPR. Further, the GNSO Council has now responded to the PPSAI IRT to confirm the

status of that Framework, namely that while “This model is not a binding policy to be implemented verbatim, but it also not merely an example and should be implemented as faithfully as practical with any variations to be communicated transparently and well documented,” bringing to an end any suggestion that the Framework can be discarded.

Recommended Path: To achieve appropriate disclosure of underlying privacy/proxy customer data, the PPSAI recommendations previously adopted by the GNSO Council and ICANN Board should be revisited and the implementation review team (IRT) should be reconvened urgently to integrate those recommendations into existing Registration Data Policy and the RDRS. Where questions arise as to whether any previously adopted recommendations are still valid in light of intervening policy developments, the IRT should flag these for review by the GNSO Council to consider whether any further policy development work is required. If the GNSO Council determines additional policy work on such issues is required, it should initiate a focused policy development process (PDP/EPDP) to address these specific issues.

3. Response Timeline and Service Level Agreements for Urgent Requests.

Issue: The current Registration Data Policy (which resulted from EPDP Phase 1) requires registrars to respond to disclosure requests “without undue delay, but no more than 30 calendar days” in most cases. However, it does not provide a faster timeline for “Urgent” requests, even though EPDP Phase 1 Recommendation 18 had envisaged establishing such an expedited timeline during implementation. Due to a lack of consensus in the Phase 1 IRT, the published Policy (effective August 2025) simply has the 30-day outer limit for all requests, urgent or not. Meanwhile, the EPDP Phase 2 (SSAD) recommendations *did* specify separate turnaround times for urgent vs. normal requests (*e.g.*, 1 business day for urgent). The RDRS pilot, by design, excluded urgent request handling from its scope and has no special SLA for such cases. The gap is that no binding, adopted, policy today guarantees a rapid response for truly urgent disclosure needs, notwithstanding that there is Board-adopted policy requiring that urgent requests be dealt with more rapidly than normal requests, but without setting a specific timing.

IPC Position: The lack of a binding timeline for the handling of urgent requests is a serious concern for the IPC (and others like the Governmental Advisory Committee). Examples of urgent scenarios include threats to life, critical infrastructure attacks, or ongoing phishing/fraud where a quick reveal of registrant information could prevent or significantly mitigate harm.

Recommended Path:

EPDP Phase 1 Recommendation 18, which has been adopted by the Board, makes a recommendation that there should be an expedited time limit for dealing with urgent requests, and that this time limit should be established during implementation.

The IPC supports introducing an authentication system for law enforcement as a first step. Accreditation is critical to improving efficiency and trust in disclosure processes, but the IPC recognizes that the SSAD model raised cost concerns. Therefore, IPC favors a lighter-weight approach that starts with law enforcement. ICANN should develop a streamlined accreditation framework for law enforcement. This can be achieved through implementation guidance and incremental enhancements rather than a new policy process. The goal is a practical, phased solution that balances cost, scalability, and the urgent need for trusted access.

There is currently a public consultation underway on this very issue. Following the conclusion of that public comment and any consequential revision, that timeline should be adopted. No further policy work is needed on the aspects of urgent requests currently being consulted-on.

4. Accreditation and Authentication of Requestors (Law Enforcement and Others)

Issue: The RDRS pilot is a lightweight ticketing system that does not include any formal accreditation or identity verification for requestors. Anyone with an account can submit requests, and registrars must manually judge each request's legitimacy. In contrast, the SSAD model envisioned a centralized accreditation authority and a requirement that all requestors be authenticated to some degree. The Board's list of key components for an enhanced system includes "accreditation/authentication for law enforcement authorities" and a phased approach toward federated authorization for other groups. The lack of an authentication mechanism in RDRS has several implications: (1) no automation – because requestors are not pre-vetted, contracted parties cannot auto-approve even obviously lawful requests, which was something contemplated for SSAD in limited cases; (2) concern for contracted parties – without knowing the requester's bona fides, registrars err on the side of caution or delay, especially for urgent cases, as discussed; (3) inefficiencies – requestors (like IPC members) must repeatedly provide evidence of their legitimacy or purpose, which could be streamlined if re-usable accreditation credentials were in place.

IPC Position:

The IPC supports introducing an authentication system for law enforcement as a first step, while also advocating for accreditation of other trusted requestors, such as IP professionals. Accreditation is critical to improving efficiency and trust in disclosure processes, but the IPC recognizes that the SSAD model raised cost concerns. Therefore, IPC favors a lighter-weight approach that starts with law enforcement and IP professionals, avoiding unnecessary complexity while delivering meaningful improvements.

Recommended Path:

The IPC recommends building on existing EPDP Phase 2 policy principles without launching a costly full SSAD implementation. ICANN should develop a streamlined

accreditation framework for law enforcement and expand it to IP professionals in subsequent phases. This can be achieved through implementation guidance and incremental enhancements rather than a new policy process. The goal is a practical, phased solution that balances cost, scalability, and the urgent need for trusted access.

5. Standardization of Request Handling and Transparency of Responses

Issue: Beyond the formal policy gaps identified by the Board, the IPC has observed a serious operational issue during the RDRS pilot: the lack of standardized procedures and feedback for processing requests. Because RDRS is currently just a voluntary framework and there are no specific contract/policy requirements governing *how* registrars evaluate and respond to requests, each provider handles them in their own manner. This has led to inconsistent outcomes and a frustrating experience for requestors. The IPC and its members (some of whom have used RDRS extensively over the past year) have identified patterns such as: some registrars appear to summarily deny most requests with minimal explanation; reasons given for refusal are often vague or boilerplate, making it impossible for the requestor to understand what might be lacking; in some cases, registrars provided a laundry list of alternative methods (e.g. "seek a court order, contact law enforcement, file a UDRP, use other channels") instead of addressing the merits of the RDRS request; other refusals cited things like "the requestor failed to respond to additional information requests" when in fact no such follow-up was ever sent. This Wild West of response quality is a major problem – it undermines confidence in the system and stymies the collection of useful metrics (since denials lack meaningful codes or reasons). It also contradicts some of the principles laid out in the EPDP Phase 2 recommendations for standardized processing.

For example, EPDP Phase 2 Recommendation 8.5 explicitly says that a request should not be denied *"solely because it is founded on alleged intellectual property infringement"* . Yet IPC members have witnessed exactly that happening: requests motivated by trademark or copyright enforcement being rejected out-of-hand with the rationale that the requester should involve law enforcement instead. This indicates a misalignment between community guidance and registrar practice that needs correction.

IPC Position:

The misalignment referred to above must be corrected. Requestors of the registration data must either receive the disclosure of that data or a clear and comprehensible rationale for the refusal to disclose. The Registration Data Policy, which has been fully in force since 21 August 2025, requires nothing less.

Recommended Path:

Although the Registration Data Policy is now fully in-force, this was not the case for the majority of the operation of the RDRS pilot. There is therefore now explicit and

unambiguous policy that requires "a clear explanation of how [the contracted party] arrived at its decision that is sufficient for a requestor to objectively understand the reasons for the decision," where the requested data is not disclosed (s10.6.2 Registration Data Policy). Registrar compliance with this obligation ought to address the lack of adequate and meaningful explanation that so many requestors have experienced to date, and the IPC expects ICANN Compliance to vigorously enforce this.

The current obligations must be enhanced by the Board-adoption of EPDP Phase 2 Recommendation 8.5 (or equivalent policy recommendation, since these recommendations were expressed to be a package).

The Implementation Notes for the Registration Data Policy should also be enhanced.

6. API Integration and System Integration for Efficiency

Issue: The current RDRS web portal, while functional, is a manual, web-based interface that can be cumbersome for high-volume users and for integration into existing workflows. The Board's proposed enhancements (and the RDRS Standing Committee) highlight the addition of Application Programming Interfaces (APIs) for both requestors and registrars as a key improvement. An API would allow automated submission of requests and pulling of responses, enabling organizations to incorporate RDRS into their own case management systems or allowing registrars to integrate with their ticketing systems. The Standing Committee specifically recommended API integration and noted it requires no policy change to implement. The main challenge is operational and resource-based – ICANN org would need to develop and support the API functionality. During the pilot, ICANN org has also explored whether alternative solutions (besides a full API) could ease integration.

From the IPC perspective, the lack of an API is not a "policy gap" per se, but it is a practical limitation that, if addressed, can improve adoption and user satisfaction. For example, larger IPC members (like tech companies or law firms that send many requests) could automate parts of their workflow, reducing the time spent on data entry. Similarly, registrars who handle many requests could see efficiency gains, improved consistency, and fewer errors if they can use an API rather than logging into a web UI for each request.

IPC Position:

The IPC supports the rapid implementation of APIs for RDRS. We agree with the Standing Committee that this does not require new consensus policy – it is within ICANN org's remit to improve the system's technical features. We also believe that a more efficient system benefits all parties: it lowers transaction costs, and encourages participation. The cost concerns raised in the SSAD ODA about a complex system might be mitigated if incremental improvements like APIs are added gradually and targeted to real needs, rather than building a huge system from scratch. The usage data from the first year of RDRS can inform what the API should prioritize.

Recommended Path:

The IPC recommends that ICANN org prioritize API development as part of the RDRS maintenance and evolution, and that the ICANN Board encourage allocation of resources to this end. The Standing Committee found that no further policy work is required for implementation of an API. This means ICANN could proceed on this operational improvement immediately.

7. Optional Participation for ccTLDs.

Issue: The Board's analysis also mentions providing operational options for country-code TLDs (ccTLDs) to voluntarily participate in the RDRS (or its successor). ccTLDs are not bound by ICANN's gTLD policies or contracts, but there has been community interest (including from the GAC) in allowing interested ccTLDs to use the same system for disclosure requests. This could make life easier for requestors who deal with both gTLD and ccTLD registration data issues. However, there are challenges: ccTLDs operate under their national laws and policies which can differ greatly; their data models might not align exactly with the RDRS schema; and many ccTLD operators have expressed caution (as noted by the ccNSO) about joining due to these differences.

IPC Position: The IPC views ccTLD participation in a centralized system as a positive objective. We note that from the requestor's standpoint, a one-stop system is ideal – it would be beneficial if ccTLDs could opt in and appear in the same interface when one files a request. This could potentially broaden the utility of the system for IPC members who often have to pursue bad actors across multiple TLDs.

We also recognize that because ccTLDs are sovereign in policy, this cannot be mandated. It must remain voluntary. Therefore, it's not something the GNSO policy process can directly solve, but the IPC encourages continued dialogue between ICANN and ccTLDs on how to make this work.

Recommended Path:

From a policy comment perspective, the IPC would welcome voluntary expansion of the RDRS to ccTLDs, as it could enhance the overall ecosystem of domain data disclosure. It is, as the Board calls it, an operational option – so our main recommendation is to keep the door open and design the RDRS successor system in a way that a ccTLD *could* plug in with minimal fuss, should they later decide to opt in. This means avoiding any hard-coding of gTLD-only assumptions in the design.