Namecheap, Inc., Public Comment: Timeline for Urgent Requests for Lawful Disclosure of Nonpublic Registration Data.

Namecheap, Inc. appreciates the opportunity to comment on the Timeline for Urgent Requests for Lawful Disclosure of Nonpublic Registration Data. In addition to the comment below, Namecheap supports the comment submitted by the Registrar Stakeholder Group (RrSG).

Namecheap operates in several jurisdictions, and we support targeted, lawful access to registration data to address genuine emergencies. Furthermore, Namecheap already has processes in place to do just that, and we are not aware of any instances when valid urgent requests for data disclosure from proper authorities were not timely addressed. Our comment below highlights some of our reservations and concerns with the Urgent Request disclosure requirements as currently drafted.

Namecheap would like to preface this comment by emphasizing that we believe every valid urgent request for data from authorized requestors (e.g. local law enforcement) should be actioned as promptly as possible. When there is risk to human life, every second counts, and the feedback in this comment should not be interpreted as even remotely against responding timely to valid urgent requests. The main concern is that although such urgent requests do happen, based on Namecheap's decades of experience, partnering with law enforcement within the US and in other jurisdictions, and feedback from law enforcement in ICANN forums, urgent requests happen at most once every few years in the registrar ecosystem. When those urgent requests do happen, the requests are acted upon timely and promptly. **Namecheap is not aware of a single urgent request not being actioned timely or resulting in serious injury or death due to such a delay**. While it is important that such requests are addressed, Namecheap believes that existing laws and regulations already properly provide for non-ICANN methods of addressing urgent requests, and registrars still need to comply with these existing laws under the Registrar Accreditation Agreement (RAA). An ICANN policy would be a complicated overlay that yields no better results and is actually likely to frustrate tried and true working methods.

The amount of collective effort within the community to address something that might potentially be a remotely distant possibility rather than addressing actual existing online harms and problems is indicative of a disconnect between those involved in developing policy and those who actually work in the roles that this policy will impact. **If there are urgent requests that are not being timely addressed then the ICANN community**

should work to resolve and prevent this issue from reoccurring, but absent such evidence, this is a hypothetical exercise that will create significant work and effort for all registrars to likely not actually solve anything. The cost to registrars (and thus registrants) will be significant, and although large registrars like Namecheap are better equipped to comply with these obligations, the proposed policy wording will be onerous and potentially cost-prohibitive for smaller registrars and especially those in underserved regions.

According to Namecheap's legal team, over the past eleven years, there has been only **one** legitimate urgent request from law enforcement requesting underlying registrant data (and the request was many years ago). It involved a potential bomb threat, and through existing legal requirements and processes, Namecheap collaborated with law enforcement and provided the requested data within several hours of the request. Over this time period, Namecheap was one of the largest registrars in the world and now has over 21 million domains under management. **To summarize, over more than a decade, covering tens of millions of domains under management, Namecheap is aware of only one urgent registration data request and it was timely addressed through existing non-ICANN structures**.

As part of Namecheap's participation in the RDRS, we tracked all RDRS requests including those self-identified as "expedited". As of 15 December 2025, Namecheap received 1,042 RDRS requests. Of these, 63 (or 6% of the total) were submitted as "expedited". Upon review, only one potentially expedited request was received: for an alleged ransomware attack with a 24-hour deadline. This single request represents 0.1% of all RDRS requests received by Namecheap, and might not meet the definition of urgent as anticipated in this policy work. The other 99.9% of requests received by Namecheap through the RDRS did not involve risk to human life, other highly dangerous or illegal activity, or any facts justifying immediate processing. Claimed reasons for expedited processing included:

- Data requests for UDRP filings (the majority of "expedited" requests)
- Underlying data for the requestor's domain
- Copyright infringement
- Part of a take-home exam for a job as a security consultant
- Previous registrant of the domain name
- Claimed to be a co-creator of Bitcoin
- Desire to purchase the domain name
- Domain is being used for phishing or malware
- Technical support for a website operating on the domain (not hosted by Namecheap)

Our concern is that urgent requests must only be limited to authenticated local law enforcement, and that what is considered urgent should not be expanded now or in the future. As more items and categories of requests start being considered “urgent”, then nothing is urgent because of the increase in volume. There should be strict limits, controls, and penalties for improper requests classified as urgent to ensure registrars can focus only on those requests that are truly urgent.

Thank you for your consideration of this feedback.

Sincerely,

Owen Smigelski
Head of ICANN Compliance and Relations
Namecheap, Inc.

Responses to ICANN Org questions

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, the draft language clearly describes the applicable requirements.

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?

Namecheap believes that the proposed Urgent Request timeline does not align with the requirements in EPDP Phase 1 Rec 18. The recommendation in the final report explicitly referenced *business* days, but the proposed language appears to ignore that recommendation in favor of defining the timeline in hours.

Namecheap strongly believes that the working group’s recommendations should be followed; our registrar also supports the RrSG’s position to adhere to the original

recommendations, but unfortunately, it was decided to change the recommendation after consensus was reached in July 2023 and against unified registrar opposition. We take exception with that development and with ICANN's request to comment on the degree of alignment with expectations of specific stakeholders while ignoring the input of the RrSG. The voice of registrars- the ones that will actually have to implement this policy- was completely ignored.

Finally, the IRT's job is not to make policy, but to implement recommendations made during the policy development phase.

The Board: When the Board approved Rec 18, it approved it as written and recommended by the working group. From that one fact, we can infer that the proposed draft language does not align with the Board's expectations.

The GAC: We are again puzzled as to why ICANN org is asking the community to comment on the GAC's expectations. GAC members participated in the EPDP Phase 1 discussions and had the chance to express their concerns. ICANN policies are made through a multistakeholder process, and as a result, we have a policy that is hopefully balanced and reflects the participation of all stakeholders. The GAC is just one of those stakeholders, and we value their opinion; however, registrars are the most affected by the shortened response timeline and the burden it places on smaller registrars and registrars from underserved regions.

GNSO Council - It should be in the interest of the GNSO Council that the EPDP Phase 1 Rec 18 is followed and implemented as recommended by the working group. The current draft does not align with GNSO Council's expectations, as it does not align with the recommendation from the working group. GNSO Council acknowledged that there is no clear policy that dictates revisiting prior Board-approved recommendations and agreed that there is a concern within some members of the community with Rec 18, but also pointed out that we don't have a mechanism for validating LEA at this time. GNSO did not mention 24-hour timeline in the 29 August 2024 Council Chair communication, the only communication on the subject matter.

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?

An authentication mechanism within the proposed urgent request timeline is required. With almost 18,000 law enforcement agencies in just the United States alone (and likely many thousands more worldwide), it is very likely that simply authenticating a user submitting an urgent request will take longer than 24 hours. Namecheap and other registrars regularly receive fake police and court requests, and because of the sensitive nature of releasing customer data, it is imperative that we have assurances that any urgent request is from a valid and applicable law enforcement agency. Without such an authentication process, registrars cannot be expected to comply with the proposed timeline for disclosure. Additional policy development is required for this (e.g. it cannot be accomplished through non-policy methods). We support additional policy development to design, test, and implement this mechanism and will join any policy efforts to that end. There are many challenges and concerns that will need to be addressed prior to adopting any authentication system, and a policy development process is a good place to make sure all stakeholders' concerns are addressed.