

# Amendments to the Base gTLD RA and RAA

#  to Modify DNS Abuse Contract Obligations

Submitted July 20, 2023

These comments are submitted by the Intellectual Property Constituency (“IPC”), whose membership includes and represents trade associations, large multinational corporations, as well as small businesses and individuals.

The IPC applauds the efforts of ICANN and Contracted Parties to negotiate the proposed amendments to the Registrar Accreditation Agreement (“RAA”) and Base gTLD Registry Agreement (“RA”) to enhance Domain Name System (“DNS”) abuse mitigation. These amendments generally represent progress from requirements in the existing contracts.

Without taking away from the above sincere expression of appreciation for these efforts, and the IPC’s support for ratifying the proposed amendments, the IPC does wish to outline some areas where it believes additional improvements could be considered. These are discussed below and are reflected in the attached “cumulative redline” that contains additional suggested amendments integrated with the existing proposed amendments.

1. Defining “DNS Abuse”

The “DNS Abuse” definition used in the proposed RAA and RA amendments excludes certain activities that are generally recognized as illegal and harmful to consumers and Internet users generally under international and national laws, stemming from the misuse of intellectual property.  Accordingly, the definition of “DNS Abuse” should be expanded to include trademark infringement, counterfeiting, copyright infringement, and content piracy. Inclusion of these activities is important because, in addition to being harmful in their own right, they are also common vectors of achieving other forms of DNS Abuse identified in the current definition, including phishing and distribution of malware.

Including such activity within the DNS Abuse definition does not impermissibly constitute regulation of content by ICANN. As made clear by SAC115 (which ICANN points to as the “source” of the current DNS Abuse definition, even though the definition originates from the Voluntary Framework on DNS Abuse created by contracted parties), to determine whether a domain name is being used for malware, a registrar must examine the “software, installed and/or executed on a device …. [and determine that it] disrupts the device’s operations, gathers sensitive information, and/or gains access to private computer systems.” Similarly, to determine whether a domain name is being used for phishing a registrar must determine that an email or website content is being used to “tricks a victim into revealing sensitive personal, corporate, or financial information (e.g., account numbers, login IDs, passwords). SAC115 highlights that phishing is sometimes accomplished through sending fraudulent or “look-alike” emails (i.e., trademark infringement), or luring end-users to copycat websites (i.e., copyright infringement).

Furthermore, these activities have long been incorporated into the set of prohibited activities described in Specification 11, Section 3(a) of the RA.[[1]](#footnote-1)

Thus, excluding trademark infringement, counterfeiting, copyright infringement, and piracy from the DNS Abuse definition is a missed opportunity to further enhance protections for consumers and Internet users worldwide.

That said, rather than taking a prescriptive approach to defining DNS Abuse at all, the IPC proposes an alternative definitional approach that focuses on the ultimate harm to end users. Under this approach, the IPC suggests the following definition of “DNS Abuse”:

*“DNS Abuse” means any activity that makes, or intends to make, use of domain names, the Domain Name System protocol, or any digital identifiers that are similar in form or function to domain names to carry out deceptive, malicious, or illegal activity.[[2]](#footnote-2)*

The following context in the SAC115 report in relation to the DNS Abuse definition supports this alternative approach: “To be clear there are additional abuses that are worthy of discussion. SSAC finds some of the specific definitions limited, and the above do not provide a general definition of abuse that may accommodate the evolving natures of abuse and cybercrime over time.”

1. Webforms

The IPC appreciates that the use of webforms by registrars and registry operators can be used to helpfully streamline the abuse report intake and response process. On the other hand, webforms can be, and have been, used to prejudice reporters through things like very low character limits, inability to attach supporting documents, lack of receipt confirmations, and other drawbacks.

Therefore, the amendments permitting use of webforms for abuse reporting should incorporate explicit guardrails against these kinds of shortcomings. In particular, at a minimum, any webform reporting options should expressly require that the webform: (i) not impose unreasonable rate limits on submissions; (ii) allow users to submit attachments up to a reasonable file size limit; and (iii) send a confirmation of the form submission that includes the content of the report by email to the submitter.

Furthermore, we note that while the RA amendments already require prompt confirmation of receipt of reports (whether by email or webform), this same requirement does not appear to be carried over in the RAA amendments. This should be a commonsense addition to the current proposed RAA amendments.

1. Response Timeframes

The IPC appreciates that Contracted Parties need flexibility to prioritize DNS Abuse mitigation depending on various factors, such as the severity of harm stemming from a particular incident. Thus, while inclusion of the requirement that Contracted Parties take mitigation action “promptly” is helpful, some further guidelines or SLAs to cap response times would be helpful to ensure certain reports are not deprioritized to the point of untimeliness. The IPC suggests no more than 2 business days to confirm receipt of reports, and no more than 10 calendar days to respond substantively to non-LEA reports, absent extenuating circumstances.

1. Content of Responses

Without prescribing any particular form or content for substantive responses to abuse reports beyond what is required by the current amendments, the IPC notes that some reasonable level of consistency in terms of the kinds of information provided in responses would be helpful. For example, at a minimum, reporters should be informed of the specific mitigation action(s) taken as a result of the report. Sometimes, such action(s) may be obvious, but in other cases less so. Perhaps more importantly, though, if the registrar or registry operator determines that no action by them is appropriate in a particular case, they should have an obligation to report this to the abuse reporter with an explanation as to why no action is considered appropriate and to identify what other options the reporter has for addressing the reported abuse.

1. Registry Obligations

Under the current amendments, registry operators have an obligation to refer abuse reports to the registrar or can take direct action at their discretion. However, the amendments do not expressly account for a scenario where the registrar to whom such a report is referred fails to take appropriate mitigation action. While this may constitute a breach of the registrar’s obligations under the amendments, actionable through an ICANN Compliance complaint, pursuing a remedy through Compliance may not be sufficiently prompt to timely address the actual abuse. Therefore, the RA amendments should include an obligation for the registry to act if, after referring an abuse report to the registrar, the registrar fails to adequately act to mitigate the reported abuse.

1. Registrant Verification

The IPC notes that the current proposed amendments do not include any changes relating to registrant data accuracy verification obligations. In the IPC’s view, this is a missed opportunity, as enhanced registrant verification could be a meaningful abuse prevention and mitigation tool, and simultaneously would also help bring the RAA and/or RA more in line with the data accuracy provisions in the EU NIS2 Directive, which was adopted in December 2022.[[3]](#footnote-3) Such provisions could include requiring submissions of government issued identification documents, multi-factor authentication for access to accounts, and any additional information that a Contracted Party believes necessary or appropriate to ensure that domains registered with them (including in particular in bulk or with suspicious details) can be verified to meet the goal of preventing and/or mitigating abusive registrations and uses of abusively-registered domain names – frequently conducted by parties using false or inaccurate registration information.

1. Abuse Prevention

Along similar lines, while the proposed amendments should help *mitigate* DNS Abuse that is already occurring, the IPC believes more could be done in the agreements to help proactively *prevent* abuse. In addition to enhancements to accuracy verification, as discussed above, for example, where a registrar confirms multiple (e.g. 3 or more) incidents of abusive behavior perpetrated by the same registrant, the registrar should have an obligation to suspend or terminate the registrant’s account(s) and use commercially reasonable efforts to prevent the same registrant from creating new accounts or otherwise registering any additional domains with the registrar. Registrars should also maintain a shared “blacklist” of such registrants so that other registrars are aware of abusive registrants and can help identify and disrupt patterns of abusive registrations and registrar-hopping by such bad actors.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The IPC appreciates its role in the ICANN multi-stakeholder model and trusts that ICANN and Contracted Parties will take these comments into consideration as they pursue the proposed RAA and RA amendments. We look forward to engaging in further discussions and joint efforts to continue to achieve progress in the shared goal of minimizing DNS Abuse and protecting consumers and Internet users.

 Submitted on behalf of the IPC,



 Lori Schulman, President, IPC

1. See ICANN, Base gTLD Registry Agreement (last updated April 30, 2023), Specification 11, Section 3(a) available at https://itp.cdn.icann.org/en/files/registry-agreements/base-registry-agreement-30-04-2023-en.html (“Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.”) [↑](#footnote-ref-1)
2. This definition has been adopted by the International Trademark Association (INTA), through a resolution of its Board of Directors on May 16, 2023. See https://www.inta.org/wp-content/uploads/public-files/advocacy/board-resolutions/INTA-Board-Resolution-on-Domain-Name-System-Abuse-May-2023.pdf. [↑](#footnote-ref-2)
3. See European Parliament, Directive (EU) 2022/2555 (Dec. 27, 2022), art. 28, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555: “For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall require TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with Union data protection law as regards data which are personal data. For the purposes of paragraph 1, Member States shall require the database of domain name registration data to contain the necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs…. Member States shall require the TLD name registries and the entities providing domain name registration services to have policies and procedures, including verification procedures, in place to ensure that the databases referred to in paragraph 1 include accurate and complete information. Member States shall require such policies and procedures to be made publicly available.” [↑](#footnote-ref-3)