SSAC
ICANN Security and Stability
Advisory Committee

18 July 2023

Subject: SSAC2023-14: SSAC Public Comment on Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations

Background

This correspondence provides comments from the ICANN Security and Stability Advisory Committee (SSAC) on the Proposed Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations.[1]

The SSAC wishes to thank and commend the contracted parties and ICANN org staff for their initiative and efforts to address DNS Abuse by updating relevant contracts to include enforceable provisions and obligations for contracted parties. We look forward to seeing them implemented and further evolved over time. The SSAC would like to see the vision contemplated in the background information provided in this public comment request:

> *Taking this approach … is an important building block in a longer journey that could include policy discussions open to the full ICANN community, and potentially future negotiations between the CPH and ICANN org. Further policy development could also be pursued in the Generic Names Supporting Organization (GNSO) to broaden the examination of what additional obligations should exist and define in more detail what is expected of registrars and registry operators in a community-wide process.*

Per its role, the SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), administrative matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). The SSAC engages in threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate.

[1] See Public Comment on Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations, https://www.icann.org/en/public-comment/proceeding/amendments-base-gtld-ra-raa-modify-dns-abuse-contract-obligations-29-05-2023

SSAC Comments

Comment 1: On the topic of the overall goal to "enhance obligations by requiring registrars and registry operators to promptly take reasonable and appropriate action to stop or otherwise disrupt DNS Abuse," the SSAC enthusiastically supports this aim and effort. This aligns with prior SSAC advice as well as advice from many other SO/ACs in the ICANN community.

The SSAC would encourage all parties to work diligently during the implementation phase of these new amendments to ensure that the overall goals are met, and measurable progress can be made towards the goals of reducing DNS Abuse. The SSAC observes that measurement against goals requires data collection and reporting, and that these implementation issues will be critical to the success of this initiative. The SSAC would appreciate the community being kept up-to-date on implementation of these amendments and how ICANN Org will measure progress against overall goals.

Comment 2: The definitions of DNS Abuse in the proposed contractual language reference SAC115. The SSAC appreciates being cited as a reliable source for such a definition. However, we note that the definition in SAC115 is not a definition of DNS abuse originated, or adopted, by the SSAC itself, but rather, a synthesis of multiple definitions adopted for discussion purposes within the scope of SAC115. The cited definitions are the outcomes of much work and of multi-stakeholder processes, not only by the SSAC.

In particular, the proposed new contractual language states:

> *For the purposes of the proposed amendments, DNS Abuse means malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse, namely, malware, botnets, phishing, and pharming) as those terms are defined in Section 2.1 of the Security and Stability Advisory Committee Report on an Interoperable Approach to Addressing Abuse Handling in the DNS (SAC115).*[2]

For clarity, Section 2.1 of SAC115[3] does not contain SSAC's definitions of abuse, and the proposed contract definitions of abuse are not endorsed by SSAC. SAC115 Section 2.1 quoted, for discussion and illustration purposes, definitions from the Contracted Parties' DNS Abuse Framework and the Internet and Jurisdiction Policy Network's "Operational Approaches, Norms,

[2] See 3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse, Proposed Redline 2013 Registrar Accreditation Agreement, 29 May 2023, https://itp.cdn.icann.org/en/files/registry-agreement/proposed-redline-2013-registrar-accreditation-agreement-29-05-2023-en.pdf

[3] See SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS, https://www.icann.org/en/system/files/files/sac-115-en.pdf

Criteria, Mechanisms" document. SAC115 stated a qualification about those definitions: "To be clear there are additional abuses that are worthy of discussion. SSAC finds some of the specific definitions [in section 2.1] limited, and the above do not provide a general definition of abuse that may accommodate the evolving natures of abuse and cybercrime over time."

Comment 3: Part of the proposed contractual language appears to be internally inconsistent, and may need modification or clarification. SAC115 Section 2.1 states that spam is "unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content."

Since this term is "defined in" SAC115 section 2.1, that definition of spam is apparently incorporated by reference in the agreements. However, the contract revisions also define spam as something more narrow: only "when spam serves as a delivery mechanism for the other forms of DNS Abuse listed in this Section." The new contractual language therefore could be interpreted to define spam in two different ways, and could thus be confusing.