**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 "High Priority" or "Standard Priority." "High Priority" 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.

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 Processing: Standard Priority Request:

3.2.1. Within two business days (as observed in the location of Provider'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.

3.2.3. Upon completion of the receipt process specified in Section 3.2.1 of this Specification, Provider will seek to action, in accordance with Sections 4.2 and 4.3 of this Specification, a Standard Disclosure request in accordance with the deadline specified in the request. If Provider cannot adhere to such deadline, Provider should notify the LEA Requestor and provide a reasonable timeframe for response.

3.3. Receipt and Processing: High Priority Request

3.3.1 The LEA Requestor will detail the threat type and justification for a request with a Priority Level of High Priority. Where a disclosure request has been categorized as High Priority, this must be actioned, in accordance with Section 4.1. and 4.2, within [24 hours] [one business day, as observed in the location of the Provider's principal place of business] of receipt by Provider.

## 4. Provider Response Actions

4.1. Disclosure:

4.1.1. 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.

4.1.2. Disclosure can be reasonably refused by Provider for reasons consistent with the general policy stated herein, including without limitations any of the following:

4.1.2.1. The LEA Requestor failed to provide to Provider information to meet the minimum standard for acceptance as outlined in Section 2 of this Specification;

4.1.2.2. If disclosure would lead to a contravention of applicable law; or

4.1.2.3. Where the Customer has provided, or Provider has found, specific information, facts, or circumstances showing that disclosure will endanger the safety of the Customer.

4.1.2.4 Where Provider has not been able to verify the identity of the LEA Requestor, in accordance with 3.2.2.

4.1.2.5 Where Provider has found, after investigation, that the LEA Requestor's request is not well-founded.

**Commented [1]:** No IRT consensus on this provision. PSWG position: "high priority" requests should be actioned immediately. PSWG is willing to compromise to a 24-hour period.

Registrar members of the IRT contend that a 24-hour period is not workable. Registrars would agree to compromise to one business day.

**Commented [2]:** Comment from Steve Metalitz: This strikes me as a reasonable list of reasons why a provider would not be able to respond in a timely fashion to an LEA disclosure request (whether High Priority or Standard Priority), but not of reasons to deny altogether a request that otherwise meets the requirements of the specification. Should we append this list to what is now 4.1.4 (following "acts of nature")? I would be much more comfortable including "without limitations" there rather than in 4.1.2.

**Commented [3]:** Comment from Eric Rokobauer: I agree with Sara here. Ideally again it is to cover the Provider from potential instances that we here in this IRT may not be recognizing here.

**Commented [AB4]:** Comment from Sara Bockey: "without limitations" is necessary to ensure legitimate instances not yet listed or thought of are covered. Examples of additional causes beyond the control of the Provider: war, terrorism, riots, power outage, internet outage, internet failure, server failure, foreign gov't changes, labor disputes, etc.

**Commented [5]:** Comment from Peter Roman: I think the whole phrase is problematic and "without limitation" is especially so. I don't understand why they want to be in the position of making legal judgements about requests from law enforcement. It only increases their liability and they have no relevant expertise on which to base their decisions. In essence, they seem to repeatedly be ...

**Commented [6]:** Comment from Theo Geurts: I rather keep it in, it does not hurt and I 100% agree, democracy is not a given.

**Commented [AB7]:** Comment from Sara Bockey: I see no issue with redundancy and there is no harm in including this. If anything, it protects against potential abuse (in parts of the world that are less democratic)

**Commented [8]:** Comment from Eric Rokobauer: I believe this should be removed if IRT does find to be redundant. While I do appreciate Sara's comments, if we do all agree there is duplication here with the statement, best we remove to clear any potential confusion that could come later (thinking when we ma ...

**Commented [9]:** Comment from Steve Metalitz: I still have trouble understanding what would make a request that meets all the requirements of the specification not "well founded," …Can Sara or others provide an example of when this ground for refusal of an LEA request might come into play?

4.1.3. 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.

4.1.4. 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. 4.1. Exceptional circumstances may include delays caused by acts of nature.

4.1.5. 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.

4.1.6. Nothing in this Section 4.1 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.

4.2. Customer Notification:

4.2.1. 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.

4.2.2. 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.

4.2.3. 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.

4.2.4~~3~~. Provider must notify the LEA Requestor at least three business days (as observed in the location of Provider's principal place of business) before a Customer Notification takes place.

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

**Commented [AB10]:** Comment from Sara Bockey: Not redundant and 100% necessary. Particularly for providers in parts of the world that are less democratic. We must remember this will be applied globally. Belt and suspenders! At ICANN61 this addition gave registrars that spoke with me the most comfort.

**Commented [11]:** Edit proposed by Sara Bockey, supported by Eric Rokobauer and Volker Greimann.

Comment from Nick Shorey—I think this is covered in 4.2.2.2? on 17 April call, Steve Metalitz also commented that this seems redundant.

From Nick: 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.

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.

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.

**Commented [12]:** Comment from Theo Geurts: Agreed with Eric and Sara, 4.2.6, we could move that one around some.

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.