MINIMUM NOTICE COMPONENTS FOR TECHNICAL ABUSE

REF: 20-109 | July 21, 2020

DNS Operators frequently receive complaints of technical abuse "Notices" in a broad diversity of formats that often do not contain sufficient information for investigation and action. The following table, based on Criteria C of the Operational Approaches document, therefore proposes a list of components that support actionable Notices for reporting technical abuse. [1] While the table indicates a subset of components that are necessary to make a given Notice actionable, as well as those components which significantly assist the operator in addressing the alleged abuse, all components listed are important contributions to robust and effective Notices. In general, more detailed Notices are better in assisting the operator's evaluation and response. Additionally, where the notifier submits evidence of alleged technical abuse in the form of attachments (e.g. screenshots of alleged phishing), operators may reasonably employ an added layer of security review to ensure that attachments are not infected. This may increase the timeframe for the operator's review of the Notice, depending upon the operator's internal security capabilities.

Elements marked with a red asterix(*) are components without which Notice is not actionable. Those highlighted in blue can significantly help the operator deal with the Notice.

IDENTIFICATION		Components without which notice is not actionable (A)
Time*	Date and time corresponding to the issuance of the request.	A
Type of Notifier	Refer to Typology of Notifiers (court, law enforcement, private notifier, legal representative of a complainant, Anonymous)	
Issuing Entity[2]*	Identification of the requester	A
Request ID number	Reference provided by the issuer of the request (if applicable).	
Registrar (if Notice is addressed to the Registry)	Name and Abuse Point Of Contact of the Registrar managing the registration.	

[1] The criteria for notifications for Website Content Abuse are considered separately, not in this document.

[2] While the identity of the person or entity making the Notice is generally required for operator's to fully evaluate a given Notice, there are circumstances where operators may accept and evaluate Notices that are submitted anonymously, particularly where the subject matter of the alleged abuse is especially sensitive, such as those involving allegations of Child Sexual Abuse Imagery ("CSAM").

Registry (if the Notice is addressed to the Registrar)	Registry managing the corresponding TLD extension. If not known, indicate the TLD.	
CASE - In case of court order from court of applicable jurisdiction		
Type of abuse*	Indication of the type of abuse alleged (from taxonomy list)	A
Legal basis*	A copy of the court order	A
DUE DILIGENCE[3] - In case of no court order from court of applicable jurisdiction		
Evaluation	Steps undertaken by the notifier - prior to notification of the DNS Operator - to establish the existence, and extent of the abuse in conformance with the Operators' applicable policies	
Supporting evidence	Factual documentation of the alleged abuse and evaluation. This may be in the form of listings on reputation block lists (RBLs) the operator relies upon or through direct evidence (like screenshots in the case of phishing).	
Foreign Public Authority*	An official notice, documenting the elements above, including, where necessary, effort to domesticate foreign court order, if any.	A
Proportionality	Justification that the alleged abuse meets a sufficient threshold for action at the DNS Level, and also factoring potential collateral damage and the effectiveness of action at the DNS level.	
REQUESTED ACTION		
Targeted domain(s)*	Specific domain name(s) upon which action is requested, including URL.	A
Action sought*	Indication of the specific action requested (see Operation Criteria F - Types of Actions)	A(in case of court order from

[3] For technical abuse, all requests made to ccTLD Operators by notifiers other than a court of applicable jurisdiction can be acted upon on a voluntary basis according to Operators' Terms of Service and national legislation, when applicable.

		applicable jurisdiction)
TIMING		
Deadline	When the action(s) should be executed (important in particular in case of concerted actions or emergency)	
Time range	Duration of the requested action (if applicable, If action sought is not 'transfer/delete')	
Emergency	Is this action justified by a particular emergency (nature of emergency)	
Rationale emergency*	Explanation of how the requested action will avert or mitigate the emergency	A (If notified as an emergency)
CONFIDENTIALITY		
Confidentiality	Request not to notify the registrant prior to action or potentially even ex post for a period of time (if applicable)	
Confidentiality timeline*	Requested duration of confidentiality	A(If confidentiality is requested)
Rationale for confidentiality*	Proper justification for confidentiality request and timeline (can be included in the Court Orders)	A (If confidentiality is requested)
AUTHORITY		
Authentication	Information allowing verification of the identity of the Notifier and the authenticity of its Notice	
Certification	Written self-certification by the Notifier of its competence, performance of prior due diligence and accuracy of its statements and that there is no improper motivation or illegitimate purpose for requesting the suspension/cancellation.	
CONTACTS		

Issuing entity	Contact details of the Notifier, to which notification of action (or non-action) should be sent	
SIGNATURE		