TRUSTED NOTIFIERS: TYPOLOGY AND FRAMEWORK COMPONENTS

REF: 22-101 | February 14, 2022

DNS Operators (Registries and Registrars or "Operators") receive notices asking them to take action on a wide range of alleged technical and content related abuses. However, there is a fundamental question of when it is appropriate to act at the DNS level, and the evaluation of whether the alleged abuse meets the threshold for action at the DNS level. Additionally, given the large volume of abuses occurring on the internet, existing resources, mechanisms and protocols available to Operators are in many cases insufficient to address abuses in a timely fashion. Moreover, in the case of content-related abuses, many Operators lack the subject-matter competencies and resources to identify, evaluate and verify the alleged abuse. In addition, in some cases, it may be illegal for Operators to try to verify certain types of allegedly abusive content (*e.g.* CSAM).

This Outcome consists of two parts. The first part "Trusted Notifiers Framework Clarity" consists of i) a "Typology of Trusted Notifiers" that identifies the different types of Trusted Notifiers, and ii) "Attributes of a Trusted Notifier Relationship" that provides guidance on how to establish Trusted Notifier relationships, including common attributes of formal trusted notifier arrangements.

The second part of the Outcome, "Establishing Formal Arrangements", catalogs the different substantive considerations that may form the basis of an agreement based on mutual affirmations of commitments between Notifiers and Operators. Such arrangements are intended to facilitate coordinated action on addressing abuses at the DNS Level. This part of the Outcome provides a framework upon which such formalized contractual agreements between Notifiers and DNS Operators may be based. It provides a set of options which may be incorporated in written agreements and seeks to provide actors with a common frame of reference with regards to the different options and their corresponding definitions.

It should be noted that there is no "one size fits all" model for Trusted Notifier arrangements. Trust is not a commodity which can be compelled. Each Operator makes its own decision as to whether and with whom it will enter into a Trusted Notifier arrangement. In addition, all Operators are subject to the local law of their corresponding jurisdiction(s); and, therefore, their ability to enter into Trusted Notifier arrangements is limited to instances in which such arrangements are lawful and appropriate under the Operator's Terms of Service. The purpose of this guide is to create a common understanding of the term Trusted Notifier, including common attributes and elements for consideration and possible inclusion in formal arrangements between Operators and Notifiers.

1. TRUSTED NOTIFIERS FRAMEWORK CLARITY

The term "Trusted Notifier" has no universally agreed-upon meaning and is used to describe a multitude of different types of arrangements, both formal and informal, between Operators and Notifiers. Formal Trusted Notifier arrangements are distinct from less structured arrangements that may exist between Operators and third parties making abuse notifications (*see infra*, Habitual Notifiers, Verifiers and Mandatory Notifications). For our purposes, the term "Trusted Notifier" includes third party notifiers with whom the Operator has entered into a formal, structured arrangement based on a high degree of trust and confidence. In addition, many Operators work closely with local law enforcement to mitigate online abuse and will act on their notifications even in the absence of a court order compelling action and without a formal written agreement. The high degree of trust between Operators and local law enforcement likewise establishes the predicate for a Trusted Notifier relationship. The following subsection 1.1 "Typology of Trusted Notifier" explains these two broad, but widely accepted types of Trusted Notifiers. Subsection 1.2 Attributes of a Trusted Notifier Relationship" provides a non-

exhaustive list of attributes that are pertinent to a Trusted Notifier relationship, which an Operator may wish to consider when deciding whether to enter into a Trusted Notifier relationship.

1.1 TYPOLOGY OF TRUSTED NOTIFIERS

Types of Trusted Notifiers	Description
Law Enforcement with Prosecutorial Authority	Many Operators liaise with local law enforcement authorities who have prosecutorial authority to seize or cause the suspension of domain names in the Operator's jurisdiction, and Operators may choose to act in response to notices from local law enforcement or other Notifiers without a court order or formal process on the basis of trust and with or without any formal agreement. These relationships have heightened relevance for ccTLD operators.
Formal Arrangements	Formal arrangements may take the form of contracts, Memoranda of Understanding or other written instruments which govern the relationship between the Notifier and the Operator and define the expectations and responsibilities of the parties.

1.2 ATTRIBUTES OF A TRUSTED NOTIFIER RELATIONSHIP

As noted above, Trusted Notifier relationships can help address abuse online by providing an Operator with an established process and confidence level for notifications. The elements below provide the contours of such a relationship.

Demonstrated industry knowledge / expertise: First and foremost, Operators typically require the Notifier to establish its *bona fides* as an expert in the subject matter for which the formal Trusted Notifier arrangement is being pursued. This includes a demonstrated awareness of certain operational considerations such as an understanding of Operator's systems, processes, requirements, and anti-abuse policies, as well as the production of clearly actionable notices and a commitment to not overwhelm Operator's abuse mitigation capacity and resources.

Communication: The relationship always involves communication between the two parties where they both agree how the arrangement will work. It will often result in an agreement on the process for notification and various components that must be included in the notification. This could result in formal documentation, for example, some parties will prefer to have legal agreements in place which cover the liability in relation to false positives.

Specific Nature of a Formalized Trusted Notifier Arrangement: A Trusted Notifier is a specific relationship between one Operator and one external organization or individual. In this relationship, the two parties have made an agreement on their expectations. For example, an Operator may agree to suspend a domain name following a notification from that notifier if it contains certain mandatory information or evidence, especially

with respect to certain types of abuse where there is universal or near universal normative consistency such as Child Sexual Abuse Material (CSAM). In other cases, the Operator may agree to accord the notice a heightened degree of priority but the final decision as to whether to act upon the notice remains with the Operator.

Optional in Nature: Operators decide which notifiers they trust and for what purposes. For example, having a Trusted Notifier relationship with one registry does not mean that Notifier will automatically have this status with another registry. Similarly, a given Notifier may be trusted on a particular subject matter, but not another subject matter by the same registry. An Operator may also, depending on the progression of the relationship or ongoing assessment of the relationship, choose to no longer trust a particular Notifier. Finally, certain Operators are subject to specific formal legal processes for notifications which can make the use of a Trusted Notifier unnecessary. Trusted Notifier relationships are therefore optional and implemented at the discretion of each Operator.

Distinguishable from Other Methods of Addressing Abuse Online: It should be noted that, Trusted Notifiers are not the only method available to address abuse online, nor is the concept appropriate for all Operators or all jurisdictions. The Trusted Notifier relationship should be distinguished from other types of notification or verification arrangements, some of which are listed below:

- ***Habitual notifiers that Operators trust based on previous interactions:*** These are Notifiers in whom the Operators places a high degree of confidence based on previous notices without the existence of a formal arrangement. Operators may accord such notices a heightened degree of priority.
- ***Verifiers:*** Some Operators use verifiers to help them make decisions. A verifier is an external party with relevant expertise who is known to the Operator. This may be useful when an Operator receives a notice outside of a Trusted Notifier relationship and would like additional information to help them make a decision as to whether action is appropriate, proportionate and helpful to prevent or address abuse.
- ***Mandatory notifications:*** Operators may also receive notifications from certain external organizations/authorities which they are legally required to act on. For example, law enforcement or regulators, or court orders from an applicable jurisdiction. In these cases, the discretion of whether the action against the registrant is proportionate or appropriate does not lie with the Operator. This type of notification sits outside the trusted notifier relationship – which, as noted above is an optional arrangement.

2. ESTABLISHING FORMAL ARRANGEMENTS

Previously, the Domains & Jurisdiction Program Contact Group has addressed the question of how to increase the quality of and confidence in individual notices by producing a Due Diligence Guide for Notifiers, as well as Minimum Notice Components regarding Technical Abuse. Building on these outcomes, the following set of considerations are intended to provide a basis that may define and underpin the relationship between Operators and Contractual Notifiers. These considerations are optional elements that may be included in formal Trusted Notifier arrangements.

In that spirit, Trusted Notifiers Framework Agreements can be organized around three dimensions. The first covers “Potential Elements for Notifiers to earn trust from Operators” and describes the different options that notifiers may commit to undertake as part of a formal agreement. These options seek to inform and provide

clarity to the nature of the relationship and the prerequisites for making successful notifications.

The second dimension focuses on "Potential commitments expected from Operators", clarifying the different sets of commitments that Operators may adhere to when receiving notices under such agreements, when the agreed-upon prerequisite conditions have been met.

The third dimension focuses on "Post action considerations", pertaining to the elements secondary to the subject of the arrangement, such as transparency reporting obligations and dispute resolution.

2.1 POTENTIAL ELEMENTS FOR NOTIFIERS TO EARN TRUST FROM OPERATORS

Accuracy statistics: Notifiers may be required to provide up-to-date statistics on the efficacy and accuracy of their notices both as a predicate to entering into a formal Trusted Notifier arrangement and as an on-going obligation, once the arrangement has been established.

Third party-review mechanism: in the detection and validation process. Operators may require Notifiers to incorporate third party review mechanisms in the process of identification and evaluation of alleged abuses.

Transparency: The Notifier may be required to furnish transparency information to the public regarding its abuse mitigation program and its Trusted Notifier arrangements.

Potential Liability Implications: The Notifier should be cognizant of the liability risks on Operators for actions taking on their notices. This may result in Operators requiring measure such as:

- Indemnification: The Notifier may consider whether to indemnify the costs, fees and/or any money judgment incurred by or assessed against the Operator as a consequence of its action on notices.
- Litigation Support: In lieu of or in addition to indemnity, the Notifier should consider whether to commit to provide reasonable and necessary support to the Operator in litigation arising from action taken pursuant to notice.

Additional Considerations for Content-Related Alleged Abuses:

- The authoritative expertise of Notifier in the identification of such content abuse;
- The geographic extent of the Notifier's expertise (*e.g.* understanding of local context, specialization etc.);
- The legal basis for such a relationship (e.g in some cases, certain ccTLDs may be legally obligated to act on notices issued by governmental bodies, and the competence to investigate certain types of content for specific authorities may provide confidence to certain operators, e.g. ccTLDs);
- The legal basis for such notification.

2.2 POTENTIAL COMMITMENTS EXPECTED FROM OPERATORS

Prioritization: The formal arrangement may require Operators to grant special attention and/or treatment in evaluating the notices.

Commitment: The Operator may be required to take action on notices which have been vetted and confirmed to

be present a valid abuse case.

Course of Action: The arrangement should specify the expected course of action by the Operator in response to the Notifier's notices. This may include whether there is a presumption of implementation of action upon notification without the Operator's independent verification (*e.g.* in cases involving CSAM); or, alternatively, whether the decision to take action is subject to the Operator's exercise of independent judgment and discretion according to its Terms of Service.

Response Timeframe: Operators may be required to commit to a stipulated time frame in responding to, evaluating, and acting upon notices.

Notification of Affected Parties: The arrangement may specify whether and when (ex-ante, ex-post or simultaneously) the Operator will notify affected parties, including, as applicable, the Registrar, Registrant, and the Notifier.

Disclosure of the Existence of the Trusted Notifier Arrangement: The agreement may stipulate whether or not the Operator will disclose the existence of the formal Trusted Notifier arrangement.

2.3 POST ACTION CONSIDERATIONS FOR BOTH NOTIFIERS AND OPERATORS

Transparency Reporting: Operators may publish transparency statistics on substance/subject matter, disposition and number of notices received from the Trusted Notifier.

Dispute resolution post action (between Registrant and Operator): The Notifier should be aware of and be prepared to accept the results of any dispute resolution mechanisms (*e.g.* appeals processes, ADR procedures, or the Operator's internal mechanism(s)) employed by the Operator related to disabling domain names.