

Note to reviewers: This is a working document used to draft the policy language. Please note that the section number referenced to the policy and the language may have been changed.

Note to IRT: This rationale doc is provided to document and share the conflicting IRT inputs. Therefore, please refrain from adding comments that note disagreements. Please limit your comments to missing or new information only. At the bottom of this document, there is a place for other comments such as process.

Rationale Doc: 24 hour Disclosure Requirement

Background

Recommendation 18 identified the need for 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].”

The original draft policy included language stating that if a Reasonable Request for Lawful Disclosure is considered urgent, which is limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure, or child exploitation, Registry Operators and Registrars MUST instead respond within 24 hours. This language was proposed as a result of existing requirements in the RAA (section 3.18.2) and the [Framework for Registry Operator to Respond to Security Threats](#), previously developed in consultation with Registry Operators and members of the GAC Public Safety Working Group. The Framework encourages Registry Operators to acknowledge receipt of security related requests categorized as “High Priority” within 24 hours, and to include details of what they will be doing to address the request moving forward, including that they may be doing nothing.

Inputs from IRT

Some IRT members have expressed concern over the response time that is required. Those members have stated that the proposed twenty-four (24) hour response time is a business hardship and have suggested that ICANN org incorporate business days into the requirements. As a result, some members of the IRT proposed the following alternative policy language:

“For an Urgent Reasonable Request for Lawful Disclosure, Registrars and Registry Operators MUST acknowledge and respond without undue delay, but within (1)

business day from receipt. If responding to a request is complex or a large number of requests are received, Registrars or Registry Operators MAY extend the time for response up to an additional two (2) business days provided Registrars or Registry Operators provide notice to the requestor within the initial (1) one business day period and explain the need for an extension of time.”

Along with the above alternative policy language, IRT members suggested defining Urgent Reasonable Request for Lawful Disclosure and moving that language to the definitions section as follows:

- Urgent Reasonable Request for Lawful Disclosure means a request closely related to circumstances identified by local-jurisdiction Law Enforcement that pose an imminent threat to life, serious bodily injury, critical infrastructure, or child exploitation.

Contracted party members of the IRT also offered the following points in support of the proposed alternative policy language:

- The timeline for response is modeled after the timeline structure for data subject access requests under GDPR: an outer limit of (1) business day for acknowledgement and response with the ability to extend for an additional (2) business days provided the contracted party provides notice to the requestor.
- Practically speaking, this means most of these truly urgent requests should be acknowledged and responded to in under a business day unless there are circumstances that make that difficult, in which case the contracted party is required to communicate with the requestor about the timelines for response.
- For the truly bad actors that ignore requests all together, the requestor will be able to take action with compliance after one business day of non-response.

In contrast to the above suggestion, other IRT members expressed support for the requirement for registry operators and registrars to respond to urgent requests within 24 hours, indicating that this timeframe is reasonable. Specifically, these IRT members noted that law enforcement and others involved in protecting the public need a mechanism to deal with "urgent requests," which by definition are limited to a narrow range of situations. These IRT members believe the existing draft language with the 24 hour response requirement leaves room for registries and registrars to explain if they cannot meet this deadline. Furthermore, these IRT members point out that this timeline is consistent with other existing frameworks:

1. The Registrar Accreditation Agreement (Section 3.18.2), provides for 24/7 24 response to LEA requests: *“3.18.2 Registrar shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the Registrar is established or maintains a physical office. Well-founded reports of Illegal Activity submitted to these contacts must be reviewed*

within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report. In responding to any such reports, Registrar will not be required to take any action in contravention of applicable law.”

2. The Security Framework for Registry Operators (2017) also provides for 24 hour timeframe for responding to "High Priority" requests of a legitimate and credible origin.

Another idea discussed in the IRT is to consider adding an SLA that 95% of the time the response is within the 24 hour time frame to allow flexibility for requests that take longer to fulfill. Members supporting the 24 hour timeframe also reacted to the use of “business days,” noting that by adding “business” the 24 hours becomes three days or more if it’s over a weekend, which then weakens the 24 hour requirement. Ultimately, this group of IRT members finds that the 24 hour period is a reasonable turnaround for this narrow category of urgent requests.

Rationale for Current Policy Language/Requirement

The current draft policy language includes the following section:

10.5 Registrars and Registry Operators MUST acknowledge receipt of a Reasonable Request for Lawful Disclosure within two (2) business days from receipt, and MUST respond without undue delay, but within thirty (30) calendar days, absent exceptional circumstances. Exceptional circumstances MAY include the receipt of a large number of requests, such that a response time of greater than thirty (30) days would not be unreasonable. If a Reasonable Request for Lawful Disclosure is considered urgent, which is limited to circumstances identified by local-jurisdiction Law Enforcement that pose an imminent threat to life, serious bodily injury, critical infrastructure, or child exploitation, Registry Operators and Registrars MUST instead respond within 24 hours.

As noted above, this language takes a similar approach as section 3.18.2 of the 2013 RAA and the Framework for Registry Operator to Respond to Security Threats. Section 3.18.2 of the RAA requires registrars to maintain a designated abuse point of contact to receive reports of abuse involving illegal activity by law enforcement, consumer protection, quasi-governmental or other similar authorities. Registrars must review well-founded reports of illegal activity submitted to the contact within 24 hours by an individual who is empowered to take necessary and appropriate actions in response to the report. Furthermore, the Framework for Registry Operator to Respond to Security Threats, which was developed by representatives from registries, registrars, the Public Safety Working Group of the GAC and ICANN org, encourages Registry Operators to acknowledge receipt of security related requests categorized as “High Priority” within 24 hours. The Framework also defined the term “high priority” as “an imminent threat to human life, critical infrastructure or child exploitation.” Since this definition and expected response time was developed by the collaboration of

multiple stakeholders, it was incorporated into the definition and requirements of urgent requests.

Since the term “urgent request” is narrowly defined, there are limited circumstances in which an acknowledgement must be sent within 24 hours (i.e. “circumstances identified by pose an imminent threat to life, serious bodily injury, critical infrastructure, or child exploitation”). The definition presents a high threshold and therefore there may be a lower likelihood that Registry Operators/Registrar will receive requests that meet the standard of urgent frequently or in a high volume.

Additionally, the 24 hour requirement takes “business days” out of the equation since the term does not have a standard definition in different regions and the use of business days could result in acknowledgements that occur well beyond 2 calendar days. As “business days” may be defined differently depending on the region or individual business it applies to, use of business days in the policy language creates significant challenges for enforcement of a standard response time.

In response to questions from the IRT as to why the definition of urgent requests is included in Section 10.5 of the draft policy rather than the definitions section: this was incorporated into the relevant paragraph because it was related to this specific section and not relevant to the policy more globally. However, based on the suggestion we have added the term to the definitions section.

Place for Miscellaneous comments: Process etc.

CPH Response:

We would encourage the IRT team to dedicate meeting time to discussing the CPH proposed timeline for urgent disclosure requests. Copied from the comment on OneDoc section 10:

“For an Urgent Reasonable Request for Lawful Disclosure, Registrars and Registry Operators MUST acknowledge and respond without undue delay, but within (1) one business day from receipt. If responding to a request is complex or a large number of requests are received, Registrars or Registry Operators MAY extend the time for response up to an additional two (2) business days provided Registrars or Registry Operators provide notice to the requestor within the initial (1) one business day period and explain the need for an extension of time.”

We believe this to be a reasonable timeframe for responses in this context, and it aligns with

the EPDP Phase 2 Initial Recommendation #9 as well as preliminary discussions within the IRT.

We note that these are one-off requests that are not submitted through the SSAD, and Law Enforcement already has the means to contact Contracted Parties directly to request disclosure of data; Contracted Parties remain dedicated to working with Law Enforcement and providing timely responses. We would appreciate further specific information regarding gaps in the existing process(es) and how this can be further refined to provide more effective responses for urgent requests.

There do remain some other open questions around urgent requests which the IRT should review (besides the question of response time).

There are gaps in the current requirements around urgent disclosure requests. What happens if a requestor abuses the urgent request process? What recourse does a Contracted Party have if a request is marked as urgent but the Contracted Party disagrees with that characterization?

The definition of urgent also still requires further refinement. "Critical infrastructure" is a broad term that is not yet standardized and would benefit from team discussion.