DNS-LEVEL ACTION TO ADDRESS TECHNICAL ABUSE
DUE DILIGENCE GUIDE FOR NOTIFIERS

REF: 20-113 | November 2, 2020

All notifiers have a duty to conduct due diligence before making notifications of alleged technical abuse[1] to DNS Operators and requesting action at the DNS level to remedy such abuse. While action at the DNS level may be appropriate to address certain types of technical abuse, DNS-level action has a major impact not only on the domain name, itself, but potentially on other activities linked to the domain name, such as email, name servers, databases and other services which are linked to the domain. DNS-level action to address alleged technical abuses must be therefore not only effective, but efficient and proportionate to the harm(s) alleged. By employing *procedural and substantive*[2] due diligence measures before making notifications to the DNS Operator, notifiers can increase the efficiency and effectiveness with which the Operator evaluates and addresses notifications of alleged abuse.

This document lists a series of questions notifiers should ask themselves in order to determine that making notices to operators is appropriate. This guide is structured around three parts; Identification; Evaluation; and Notification. The Identification and Evaluation sections list the *substantive* due diligence a notifier is encouraged to perform to determine that abuse is present and whether action at the DNS level is appropriate to address it. The Notification section indicates the level of *procedural* due diligence that notifiers are encouraged to conduct in order to ensure that the notice is addressed efficiently and effectively.

Acting at the DNS level can be justified to remediate technical/infrastructure abuse in order to protect the stability and security of the global infrastructure of the internet. DNS operators rely on a variety of internal and external resources to identify, evaluate and take action to remediate technical abuse. While establishing whether a domain is being used to perpetrate technical abuse tends to produce binary results (i.e. the domain is or is not engaged in technical abuse), care should nonetheless be taken to ensure that action at the DNS level to remediate said abuse is appropriate and proportionate.

IDENTIFICATION

The following questions will help notifiers when identifying potential abuse

- What triggered the Notifier's attention to this abuse and does the Notifier have first-hand knowledge of the alleged abuse?
- What is the type of technical abuse at stake? Does this appear to be something that can and should be mitigated at the DNS level?
- What is the evidence for the existence of such alleged abuse?
- Is it likely that the domain has been compromised, i.e. the infringing action has been done without the knowledge or intent of the registrant/site operator?

[1] For scope of technical abuse, Refer to Annex in Domains & Jurisdiction Program Outcome on DNS Operators' Decision-making Guide To Address Technical Abuse

[2] Refer to Criteria E2: Due Diligence by Notifiers in Domains & Jurisdiction Operational Approaches

EVALUATION

When making a referral to a DNS Operator or Infrastructure Provider, notifiers should make the referral to the entity closest to the abuse and most likely to be able to evaluate the specific problem and remediate it with the least collateral damage. The questions below can help a Notifier determine which Operator is best positioned to help.

- Where is the abuse taking place, e.g. sublevel domain, specific url etc.
- Is action at the DNS level[3]appropriate or are there other means to address the abuse?
- If there is a more appropriate actor than a DNS Operator to address the abuse (e.g., hosting provider or site operator), has there been an attempt to address the abuse at that level?
- Would action at the DNS level create collateral damage disproportionate to the harm caused by the alleged abuse?
- What could be the appropriate choice of action at the DNS level to address the abuse?
- Who are the relevant registry and registrar and how do their respective Terms of Service address such type of abuse?
- Is there a way to assess (including through interaction with relevant authorities) if there is an ongoing investigation that a DNS-level action could jeopardize?

NOTIFICATION

When making notification to DNS Operators, Notifiers should consider the following questions to improve the efficiency and efficacy of their notices.

- When action at the DNS level is appropriate, to whom should notification be made: Registrar, Registry, both?
- Does the notifier have an existing contractual relationship with the Operator and have the terms of such contract been met?
- What is the DNS Operator's preferred channel for notification of abuse?
- Does the DNS Operator have a prescribed reporting format?
- Does the notice contain all the required components for a good/effective notice[4]?
- Should the notice be designated confidential, e.g. in cases where there is a risk of jeopardizing an investigation?

[3] Refer to I&J Educational Resource on Effects of Action at the DNS Level

[4] Refer to Domains & Jurisdiction Program Outcome Minimum Notice Components for Technical Abuse