

## **SPECIFICATION 5: LAW ENFORCEMENT AUTHORITY DISCLOSURE FRAMEWORK SPECIFICATION**

Provider shall implement and comply with the requirements set forth in this Law Enforcement Authority Disclosure Framework Specification.

### **1. Definition of Terms**

- 1.1. The “LEA Requestor”: A Requester that is a law enforcement, consumer protection, quasi-governmental or other similar authority designated from time to time by the national or territorial government of the jurisdiction in which Provider is established or maintains a physical office.
- 1.2. The “Requested Information”: The data asked for by the LEA Requestor. This must be detailed in the request submission.
- 1.3. The “Priority Level”: The urgency with which the disclosure request should be actioned. Disclosure requests may be categorized as “~~H~~igh ~~P~~riority” or “~~S~~tandard ~~P~~riority.” “High ~~P~~riority” requests are limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure or child exploitation.

### **2. Minimum Standards for Disclosure Request Submissions**

- 2.1. As a minimum standard for acceptance, disclosure request submissions must contain:
  - 2.1.1. Domain name or URL involved;
  - 2.1.2. Deciding authority (e.g. prosecutor, judge, police authority) behind this request and source of legal authority for request;
  - 2.1.3. Details of Requested Information;
  - 2.1.4. Priority Level, including detail about threat type and justification for Priority Level, and/or suggested deadline for response;
  - 2.1.5. Instructions regarding timeline requirements for Customer notification;
  - 2.1.6. Requestor contact details, including instructions for identity verification;
  - 2.1.7. Any details otherwise required by applicable law.

**Commented [AB1]:** Edits proposed by Sara Bockey have been supported by Eric Rokobauer, Volker Greimann

Theo Geurts and Michele Neylon said that more time is needed to consider proposed edits. No other IRT feedback has been received on this draft of the specification.

**Commented [AB2]:** Proposed edit to capture concept that High Priority (and standard priority, by comparison) is a defined term.

2.1.8. A verification statement (e.g. all provided information is true and correct).

2.1.9 A clear statement that the domain name or URL involved is part of an official investigation.

2.1.10 Except in the case of High Priority requests, a clear statement that the Law Enforcement Authority has attempted to contact the relevant parties and has no other means of identifying them.

2.1.11 For High Priority requests, in addition to the requirements specified in 2.1.1-2.1.9, the Requestor must provide specific information demonstrating that the request is High Priority due to an imminent threat to life, serious bodily injury, critical infrastructure or child exploitation.

2.2. To assist Provider, further additional information may include:

2.2.1. Evidence of earlier contact (attempts), if any, and if deemed relevant by the Requestor;

2.2.2. Requestor contact details for the Customer;

2.2.3. Reference to applicable law or ICANN regulation(s);

2.2.4. Details of decision to order disclosure of information.

### 3. Receipt Process

3.1. Pre-Request: Provider will establish and maintain a designated LEA Requestor point of contact for submitting disclosure requests. Provider shall publish on its website the designated contact (e.g. email address, telephone number, form, or other means for LEA to obtain designated LEA contact information).

3.2. Receipt Process:

3.2.1. Within two business days (as observed in the location of ICANN's principal place of business) of ~~a Standard Priority~~ disclosure request being submitted by a LEA Requestor, Provider will review the request and confirm to the LEA Requestor it has been received and contains the relevant information required to meet the minimum standard for acceptance. If the request does not meet the minimum standard for acceptance, Provider will notify the LEA Requestor.

3.2.2. Where the LEA Requestor is not known to Provider, Provider will verify the identity of the LEA Requestor.

**Commented [AB3]:** Edit proposed by Sara Bockey

**Commented [AB4]:** Edit proposed by Sara Bockey

Additional edit suggested by Steve Metalitz, add "Except in the case of High Priority requests."

**Commented [AB5]:** Edit proposed by ICANN org to address IRT concern that priority level be substantiated, to avoid all requests being labeled "high priority."

Edit proposed by Steve Metalitz—remove reference to 2.1.10

**Commented [AB6]: Note to IRT:** See note below in Section 4.1.1. Feedback is requested on this edit, which has been proposed to reflect IRT discussions on this process thus far.

## 4. Provider Response Actions

### 4.1. Prioritization:

- 4.1.1. Upon completion of the Receipt Process specified in Section 3 of this Specification, Provider will action, in accordance with Sections 4.2 and 4.3 of this Specification, the disclosure request in accordance with the Priority Level.
- 4.1.2. Where a disclosure request has been categorized as High Priority, this must be actioned within 24 hours. The LEA Requestor will detail the threat type and justification for a request with a Priority Level of High Priority.
- 4.1.3. For all other disclosure requests not identified as High Priority, Provider should seek to action these in accordance with the deadline identified in the request. If Provider cannot adhere to such deadline, Provider should notify the LEA Requestor and provide a reasonable timeframe for response.

### 4.2. Disclosure:

- 4.2.1. Within the applicable timeframe for a request's Priority Level, Provider will disclose to the LEA Requestor, using a secure mechanism, the Requested Information it holds associated with the account.
- 4.2.2. Disclosure can be reasonably refused by Provider for reasons consistent with the general policy stated herein, including without limitations any of the following:
  - 4.2.2.1. The LEA Requestor failed to provide to Provider information to meet the minimum standard for acceptance as outlined in Section 2 of this Specification;
  - 4.2.2.2. If disclosure would lead to a contravention of applicable law; or
  - 4.2.2.3. Where the Customer has provided, or Provider has found, specific information, facts, or circumstances showing that disclosure will endanger the safety of the Customer.
  - 4.2.2.4. Where Provider has not been able to verify the identity of the LEA Requestor, in accordance with 3.2.2.
  - 4.2.2.5. Where Provider has found, after investigation, that the LEA Requestor's request is not well-founded.

**Commented [AB7]: Request for Feedback:** As written, this receipt process may be read to apply to High Priority requests, resulting in a required processing time for High Priority requests of 2 business days plus whatever requirement is settled upon in Section 4.1.2, below.

IRT discussions have been inconclusive on whether this is the intended effect. Given the majority of the IRT's resistance to the adoption of a 24-hour requirement in Section 4.1.2 below, it appears that this requirement is not intended to apply to high priority requests.

Edits are being suggested in this draft to reflect this understanding of the IRT's intent, with the understanding that there is currently disagreement between registrar and PSWG members of the IRT as to what the required time for actioning a high priority request should be.

**Commented [AB8]: Request for Feedback:** 24 hours is the time period proposed by the PSWG. Registrar members of the IRT have rejected this proposal and recommended that a 1 business day requirement be adopted here.

**Commented [AB9]:** Edit proposed by Sara Bockey, supported by Eric Rokobauer and Volker Greimann.

**Commented [AB10]:** Edit proposed by Sara Bockey, supported by Eric Rokobauer and Volker Greimann.

**Commented [AB11]:** Edit proposed by Sara Bockey, supported by Eric Rokobauer and Volker Greimann.

4.2.3. If disclosure is refused by Provider, Provider must provide written notice (which may be by electronic communication) to the LEA Requestor setting for Provider’s specific reasons for refusing to disclose. Such notice must be provided by Provider to the LEA Requestor prior to any Customer notification by Provider, irrespective of the reason for refusal.

4.2.4. In exceptional circumstances, if Provider requires additional time to respond to the LEA Requestor, Provider shall inform the LEA Requestor of the cause of the delay, and agree with the LEA Requestor on a new date by which it will provide its response under this Section. 4.2. Exceptional circumstances may include delays caused by acts of nature.

**Commented [AB12]:** Edit proposed by Sara Bockey (originally proposed as new Section 4.2.4.1; staff proposes to add to 4.2.4 since there is no 4.2.4.2).

4.2.5. For all refusals made in accordance with the policy and requirements herein, Provider must accept and give due consideration to the LEA Requestor’s requests for reconsideration of the refusal to disclose.

4.2.6. Nothing in this Section 4.2 shall be interpreted nor is it intended to imply that Provider shall forego due process within its applicable jurisdiction to satisfy the LEA Requestor’s request, regardless of Priority Level.

**Commented [AB13]:** Edit proposed by Sara Bockey, supported by Eric Rokobauer and Volker Greimann.

#### 4.3. Customer Notification:

Comment from Nick Shorey—I think this is covered in 4.2.2.2?

4.3.1. Provider will notify the Customer of the disclosure request (“Customer Notification”) in accordance with its published Terms of Service and the timeframe identified by the LEA Requestor. subject to any additional requirements under applicable law or court order.

Could this be combined into a new 4.2.2.2, *If disclosure would lead to a contravention of applicable law, or require the Provider to act outside of due legal process within its required jurisdiction, irrespective of Priority Level.*

4.3.2. Provider may voluntarily set a generic timeframe for Customer Notifications (e.g., 90 days), which can be extended at the behest of the LEA Requestor. Details of any generic timeframe must be published on Provider’s website, and the LEA Requestor with a pending Request should be informed in advance of any time limit being implemented or changed.

If the intent is to give the ability of the Provider to challenge the veracity of Request when appropriate legal authority (court order etc) has been provided I disagree, as I believe the judicial process should ultimately determine the veracity and legality of the prosecution’s evidential case, and I think it is a dangerous thing to shift the responsibility to the Provider to make such determinations.

4.3.3. Customer Notification should take place at the earliest opportunity, unless such disclosure would pose a risk to operational sensitivity; safety of individuals; or is prohibited by law or court order. Such circumstances must be detailed in the disclosure request.

If the intent is to challenge the accuracy of the request, such as the domain name in question has been incorrectly spelt, or the privacy registration is not held with the Provider, then this should be covered in 4.2.2.1 and 4.2.3.

4.3.4. Provider must notify the LEA Requestor at least three business days (as observed in the location of ICANN’s principal place of business) before a Customer Notification takes place.

## 5. Issues of Non-Response/Non-Compliance with LEA Requests

5.1. In cases of the LEA Requestor receiving no response from Provider, or Provider fails to comply with disclosure requests within contractually defined or mutually agreed timelines, the issue may be escalated (a) to ICANN in accordance with ICANN's existing compliance mechanisms, or (b) through other applicable legal mechanisms.

## **6. Additional Guidance**

6.1. Provider may voluntarily action disclosure requests from non-designated government authorities in accordance with the processes detailed within this Specification so long as such action does not conflict with applicable law.

6.2. A LEA Requestor must comply with all applicable data protection laws and may only use any information disclosed to it solely for the purpose of determining whether further action on the issue is warranted, to contact the Customer, or in legal proceedings concerning the issue for which the request was made.