ICANN | RrSG
Registrar Stakeholder Group

RrSG Input: RDRS System Enhancement for Law Enforcement Requests

27 February 2026

The Registrar Stakeholder Group ("RrSG") offers the following input on the topic of RDRS System Enhancement for Law Enforcement Requests, with the understanding that this request was sent directly to participating registrars, as this is a topic of significant importance and concern to ICANN-accredited registrars. Registrars who do not participate in the RDRS pilot project must still respond to disclosure requests from Law Enforcement Agencies, and their experience has resulted in pragmatic and valuable feedback. This input is especially important because this proposed LEA Authentication process is being considered in the context of not only the RDRS but also the disposition of the SSAD Recommendations and the Registration Data Policy implementation of the Urgent Requests process. This input has been collected from Registrar Stakeholder Group members and is submitted on the group's behalf.

The Registrar Stakeholder Group is the representative body of ICANN-accredited domain name registrars. Operating with numerous subgroups focused on specific topics of interest, the RrSG contributes to policy development, issue advocacy, and negotiations with ICANN. We work to advance the interests of registrars and our customers by promoting data-driven policy outcomes. Learn more about the RrSG on our website rrsg.org.

At a high level, **providing data indicating that the Law Enforcement user's email domain is the correct email domain would provide some value to registrars in reviewing requests. That value is rather limited** and so the Registrar Stakeholder Group cannot offer input as to whether it is sufficient to justify the cost of implementation. We note specifically input from our Public Comment on the Registration Data Request Service (RDRS) Policy Alignment Analysis:

> [T]he process should be managed and funded by the group itself (not by ICANN). We note that no other groups should be able to submit Urgent Requests as only Law Enforcement can meet the definition of Urgent Requests.

LEA User Authentication is a useful component

The RrSG supports the Registration Data Request Service Standing Committee Council Report statement (page 32) that "*the onerous part of data disclosure is generally not authentication but rather balancing the requestors' documented proof of purpose/need versus the registrant's right to privacy,*" and refers to our Public Comment in which we noted that authentication is "useful but not an essential or mandatory component of a future system."

The RDRS pilot period demonstrated that requestors are willing to falsely identify themselves as representing Law Enforcement, presumably in order to be able to submit an RDRS request in the "Law Enforcement" category. This remains a source of concern and

dismay to registrars**. If the LEA request category can only be selected by Authenticated LEA users then this LEA Authentication process would provide value by reducing this misuse of the RDRS and enabling registrars to easily find and potentially prioritise requests that do actually come from Law Enforcement Agencies.**

LEA User Authentication is one piece of the puzzle

LEA User Authentication as envisioned in this context would provide confirmation to the registrar that the email domain used by the RDRS requestor was *at one time* confirmed to be used by a given Law Enforcement Agency in a specified country. Later in this comment we address security concerns relating to the ongoing user management process.

Authentication will not result in automatically-approved disclosure requests; the balancing test must still be conducted after authentication is completed and the responding registrar confirms that the requesting Law Enforcement user has legal authority in the situation, such as originating in the correct jurisdiction.

We note that individuals supporting a Law Enforcement Agency may be issued email addresses at the Agency's domain without having authority to conduct this type of investigation or training in data management and protection. As such, **confirming that the email comes from the correct domain is not sufficient to confirm that the request should be granted.**

Responsibility for decisions remains with the registrar

There is recognition that the authentication may be flawed or outdated; as such, **the registrar must still make a determination as to whether the requestor is indeed a Law Enforcement representative.** This results in liability remaining with the registrar, reducing the value offered through this Authentication process. In addition, **even after the authentication is confirmed the registrar must consider the requestor's jurisdiction and the other elements of the request when determining how to respond.**

Security and privacy considerations remain

Processes and requirements relating to privacy, security, and data protection remain unknown and should be further considered in collaboration with both the requestor and registrar communities.

The Registrar Stakeholder Group is aware that .gov and similar domains have in recent years been compromised, reducing certainty that a user with an email address at a government-controlled domain truly does represent that government's Law Enforcement Agency.

Noting that legitimate Law Enforcement contacts may use free or public mail services in their communication with registrars, the implications of this process on a 'domain-only' verification list may necessitate that these free or public email services cannot be accepted in this context; otherwise, we may find that a service such as gmail.com is authorized as the email

domain for a given Law Enforcement Agency and then requests from other users are improperly tracked as authenticated LEA requests.

The question of **responsibility for maintaining the list of Law Enforcement Agency domains and accountability in case of error or omission remains open**. **There must be a user revocation process for LEA representatives whose responsibilities change or who depart their Agency, and there must be a regular review process to ensure that existing authentications remain valid over time.** This gap in managing user access may be addressed as part of the process underway with the Governmental Advisory Committee's (GAC) Public Safety Working Group (PSWG) Law Enforcement Agency (LEA) Authentication Practitioner's Group but, as this seems to be an ad-hoc group with little external communication, the Registrar Stakeholder Group remains unaware of plans or decisions in this regard.

This is even more complex in a case where a Law Enforcement Agency not included in the lists provided by the FBI, EUROPOL, or INTERPOL submit their own email domain to ICANN for inclusion in this process, as this removes a layer of oversight from that submission and raises questions about how those submissions are verified.

While the liability for relying on this Authentication process remains with the registrar, so does the significant responsibility of ensuring that disclosure decisions are grounded in accurate and reliable information.

The RrSG hopes that this input is useful to the RDRS Standing Committee and Governmental Advisory Committee's (GAC) Public Safety Working Group (PSWG) Law Enforcement Agency (LEA) Authentication Practitioner's Group, and looks forward to ICANN publishing a report documenting the input from all respondents.

Thank you,

Owen Smigelski

Registrar Stakeholder Group Chair