Comment on:
Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations

After long and often conflictual discussions around the very notion of DNS Abuse, these concise and balanced amendments represent significant progress and deserve to be welcomed by all actors. Within a clearly defined scope of abuses, they set very specific, yet flexible, responsibilities for contracted parties when dealing with abuse reports. The Secretariat of the Internet & Jurisdiction Policy Network (I&JPN) therefore strongly encourages the adoption of these amendments, as this will constitute a litmus test for the capacity of the multistakeholder approach to enact meaningful binding rules.

For a long time, arguments about the meaning of "DNS abuse" prevented fruitful discussions within the ICANN community on when and how it is appropriate to act at the level of the DNS to address abuses online. The proposed amendments represent a significant and welcomed step in the right direction, in particular because they clarify very important points, through concise and balanced formulations, including:

1) **A clarified scope and definition**
   The amendments define DNS abuse as: malware, botnets, phishing, pharming, and spam (when used as a delivery mechanism), clearly distinguishing such abuses from other, content-related ones. This list, introduced in I&JPN's Operational Approaches in 2019 was enshrined in 2021 within SAC 115 with detailed definitions. This provides a useful operational scope, focusing on abuses of high importance and where action at the level of the DNS is the most justifiable.

2) **Confirmation of reporting**
   An obligation to provide confirmation of receipt of an abuse report is introduced in the gTLD Registry Agreement. This was a longstanding request and represents a simple measure that will reduce uncertainty for notifiers and build trust. **Note**: this provision is not yet included in the parallel agreement for Registrars. This might be considered as a useful addition.

3) **Actionable evidence**
Too many abuse reports are ill-formed, incomplete or otherwise not actionable. The expression "actionable evidence" in the amendments highlights the importance of providing sufficient information for DNS operators to evaluate, without an excessive burden, the opportunity to act and choose the appropriate action. The list of minimum components of notices developed by I&JPN's Domains Contact Group can provide useful guidelines in that regard.

4) **Appropriate action**
DNS operators have only 5 ways to act on a domain name under their purview and there are often misunderstandings regarding their effect and impact on abuse mitigation. Choosing the right action is an important decision and the amendments rightfully anticipate that this "*may vary according to the circumstances of each case, taking into account the severity of the harm from the DNS Abuse and the possibility of associated collateral damage*". This flexibility is necessary to account for the general bluntness of action at the DNS level.

5) **Actions that are reasonably necessary**
This expression elegantly enshrines the dual objective of necessity and proportionality, in line with point 4) above.

6) **Must promptly take mitigation action**
This provision rightly stresses that time is of the essence when mitigating DNS Abuse. But most importantly, it establishes, for the first time, an obligation to act when actionable evidence has been provided. This usefully sets a strong actionable basis for ICANN's compliance mechanisms, and establishes a baseline standard of behavior to reduce the free-riding of some actors that still harms the community's reputation.

7) **Use of webforms**
This apparently minor change has a significant positive potential to improve the notification and mitigation workflow. Webforms can reduce the risk of abusive reporting that mere email addresses entail, ensure the production of better-documented notices, and pave the way to more automated notification (but not decision-making) processes. In that regard, the NetBeacon reporting tool developed by the DNS Abuse Institute (in cooperation with CleanDNS) already provides a useful centralized reporting interface that could in the future help smaller operators implement such webforms without the burden of the related development costs.

8) **Registry-registrar interactions**
Finally, the combination of the two proposed amendments clarifies the respective responsibilities of registries and registrars, as the Registry shall, at minimum, refer the notified abuse (with relevant evidence) to the sponsoring Registrar, or take action itself when it deems it appropriate.

The I&JPN Secretariat is pleased that the 5 years of work in its Domains & Jurisdiction Contact Group helped pave the way for the initiative to develop these balanced amendments, which represent a significant achievement. **We strongly encourage contracted parties to adopt them**, as this represents a litmus test for ICANN's capacity to enact meaningful binding rules in the public interest.

Failure to achieve sufficient support would, in a context of renewed regulatory pressure regarding abuses online, feed into a narrative that the multistakeholder approach is unable to impose on irresponsible actors any constraint, however necessary and proportionate.

Conversely, **adoption of these amendments will send a strong signal** both within the ICANN Community and outside of it that DNS operators are ready to fully fulfill their specific responsibilities in the collective effort to address DNS Abuse. It also will demonstrate the capacity of ICANN to achieve progress on a contentious issue.
