Timeline for Urgent Requests for Lawful Disclosure of Nonpublic Registration Data

NCSG Comments

December 15th, 2025 *(deadline)*

About NCSG

NCSG represents the interests of non-commercial domain name registrants and end-users in formulating the Domain Name System policy within the Generic Names Supporting Organisation (GNSO). We are proud to have individual and organizational members in over 160 countries, and as a network of academics, Internet end-users, and civil society actors, etc., we represent a broad cross-section of the global Internet community. Since our predecessor's inception in 1999, we have facilitated global academic and civil society engagement in support of ICANN's mission, stimulating an informed citizenry and building their understanding of relevant DNS policy issues.

About this Public Comment Proceeding (Background)

https://www.icann.org/en/public-comment/proceeding/timeline-for-urgent-requests-for-lawful-disclosure-of-nonpublic-registration-data-22-10-2025

The Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data (EPDP) Phase 1 Recommendation 18 (Rec 18) anticipated **"a separate timeline for** responses to **urgent requests for lawful disclosure of non-public registration data"** and indicated that the response time and criteria would be established during implementation. The relevant section reads that a:

> ***separate timeline of [less than X business days]*** *will be considered 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].*

Currently, no such timeline exists in the Registration Data Policy, which went into effect on 21 August 2025. As part of Rec 18's further review, in its 3 June 2024

correspondence, the Board identified the concern that urgent requests would more appropriately be responded to within minutes or hours rather than the previously proposed business days, specifically:

To the extent that law enforcement needs registration data to respond to situations that pose an imminent threat to life, serious bodily harm, infrastructure, or child exploitation, the ***proposed timeline - whether one, two, or three business days - does not appear to be fit for purpose. To respond to truly imminent threats, a much shorter response timeline, i.e., minutes or hours rather than days, would seem to be more appropriate****.*

The GAC and GNSO Council also acknowledged that the use of business days may not be appropriate to respond to Urgent Requests for the disclosure of data.

To address the Board's concern that the use of business days is not fit for purpose to address truly imminent threats and the lack of an authoritative, legally sufficient cross-border system to validate law enforcement entities, on 15 October 2024 the GAC proposed two separate parallel tracks:

1. An authentication path where the GAC Public Safety Working Group (PSWG), in collaboration with contracted parties, would explore possible ways forward on an authentication solution.
2. "Discussions about an appropriate response time for Urgent Requests should be based on an assumption that urgent requests received by registrars have been authenticated"

Subsequently, the GNSO Council, GAC, and ICANN Board held two trilateral calls. During its 19 December 2024 meeting, the GNSO Council considered the IRT's previous discussions regarding the separate timeline for urgent requests and noted the IRT could not agree to a timeline, in part, because of the lack of a global authentication mechanism.

In response to the GAC's proposal, the GNSO Council assumed work on the additional timeline discussions would occur within the existing IRT. Specifically noting "To be clear, this would not constitute policy development as defined in Annex A of Bylaws (the GNSO PDP) but rather, would be continued implementation work on Recommendation 18 of the EPDP Phase 1 Final Report"

In light of the GAC's two-track proposal to develop such a mechanism, and resume timeline discussions within the EPDP-Temp Spec IRT, the Board, GNSO Council, and GAC reached an agreement during their second trilateral meeting on 12 February 2025 that implementation work should resume on Rec 18, specifically related to identifying an appropriate timeline within which registry operators and registrars should be required to respond to urgent requests for lawful disclosure. On 27 March 2025, the GNSO Council further acknowledged and agreed with the GAC's suggestion that the discussion regarding the response time for urgent requests should continue within the EPDP-Temp

Spec IRT, and subsequently encouraged that ICANN org resume IRT meetings in the near term.

To date, ICANN org has held six sessions with the EPDP-Temp Spec IRT, where the IRT members shared concerns and feedback related to the Urgent Request requirement and proposed language. Throughout these sessions, various perspectives were shared, and the language proposed for Public Comment reflects a synthesis of all the inputs and concerns that were considered.

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

I. Submission

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?**

The criteria for urgent requests should not be open-ended. For critical infrastructure, it should be clear what "public safety" and "economic security" mean and the definition should rely on a standard that registries and registrars can use.[1]As drafted, these terms are broad and risk inconsistent interpretation by contracted parties. To ensure predictability and uniform application, the definitions should be anchored in established, internationally recognized standards. We recommend referencing narrow standards with

[1] At the moment, "critical infrastructure" has been defined as " 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" (Section 3.8, ICANN org Proposed Timeline for Urgent Requests for Lawful Disclosure of Nonpublic Registration Data, v. 22 October 2025).

examples to draw up a globally unified definition for these terms in a way that registries and registrars can consistently apply. Another important factor that should be considered is that “public safety” is a vague term that can be abused to have urgent access to people’s sensitive data in order to quash uprising and peaceful protests. Therefore the term “public safety” should be narrowed down and be combined with examples and it should be acknowledged that even for urgent requests, especially when it comes to “public safety” registrars must do the fundamental rights balancing and not be punished because as result of fundamental rights balancing they did not disclose the domain name registrant private sensitive data.

As Maciek Piasecki mentions in their public comment:

“Nevertheless, it is generally accepted that bridges, airports and energy infrastructure are considered critical infrastructure. These are often used by legal protests (with an emphasis on anti fossil fuel movements) across Europe and elsewhere. It is unclear from the language of the proposal whether using paint or non-violently stalling the functioning of such infrastructure can be considered "immediate harm’. Thus governments can abuse LEAs by pressuring them into intimidating the organisers, even by an ambiguous visit by the LEOs, not to mention employing the methods stated in the paragraph above. It must be noted here that complaints after the arrests of protesters during the 2020 demonstration in Warsaw have been deemed valid in 343 of 597 of cases. The police had made efforts have been taken to thwart many of the demonstrations before they started. This included surveillance of activists and opposition politicians, including via digital means..”[2]

The draft language in Section 3.8 does not clearly convey the time-sensitivity that justifies hour-based response timelines. The phrase "where disclosure of the data is necessary" should be strengthened to "where expedited disclosure of the data is necessary" to emphasize that standard timelines are inadequate.

[2] Link to examples as provided by Maciej:
https://bip.brpo.gov.pl/pl/content/rpo-demonstranci-zatrzymania-policja-sady-zazalenia#:~:text=Zatrzymania%20manifestant%C3%B3w%20w%202020%20r.&text=za%C5%BCale%C5%84%20na%20zatrzymania%20uczestnik%C3%B3w%20protest%C3%B3w,S%C4%85du%20Rejonowego%20dla%20Warszawy%2D%C5%9Ar%C3%B3dmie%C5%9Bcia.

https://oko.press/lata-na-niego-i-caly-czas-non-stop-czyli-oblawa-na-obywateli-ujawniamy-nagrania-z-policyjnych-radiostacji

Additionally, the critical infrastructure provision should be separated from the other urgent circumstances for clarity. we recommend revising Section 3.8 as follows:

"Urgent Requests for Lawful Disclosure" ("Urgent Requests") are a subset of Disclosure Requests submitted by an Authenticated Requestor that are limited to circumstances that pose an imminent threat to life, of serious bodily injury, or of child exploitation in cases where expedited disclosure of the data is necessary in combatting or addressing this threat.

Urgent Requests also apply where there is an imminent threat to critical infrastructure and expedited disclosure 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.

This restructuring clarifies that all urgent requests must meet an expedited necessity standard. This is one of the reasons that we believe there should be a separate policy development track for clarifying the basis of urgent request, the timeline and the authentication process.

The concept of a “trusted/competent authority” in 3.9 is extremely open-ended. Without policy criteria, this may extend far beyond narrowly defined law enforcement and risks expanding the category of actors who can activate the urgent-request track in unpredictable ways. We recommend explicitly limiting this category to governmental or intergovernmental law enforcement entities, or establishing clear eligibility criteria to reduce the risk of inconsistent application. Specifically, private or parastatal actors without lay/regulatory enforcement or administrative or judicial investigative powers may be excluded.

While rapid response is critical in genuine urgent cases, the policy should explicitly reinforce that expedited disclosure does not circumvent evaluation of data subject rights, legal compliance, or proportionality. In this regard, to avoid any misinterpretation, we recommend that Section 10.7 explicitly restate that the urgent timeline modifies response times only; it does not relax or reverse the duty to carry out a balancing test, assess the legal basis for disclosure, or respect the data-subject’s fundamental rights under Section 10.4 and applicable law.

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

What is not clear in the policy text (even if it is explained in the rationale paper) is that: “Respond” does not necessarily mean “disclose data”; it can mean denial or a request for further information. Registrars and registries must still perform a balancing test and human-rights/data-protection assessment under Section 10.4; the urgent timeline does not create a presumption of disclosure.

It is recommended that the policy explicitly states that, when contracted parties respond to an Urgent Request -disclosing or denying- they must base their decision on all relevant facts and applicable law as well as human rights standards, including the Registration Data Policy, the applicable Registry Agreement or Registrar Accreditation Agreement, and local data-protection, criminal-procedure and other relevant laws and standards that help with balancing human rights. In the case of a denial (in whole or in part), the standard for the written rationale should be higher: the contracted party should be required to expressly identify the applicable legal, human rights standards and contractual grounds for refusing disclosure and explain how these have been applied to the facts of the case. Finally, the policy should require that every response to an Urgent Request (including disclosure, partial disclosure, denials, requests for clarification, and the use of extensions) be notified to ICANN through an agreed reporting mechanism, so that ICANN and the community can monitor the functioning, proportionality and consistency of the urgent-request regime. They should also be included in RDRS and future triage systems transparency reports including which law enforcement agencies or others submitted the request, where they were based and the result.

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?

The community based on external studies, industry best practices and other factors should come up with a timeline that also considers the different business models that registrars have. As well as the impact on the victims, it should also very carefully consider the impact on domain name registrants and Internet users and their access to online services that could be hampered as a result of such disclosures. Different scenarios has to be considered: does the short timeline apply only under circumstances that there is no other alternative to mitigate the harm but by accessing the domain name registrant data? Is it possible to gather the data in other legal ways?

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?**

Yes. A dedicated Policy Development Process (PDP) is necessary to establish a lawful, enforceable, and rights-respecting authentication framework for urgent requests, because authentication is not merely an operational detail of implementation but a mechanism that directly affects disclosure obligations, fundamental rights, and contractual enforceability. At present, ICANN lacks a consensus policy that obligates registrars and registries to recognize authenticated requestors, respond on accelerated timelines, or participate in a shared accreditation system; without such a policy basis, any authentication scheme remains voluntary, unevenly adopted, and legally fragile. A PDP is required to anchor authentication requirements in binding contractual obligations under the Registrar Accreditation Agreement and Registry Agreements, ensuring uniform application across jurisdictions and business models. Equally important, policy development is the only appropriate venue to define accountability and transparency safeguards, including eligibility criteria for requestors, processes for adding and removing accredited authorities, auditability, and mandatory reporting. Without policy-level requirements for transparency—such as disaggregated reporting on who submits urgent requests, from where, under what legal basis, and with what outcome—the urgent-request regime risks operating as a black box, undermining trust, enabling abuse, and exposing contracted parties to legal and human-rights liability. A PDP would therefore not only provide the contractual foundation necessary for effectiveness, but also embed accountability and transparency measures that are essential to protect data subjects' rights and preserve the legitimacy of expedited disclosure mechanisms.

3. **If you believe this requires additional policy work, please explain.**

Yes. It needs further policy. As stated in the board letter (it's not just a matter of jurisdiction but the rights and freedom of data subjects):

"At the same time, applicable law, regulation, and reasonable registrar policies will often require registrars to authenticate self-identified emergency responders and confirm the purpose(s) for which registrant data is sought prior to disclosing personal data. Even where not required by law or regulation, authentication will often be appropriate under globally accepted principles of fair information processing to protect the rights and freedoms of data subjects."

And because with policy we can bring more transparency and accountability to the authentication process or at least help with enhancing transparency in the future SSAD.

In our view, the proposed approach cannot be implemented effectively without establishing a dedicated policy framework for requestor accreditation. At present, ICANN has **no binding policy or contract** that obligates registrars or registry operators to respond to an “authenticated urgent request,” nor any policy that compels contracted parties to recognize or participate in a centralized accreditation system. Without such a policy foundation, ICANN would lack the contractual enforceability needed to ensure uniform adoption or compliance across all registrars and registries.

As a result, the urgent-requesturgent-request timeline becomes effectively optional and this undermines the core objective of the proposal altogether. Relying solely on implementation guidance to fill this gap would not create binding obligations, and as a result, uptake of the mechanism could be inconsistent, unpredictable, and potentially at odds with the intended safeguards and urgency standards.

A dedicated Policy Development Process (PDP) is necessary to establish a lawful, enforceable, and rights-respecting authentication framework for urgent requests, because authentication is not merely an operational detail of implementation but a mechanism that directly affects disclosure obligations, fundamental rights, and contractual enforceability. At present, ICANN lacks a consensus policy that obligates registrars and registries to recognize authenticated requestors, respond on accelerated timelines, or participate in a shared accreditation system; without such a policy basis, any authentication scheme remains voluntary, unevenly adopted, and legally fragile. A PDP is required to anchor authentication requirements in binding contractual obligations under the Registrar Accreditation Agreement and Registry Agreements, ensuring uniform application across jurisdictions and business models. Equally important, policy development is the only appropriate venue to define accountability and transparency safeguards, including eligibility criteria for requestors, processes for adding and removing accredited authorities, auditability, and mandatory reporting. Without policy-level requirements for transparency—such as disaggregated reporting on who submits urgent requests, from where, under what legal basis, and with what outcome—the urgent-request regime risks operating as a black box, undermining trust, enabling abuse, and exposing contracted parties to legal and human-rights liability. A PDP would therefore not only provide the contractual foundation necessary for effectiveness, but also embed accountability and transparency measures that are essential to protect data subjects’ rights and preserve the legitimacy of expedited disclosure mechanisms.

4. **If you do not believe this requires additional policy work, please explain.**

II. Summary of Submission

Qwery qwerty

III. Summary of Attachment (optional)

[To summarize the PDF file that will be submitted, if any description different than the Summary of Submission is needed - if there are appendices, for example]