

The ICANN GNSO “Business Constituency”



ICANN Business Constituency (BC) Comment on [Registration Data Request Service \(RDRS\) Standing Committee Report](#) [for GNSO Council Review](#)

29-Sep-2025

Background

This document is the response of the ICANN Business Constituency (BC), from the perspective of business users and registrants, as defined in our Charter. The mission of the BC is to ensure that ICANN policy positions are consistent with the development of an Internet that:

1. Promotes end-user confidence because it is a safe place to conduct business;
2. Is competitive in the supply of registry and registrar and related services; and
3. Is technically stable, secure and reliable.

Comment

The BC appreciates the opportunity to provide feedback on the RDRS Standing Committee (SC) Council Report dated August 19, 2025. This Report provides valuable insights from the RDRS pilot that will be crucial for developing a permanent solution for accessing non-public gTLD registration data.

From the perspective of BC members, we strongly support the overarching goal of an effective and standardized access/disclosure system (SSAD) to combat domain name system abuse and attempts to defraud our members' customers. However, in our view, a "standardized" system does not require a centralized system, and we strongly recommend rethinking the centralized approach embodied in the original SSAD proposal. See (E) below.

The RDRS pilot, while a useful stopgap, identified key areas where the SSAD framework needs to be re-oriented to meet the legitimate needs of businesses that use the DNS to reach their customers.

What BC members learned from the RDRS Pilot:

The Report confirms that businesses who operate domains, primarily categorized as “IP Holders” in RDRS nomenclature, are a significant user group of the RDRS. The data show they were the most frequent requestors, submitting 1,058 requests, representing one-third of all requests. This high volume underscores the critical need for a functional system that allows business domain owners to access registration data to protect their customers.

Other key learnings from the RDRS Pilot:

A. System Limitations and "User Friction." The Report notes that over 60% of RDRS lookups that were eligible to proceed did *not* result in a submitted request. The Report attributes this primarily to "user friction," which includes complicated online forms and a lack of awareness or understanding of the system. This friction disproportionately impacts businesses who are trying to efficiently process multiple requests, often with urgency when phishing attacks are threatening their customers

B. Low Success Rate and Inadequate Rationale for Denials. The overall denial rate for requests is high, with a large number of denials resulting from "incomplete requests" or a need for "more information." As the Report points out, this highlights a need for registrars to provide more detailed rationales for denying a request, beyond simple pick-list options. The current system often requires businesses to submit separate requests outside of RDRS to retrieve the data, creating inefficiencies and reducing user satisfaction with RDRS. To address this, registrars should establish and publicize clear criteria for a successful request.

Denials need to be more than just better explained. Users also need clear and reasonable guidance on how to submit a successful request with a high likelihood of being accepted. The rejection/dropout rate of 60% is an extraordinarily strong signal that the system is not usable. In our view, submissions by experienced requestors should rarely be rejected. While new users face more rejections initially, they should be able to quickly learn the process and become proficient after only a few submissions. A high rejection/dropout rate is a waste of time and resources for everyone involved, from both requestors and data holders.

Registrars should provide useful guidance on how to submit a successful request. One way to accomplish this is for each registrar to publish its own specific instructions for guidance for common request types. Even better, registrars could collaborate to create shared advice for these common cases.

C. Voluntary Participation and Insufficient Coverage. The RDRS pilot does not require registrars to participate, and that remains a significant shortcoming from the perspective of business users of the system. With only 78 participating registrars and roughly 60% gTLD domain coverage, businesses are left without a clear path to data for a large portion of suspect domains. This is especially true for domains used by bad actors for malicious purposes, who often register domains with registrars who are not participating in RDRS. The BC strongly advocates for mandatory participation in a permanent system to ensure consistent and broad coverage.

Recommendations from the BC Perspective:

The BC supports many of the RDRS Standing Committee's recommendations but wishes to emphasize several points from the business user perspective, as protecting business customers is a core function of the Business Constituency.

A. Continue and Enhance RDRS as an Interim Step. We agree with the recommendation to continue the RDRS and see it as a valuable "stopgap" until a permanent SSAD is in place. Further, the notion of a "permanent SSAD" should be understood as providing the desired functionality. This should not be interpreted to mean that ICANN Org must implement and operate a centralized service. See (E) below. However, the continued operation of the service must include key enhancements to improve its utility for businesses.

- Specifically, we endorse the Standing Committee's top-priority enhancements, particularly the implementation of an Application Programming Interface (API) to streamline data exchange for high-volume business users and the UX redesign of the request forms to reduce "user friction" and incomplete submissions. Simpler, more intuitive forms will improve the experience for both requestors and registrars.

B. Address the Privacy/Proxy Provider Challenge: The Report correctly identifies privacy/proxy data as a crucial area for further policy work. The BC reiterates that businesses are often left without an avenue to access data when it is held by a privacy or proxy service. We support the recommendation for policy work that would integrate privacy/proxy providers into the disclosure system to increase efficiency and user satisfaction. This is a critical step for businesses to effectively combat online infringement and DNS abuse.

C. Strengthen Response Requirements for Registrars. The Report's findings on denials are particularly concerning for businesses. We recommend that the SSAD include a requirement for registrars to provide more detailed and specific reasons for denial. This would improve transparency and enable businesses to refine their requests as they learn what is required for a successful submission. We support the recommendation that registrars should conduct a preliminary review and request additional information from the requestor before issuing a

denial. This would reduce the need for business users to submit multiple requests for the same domain name.

D. Require Registrars to provide effective guidance on how to submit successful requests for common use cases. As noted above, registrars should provide useful guidance on how to submit a successful request.

E. Redirect the system design toward a decentralized architecture. ICANN should not be an intermediary for every transaction. ICANN's proper role is to establish policies for the contracted parties and the broader DNS registration community in order to define a system that uses common protocols to provide a service that benefits the entire Internet community. This should be done without the inherent costs and delays of a centralized system. Further, a decentralized design will protect ICANN from being a target of government surveillance.

Conclusion

The RDRS pilot has demonstrated that a system for accessing non-public registration data is feasible and in high demand by businesses who use domain names to interact with the world. The data and lessons learned from the RDRS Standing Committee Report provide the necessary evidence to move forward with a more robust, mandatory, and transparent SSAD. While we acknowledge the importance of balancing privacy and data access, the continued ineffectiveness of the current system in meeting legitimate requests for consumer protection is a significant concern. The BC urges the GNSO Council and ICANN Board to use the RDRS Report to immediately prioritize the development of a permanent solution that is scalable, efficient, and addresses the critical needs of businesses globally.

This comment was drafted by Mary Penn, with help from Steve Crocker and Steve DelBianco. It was approved in accordance with our [Charter](#).