The ICANN GNSO "Business Constituency"

ICANN Business Constituency (BC) Comment on
Registration Data Request Service (RDRS) Policy Alignment Analysis

9-Dec-2025

Background
This document provides input from the ICANN Business Constituency (BC), from the perspective of business users and registrants. We advocate for ICANN policy 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
3. is technically stable, secure and reliable.

General Comment:
Thank you for the opportunity to comment on the ongoing matter of registration data access via the Registration Data Request Service (RDRS). The Business Constituency's (BC) comment follows here.

Overarching comment

The BC's long-held position is that RDRS, while marginally helpful in routing and managing requests for non-public domain name registration data, has not been proven a success, either in the provisioning of data or in satisfying its objective of measuring overall demand for such data.

RDRS shortcomings are significant and well documented. Among them, the system:

- Lacks meaningful registrar and / or registry participation;
- Is not well known outside the immediate ICANN community;
- Does not require timely data disclosure, however such a timeline may be defined;
- Does not require disclosure of the true "underlying" registration data hidden by privacy / proxy services; and
- Has no authentication mechanism for law enforcement agencies (LEAs) or other legitimate requestors.

The RDRS and SSAD before it are based on ICANN running a centralized system on behalf of gTLD contracted parties. The future system should be decentralized and designed for the benefit of the *entire* Internet community, not just contracted parties. The design should accommodate and support a wide variety of policies. One of those policies should, of course, be developed by the GNSO for use by the GNSO community, but the design should not be specialized solely for the GNSO.

Accordingly, the BC advocates for the continuation of RDRS in the anticipation of development of a more robust, balanced system with greater requestor and contracted party participation.

Comment on Policy Alignment Analysis Document

3.1 SSAD Policy Recommendations

The BC generally supports the path forward described in the analysis document. The BC supports addressing the following policy gaps:

- Maintaining RDRS beyond the pilot's two-year term;
- Adding an Application Programming Interface (API) integration for both requestors and registrars to streamline data exchange between users and RDRS;
- Allowing optional participation for ccTLDs using RDAP; and
- Including authentication of specific user groups, beginning with law enforcement.

The BC takes note of the following statement in the analysis document:

> *"The report also notes that optional registrar participation in the RDRS pilot may have contributed to reduced participation by requestors and ensuring broader participation could improve requestor participation and satisfaction."*

The BC agrees and, from our perspective, "may have" can be eliminated to make the statement more accurate. Our experience is that business users of RDRS simply abandoned the system after frustration with low levels of registrar participation and inconsistent disclosures.

3.2 Disclosure of Privacy/Proxy Customer Data

As stated, the BC strongly believes that the "underlying" registered name holder data should be disclosed for legitimate requests. The BC accordingly supports further *efficient* policy work necessary to establish streamlined disclosure processes.

The BC further advocates for the following as ways to improve disclosure decisions and associated actions:

- Updating references to proxy services to "known proxy services." Doing so would include proxy services affiliated with registrars and may also include others.
- Add a data element to the domain name registration process that designates the registrant as a natural person, legal person, known proxy provider, or "unknown." This will help registrars during balancing tests.
- For privacy services, add a new role titled "Correspondent" and include contact details for the privacy service in this field. Registrant details can be included but kept private.

3.3 Response Timeline for Urgent Requests

The BC supports further policy development in this area. Recognizing that community opinions are diverse as to what constitutes an appropriate response timeline, the BC strongly urges adoption of

comparatively short timeframes to meet the needs of law enforcement, anti-abuse authorities and others in a position to assist with pressing disclosure needs.

The GAC has not yet provided data supporting the need for a separate mechanism and process for urgent requests and, further, has not defined "urgent" in this context. In fact, the currently employed definition of "urgent request" focuses on *importance* but is silent on *urgency*. This makes it very difficult to design and implement a meaningful system to support urgent requests without a definitive timeline.

We recommend consulting the GAC to document the need for expedited handling of these requests and to specify what sort of response time is actually needed (e.g. one minute, five minutes, an hour, etc.). If work on urgent requests continues, it should also include specialized pathways for law enforcement personnel to initiate such requests. At present, the clock on the registrar's response time doesn't start until they receive the request, and there is currently no pathway specified or planned that delivers an urgent request to a registrar other than the ordinary channels such as email. The absence of such a pathway is inconsistent with the idea that such requests are urgent.

3.4 Other Identified Issues

The BC supports, as articulated in the analysis document, (1) a request for registration data for one IDN variant domain name in a set means the requestor receives the data for all names in the set; (2) a requestor is able to know what names are in the IDN variant set. Such efficiencies will contribute to the ability to rapidly mitigate DNS abuse and other harms.

This comment was drafted by Mason Cole, Steve Crocker and Steve DelBianco. It was approved in accordance with our Charter.