Tucows public comment: Timeline for Urgent Requests for Lawful Disclosure of Nonpublic Registration Data

15 December 2025

Tucows welcomes the opportunity to comment on the Timeline for Urgent Requests for Lawful Disclosure of Nonpublic Registration Data ("Urgent Requests Timeline") and appreciates the work of the EPDP Phase 1 Implementation Review Team and ICANN Org Implementation Project Team in drafting this addition to the Registration Data Policy.

While the definition of "Urgent Requests" comes close to appropriately defining the circumstances in which this compressed timeline can be required, we note several areas of concern with this proposed policy language:

- Necessary guardrails are not in place for the definition of Urgent or the limitations on who can make an Urgent request
- The process for handling these requests has not been fully considered,
- The EPDP Phase 1 Recommendation has not been faithfully implemented.

Tucows notes with support the comments submitted by the Registrar Stakeholder Group ("RrSG") and by Namespace Holdings.

Definitions and Interpretation

Definition of "Urgent Requests"

Tucows generally supports definition's list of circumstances under which this Urgent Requests process can be invoked, with two concerns.

First, **"critical infrastructure" is not a well-defined term and may lead to confusion and ambiguity in request processing.** The European Union recently published clarification on how to identify critical entities across eleven sectors; in Canada, ten sectors are identified as critical while the United States has sixteen. This discrepancy could easily result in a requestor considering a request to be Urgent while the responding registrar does not; how would ICANN Compliance address a complaint about not meeting the Urgent timeline?

Second, **the Urgent Request process must only be available to requestors in the responding registrar's local jurisdiction**. ICANN Consensus Policy cannot be used by law enforcement to extend their reach extraterritorially. If a member of law enforcement identifies an issue of this nature in another jurisdiction they would, as a matter of course, need to work with local law enforcement to address it, following established processes (including MLAT). ICANN should not presume to insert itself into internationally-negotiated treaties; if the current mechanisms are lacking, ICANN is not the appropriate venue to resolve those issues. We expect that law enforcement follow standard processes, whether within their own jurisdiction or outside of it

As such, Tucows proposes the following modified definition (**bold** is new, ~~strikethrough~~ is to be removed):

> "Urgent Requests for Lawful Disclosure" ("Urgent Requests") are a subset of Disclosure Requests submitted by an Authenticated Requestor **which is a member of local law enforcement** that are limited to circumstances that pose an imminent threat to life, of serious bodily injury, ~~to critical infrastructure,~~ or of child exploitation in cases where disclosure of the data is necessary in combatting or addressing this threat. ~~Critical infrastructure means the physical and cyber systems that are vital in that their incapacity or destruction would have a debilitating impact on economic security or public safety.~~

Definition of "Authenticated Requestor"

Tucows supports the definition of Authenticated Requestor presented in the Timeline.

Policy work is necessary for the authentication mechanism

Tucows agrees with the statement in the definition that an authentication mechanism must be "implemented pursuant to ICANN Consensus Policy."

Registrar requirements are documented and formalized in the Registrar Accreditation Agreement and Consensus Policy; if a process is not governed by one or the other then it cannot be mandatory and enforceable by ICANN Contractual Compliance. As such, **using an authentication mechanism, either as a member of law enforcement who is being authenticated or as a registrar confirming the identity and affiliation of the requestor, can only be a mandatory requirement if Policy or the contract determines that to be the case**.

The absence of policy governing how this authentication mechanism would work results in unclear or incomplete requirements; in an effort to support better consideration of this

topic, we have attempted to list out at least some of the questions which should be addressed through the policy development process:

- Who pays for the system?
- Who operates the system?
- Who provides hosting services? Where is the data hosted and how are cross-border data transfers handled?
- Who provides support to users?
- Who makes sure users are added and removed when required?
- Who has access to view and manage users?
- Does the system track data on how the authentication is used in relation to disclosure requests? Who has access to that data?
- Who handles disputes and issues of incorrect authentication?
- What security measures are in place (both technical and organizational)?
- How long is the data retained?
- What public reporting is done? What private reporting is done, and to whom?
- When will a Human Rights Impact Assessment and a Data Protection Impact Assessment be conducted?
- Who audits the system operator to ensure adherence to requirements?
- What happens if the system operator does not adhere to requirements?

Decisions on these and related areas must be taken via the multistakeholder policy development process. Under the multistakeholder process, the creation and mandated use of an authentication mechanism cannot be simply directed by an Implementation Review Team that has no related Policy Recommendations on which to base decisions. Tucows is shocked by the implication that it could.

Disclosure Requests

Tucows does not support the proposed 24-hour timeline for response to Urgent requests. It does not properly implement the Working Group's recommendation, poses an unreasonable burden on registrars, and has not been demonstrated to be necessary or to address a real problem.

Insufficient time for a well-considered review

The EPDP Phase 1 team recommended a timeline measured in business days; the IRT was directed to implement a timeline measured in hours. These situations certainly warrant a response provided without undue delay but the initial Recommendation recognized that registrars need time to properly assess the request and make a balanced determination.

Registrars need time to confirm the authentication of the requestor, engage external legal counsel if needed, determine whether the situation qualifies as "Urgent", and, finally, decide whether data can legally be disclosed to that requestor. This can happen within 24 hours but setting an artificially constrained deadline for such a complex operation devalues the necessary balancing of rights that a registrar must still undertake, potentially putting due process at risk.

Due process is the law.

We want to help law enforcement in their investigations but we—and they—must do so within the bounds of the law and with full respect for due process. A required 24-hour turnaround time could potentially put our business at risk if we insist upon due process for our customers and their personal data—as is our right under the law.

If an investigation cannot accommodate a delay of a few hours for the matter to be legally reviewed, then **law enforcement still has the option to get a warrant (or subpoena) for the data. Alternatively, the requestor could expedite the process even further by asserting that the situation is "exigent" and require that the data be disclosed before they go through the process of getting a warrant.**

This important legal protection, including review of the evidence by a judge or magistrate, ensures that law enforcement is conducting a legitimate, well-founded investigation that remains within the bounds of the law.

Obviously, when we receive due process or notice of exigency, we comply with our legal obligations—and that is not a matter for ICANN Policy to opine on.

What data is LEA looking for?

As we wrote in a recent blog post, the overwhelming majority of requests marked as "urgent" or to be expedited do not fall into the relevant circumstances.

Further, when a request does relate to an urgent situation typically the requestor needs hosting data, an IP address, or other details that the registrar does not have, rather than the domain name registration data.

Finally, when such an urgent situation arises, the law enforcement officer is unlikely to pursue ICANN processes but rather go directly to the provider in whatever way they can—typically via phone.

Exceptions should not be so limited

ICANN Policy should not dictate what is and is not exceptional or extenuating circumstances in a legal context.

If a short timeframe is set for required responses to Urgent requests, exceptions will need to be made, either to confirm the validity of the requestor and request or even because of typical business constraints. The extension periods laid out in this Timeline are prohibitively restrictive.

The Timeline should not include limits on what can be considered sufficient for an extension, as this goes toward the Contracted Party's evaluation of the request, which ICANN has regularly agreed must remain solely with them.

In addition, the restrictions could place compliance with policy and compliance with law at odds; our contracts confirm that we need not ever violate law to comply with Policy but we should not be put into a position where we have to prove the conflict to ICANN Contractual Compliance.

Responses to ICANN Questions

1. **Does the draft language proposed for inclusion in Sections 3.8, 3.9, 10.7, and Implementation Note K of the Registration Data Policy clearly describe the applicable requirements?**

Yes

2. **If you believe that the draft language proposed does not clearly describe the applicable requirements, what areas require additional clarification?**

n/a

3. **Does the proposed Urgent Request timeline align with the requirements in EPDP Phase 1 Rec 18, and the expectations provided by the Board, GAC and GNSO Council?**

No.

The proposed Urgent Requests timeline does not align with the requirements set in the EPDP Phase 1 Recommendation 18 in relation to Urgent requests, which is:

A separate timeline of [less than X business days] will considered *[sic]* for the response to 'Urgent' Reasonable Disclosure Requests, those Requests for which evidence is supplied to show an immediate need for disclosure [time frame to be finalized and criteria set for Urgent requests during implementation].

The proposed draft should be recalled and either work should resume to come to an implementation which does meet the Policy recommendation or the ICANN Implementation Project Team (IPT) and Implementation Review Team (IRT) should confirm that they have fulfilled the actual requirement which was to *consider* a separate timeline for Urgent requests. **Any participant in or observer of the ICANN policy process over recent years must agree that this timeline has been very thoroughly considered.**

Expectations of the Board, GAC, and GNSO are not relevant in this context, other than that these expectations should align with the PDP Working Group's Recommendations; a Working Group in which the GAC and GNSO participated.

4. **The IRT has discussed the proposed Section 10.7 and some IRT members believe the authentication mechanism (when available) would require additional policy work, while others believe the authentication mechanism is part of the implementation of Rec 18 and would not require additional policy work. Do you believe this requires additional policy work?**
    1. **If you believe this requires additional policy work, please explain.**
    2. **If you do not believe this requires additional policy work, please explain.**

Yes, this requires additional policy work.

We refer the reader to our comments above and encourage thorough consideration of the questions posed.

Tucows again thanks the ICANN Org IPT and the Implementation Review Team for their work on this important final piece of implementing the Phase 1 EPDP.

Thank you,

Sarah Wyld
Head, Policy & Privacy, Tucows