# Re: Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations

# NCSG Comments

July 10, 2023

Thank you for the opportunity to comment on the amendment. We would appreciate it if you could clarify how you address the public comments and if there will be changes to the suggested amendment as a result of public comments, and if you could provide a response to our comments.

**Changing "Security Threat" to "DNS abuse"**
"DNS abuse" is an ambiguous term and the ambiguity does not stem from technical matters but political and other intentions. So however precisely you define DNS abuse, in the end, it is open to interpretation. We are not clear on the need to change the term. There is no rationale provided. The term "Security threat" amply defines the issue, which is the threat to the DNS. DNS abuse will open issues for conversation and debate later on.

**Including Spam**
We do not believe spam should be included in the definition of security threat even with a clarification that it is narrowly described and only "when spam serves as a delivery mechanism for the other forms of DNS Abuse, namely, malware, botnets, phishing, and pharming". We don't think a proper technical consultation has been done regarding this addition. The SAC 115 invokes other forums such as the registrars-registries own initiative for providing this clarification as well as an external forum (Internet and Jurisdiction Project) and it does not seem that they have consulted with the broader technical community about this definition of spam. As the definition stands, it is very much prone to over-reporting as the spam might not be used for DNS abuse right away but potentially used in the future to deliver malware. Spam also might not be categorized as DNS abuse, as Email protocols are used to deliver spam and not the DNS. We recommend another round of consultation with the technical community and hopefully elimination of spam from the amendment.

**Mitigation Measures**
The non-commercial community remains concerned about the open-ended nature of the mitigation measures included in the revisions. We do not agree with the argument that avoiding prescriptive measures means there will always be a measured response to "DNS abuse" reports. It seems to our community that by leaving this open there is a risk that some

contracted parties will simply find it expedient to respond harshly to these reports (i.e. by simply disabling the domain), and, as is often the case, the impact will fall to the most vulnerable, which in this context means institutions without the resources to even know what is going on, much less dispute the action after the fact. Terms like “actionable evidence” and “reasonable discretion” do not begin to clarify what contracted parties are allowed to do, especially since, as pointed out above, the entire concept of “DNS Abuse” is so ambiguously defined. We see great risk if there are  no clear actions to specific threats.

**Our general concern**

We are generally concerned with the direction that ICANN and the contracted parties are going in doing bilateral negotiations to resolve very thorny policy issues. It could set a bad precedent.