CleanDNS Public Comment to gTLD RA and RAA Modification of DNS Abuse Contract Obligations

Summary

CleanDNS would like to thank ICANN and the contracted parties for the opportunity to provide feedback on the proposed amendments and we congratulate all parties on the exceptional speed and commitment to anti-DNS Abuse efforts that has been shown so far in this process. CleanDNS welcomes the proposed amendments to both the base Registry Agreement (RA) and the Registrar Accreditation Agreement (RRA). We believe that the agreed upon wording strikes a very appropriate balance, updating the terms and expectations of both agreements, while remaining true to the remit and bylaws of ICANN, in remaining content neutral in their approach.

About CleanDNS

CleanDNS (www.cleandns.com) is an anti-abuse and online harm management and mitigation platform, developed by a team of cyber security and investigative professionals who recognized the critical need for a systemized, standardized and customizable process to rein in domain name abuse and shorten the life cycle of domains used for abuse. The CleanDNS platform utilizes an evidence-based workflow that simplifies and accelerates domain abuse mitigation procedures. By facilitating early detection of abuse, CleanDNS assists with detecting likely sources of abuse with tools and processes to effectively mitigate. CleanDNS currently monitors zones of 300+ TLDs that contain ~31+ million domains. We also donated and power the technology behind the DNS Abuse Institute's (www.dnsai.org) NetBeacon (www.netbeacon.org), a tool to empower individuals and organizations to report suspected online abuse and to empower registrars to take action against online abuse.

Narrative

To begin we must acknowledge, and applaud the restraint shown in these amendments, on a sometimes emotive subject. We therefore make this comment, fully acknowledging and accepting that the proposed amendments seek only to raise the minimum expectations in abuse management. The amendments are properly aimed at contractual expectations, and do not seek to establish or enforce best practices. Whether or not individual contracted parties may seek to implement the higher standards or expectations that are reflected in established industry best practices (e.g. the Framework to Address Abuse), remains a matter for the contracted party themselves. The amendments, as drafted, do not seek to interfere on this. CleanDNS, naturally, continues to be a strong proponent of best practice in anti-DNS abuse actions, however, we accept and applaud the restraint both ICANN and the contracted parties have shown. This restraint has been aptly demonstrated in the drafting of wording that seeks to establish a contractually appropriate minimum standard, one that is based on an expectation of reasonable actions for appropriately evidenced instances of DNS Abuse.

Definition of DNS Abuse

CleanDNS welcomes the inclusion of a clear, baseline definition of DNS Abuse. In doing so, the parties have sought to establish a degree of increased contractual certainty. Arguments as to what DNS Abuse may include, when taken at its apex, should not be confused with the RySG's and RrSG's stated objective, when they initiated this amendment process. In their letters, the parties sought to establish an enforceable minimum expectation for both ICANN and the Contracted Parties alike. This appears to have been achieved. CleanDNS welcomes the inclusion of a predictable and contemporaneously quantifiable working definition of DNS Abuse as it applies to these contracts. Not only does this ensure clarity for the parties subject to the contract, but it also affords services like CleanDNS, who help support and enable a clear path towards measurable compliance for contracted parties. Such certainty also enables us to help further define and support any enhanced efforts that to be pursued by registries and registrars alike, as best practices, that go beyond such minimal contractual expectations.

ICANN Bylaws

We must also specifically acknowledge that ICANN is prohibited by their bylaws from engaging in content moderation. As such, we appreciate the parties' efforts to ensure the RA and RRA continue to respect ICANN's bylaws. We also acknowledge that nothing in these amendments restrict or prevent individual operators from seeking to intervene in matters where the objective need for such an action is high (e.g. CSAM, serious and credible and or immediate threat of harm to human life). To be clear however, this is not a matter that ICANN may seek to enforce via the contracts. As such, we welcome the fact that these contract amendments do not purport to encroach on matters of 'content'. Any related action or expectations that may be voluntarily taken by a contracted party on such matters of 'content', is outside of the ICANN remit and should continue to be a matter for that operator to appropriately decide in any given circumstance.

Actionable Evidence

In particular, CleanDNS welcomes the specific and pragmatic inclusion of the expectation of "actionable evidence". Any mitigation action should be capable of being justified. This aligns with the expectations of 'non-arbitrariness', a concept which is not only a cornerstone of due process, but is becoming a specific expectation in emerging global legislation, such as the Digital Services Act in the EU. Any action that is taken at the DNS level, should only be done with a full assessment of the evidence grounding such an action, with due regard to impact of the proposed action, given the circumstances recorded. CleanDNS is a vocal proponent of evidenced based escalations, i.e. escalation where instances of DNS abuse can be linked to clear evidence of that abuse, or that can demonstrate that a registration of a domain was for a primary purpose of DNS Abuse. It is only with such evidence to hand that an operator may properly consider the appropriate action to be taken. We applaud the pragmatic inclusion of 'actionable evidence' as an obligation in the contractual obligations, again noting this ensures predictability of expectation for contracted parties, as well as providing ICANN with a minimal evidential threshold to enforce minimum standards. In this we also appreciate the efforts undertaken in creating the companion advisory document. Although not subject to this public comment process, we do note that it certainly provides additional clarity as to the interpretation of such minimum expectations relating to evidence. We furthermore appreciate how the advisory also outlines how a subjective assessment of the available actionable evidence shall remain a key factor in the assessment of the appropriateness of the actions to stop, or otherwise disrupt that abuse, at the DNS level. CleanDNS believes that such an evidence based approach is a strength of the proposed amendments, as it is key to not only ensuring strong, enforceable compliance, but is a key factor in assessing the appropriateness and non-arbitrariness of an action in any given circumstance.

Appropriate Mitigation

CleanDNS is also very appreciative of the fact that the amendments do not purport to prescribe specific mitigation actions. We strongly believe that different instances require different responses. Sometimes this may result in the direct suspension of a domain, other times, this may only result in a good faith effort to disrupt the abuse, e.g. initial escalation to a more appropriate party, whose intervention can more effectively address the abuse. This is simply to ensure an action taken, is done with as little collateral damage to the innocent users, as possible. For example, were the amendments drafted to include a positive obligation to suspend a domain based on evidenced use or persistent abuse associated with a domain name, this would have largely unwelcome consequences. For example, suppose a large social media platform, with a very broadly used domain name, finds its platform/service being consistently abused over time; assume also that such abuses are being widely reported and demonstrated by mass media and law enforcement alike. It could be easily argued that this coverage amounts to actionable evidence that the domain is therefore being consistently used for all myriad of abuse, DNS Abuse, content abuse etc. Would it be appropriate to expect the registry operator or registrar to 'suspend' that domain, and for ICANN to enforce that expectation? One must presume not. The proposed wording therefore, takes a much more purposive stance, and seeks only to enforce the minimum standard with reasonable and appropriate action, based on actionable evidence, and an assessment of impact.

Webforms

Finally, we also support the updating of the expectations relating to the inclusion of readily accessible webforms (and acknowledgement of receipt, onscreen or otherwise) as an alternative to email reports. A webform may represent a far more interactive, and indeed where properly created, a less abused and user friendly means by which a complainant may escalate their issue. We believe that the inclusion of webforms as an optional minimum expectation supports the better education of complainants. We believe this is a pragmatic and important step towards a more focussed collection and correlation of specific data elements pertinent to the report. Properly implemented forms can be a more scalable solution for contracted parties abuse reporting intake needs, and our experience has shown that they support both the better collection of contemporaneous evidence , as well encouraging clearer and more focussed reports. Webforms can also help define better and more efficient onward escalation of received reports, paving the way for a more standardised format for the escalation of such data to the appropriate parties.