Background: Around 2019, different parts of the ICANN community, including the GAC, started to focus on the issue of DNS Abuse and what more ICANN could require of domain name registries and registrars (the "Contracted Parties"). The Contracted Parties ultimately volunteered to negotiate new obligations with ICANN relating to DNS abuse. In late 2022, the Contract Parties wrote to ICANN requesting negotiations to update the contracts, which began in 2023 and concluded in time for ICANN77. On May 29, 2023, ICANN published the updated contracts for Public Comment, along with a 15-page draft **Advisory**, which provides guidance on the interpretation of, and compliance with, the new requirements. The new requirements "are based on the actions that registrars and registry operators, respectively, can take to minimize the scope and intensity of the harm and victimization caused by DNS Abuse."[1] Comments are due on 13 July 2023.

The Contracts: Amendments are proposed to **Section 3.18** of the Registration Accreditation Agreement (RAA), between ICANN and gTLD domain name registrars; and **Specification 6, Section 4** of the Registry Agreement (RA) between ICANN and gTLD domain name registries.

DNS Abuse: For the purposes of the RAA and the RA, "DNS Abuse means malware, botnets, phishing, pharming, and spam (when spam is used as a delivery mechanism for any of the other four types of DNS Abuse)."[2]

The Amendments: "ICANN has the authority to enforce rules related to domain name registration services and domain names as outlined in the RAA and the RA."[3] The basic rules are outlined below:

- RAA: On its website, Registrar (Rr) provides the means to submit reports of DNS Abuse at a registered name; Rr confirms receipt; and if report is actionable, then the Rr must promptly act to stop or otherwise disrupt the Registered Name from being used for DNS Abuse.
- RA: On its website, Registry (Ry) provides the means to submit reports of DNS Abuse in a Top Level Domain; Ry confirms receipt; and if report is actionable, then the Ry must promptly act to contribute to stopping, or otherwise disrupting, the domain name from being used for DNS Abuse including by 1) referring the report to the Rr or, Ry thinks it would be appropriate, or 2) taking direct action.

Attachments:

1. Questions for Discussion and Consideration in preparing the draft GAC Public Comment on DNS Abuse Contract Amendments
2. Description of DNS Abuse categories
3. RAA redlines
4. RA redlines
5. Resources

---

[1] Draft ICANN Advisory DNS Abuse Amendments

[2] See definitions cited in *The Framework to Address Abuse*, http://dnsabuseframework.org/ and the Internet and Jurisdiction Policy Network's *Operational Approaches, Norms, Criteria, Mechanisms* https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf

[3] Ibid.

ATTACHMENT 1

Questions for Discussion and Consideration in preparing the draft GAC Public Comment on DNS Abuse Contract Amendments

NOTE: This is not intended as exhaustive list

1. What are the positive aspects of these amendments?
2. Are the obligations sufficiently clear to be enforceable?
3. Thoughts on the proposed definition of DNS Abuse?
4. Thoughts on the role of the ICANN Advisory on the amendments?
    a. Intended to be an evolving document?
    b. Sufficiently informative as to:
        i. What is "actionable evidence"?
        ii. When is action "prompt"?
        iii. When the registry should forward a referral v. take direct action.
5. What issues remain with regard to DNS Abuse?
    a. What subject matter areas may be appropriate for the planned PDPs?
    b. Before the next round of new gTLDs?
    c. The role of Public Interest and Registry Voluntary Commitments?
    d. Priority/ideal timing for these issues?
6. Other issues?

ATTACHMENT 2

Description of DNS Abuse categories

Malware is malicious software, installed and/or executed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.

Botnets are collections of Internet-connected computers that have been infected with malware and can be commanded to perform activities under the control of a remote attacker.

Phishing occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g., account numbers, login IDs, passwords), whether through sending fraudulent or look-alike emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install malware.

Pharming is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking can occur when attackers use malware to redirect victims to the perpetrator's site instead of the one initially requested. DNS poisoning causes a DNS server (or resolver) to respond with a false Internet Protocol address bearing malware. Phishing differs from pharming in that pharming involves modifying DNS entries, while phishing tricks users into entering personal information.

Spam is unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message is sent as part of a larger collection of messages, all having substantively identical content. Spam is only considered to be DNS Abuse when it is being used as a delivery mechanism for at least one of the other types of DNS abuse described above.

ATTACHMENT 3

RAA Amendments

3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse.

3.18.1 Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of DNS Abuse and Illegal Activity. Registrar shall publish an email address or webform to receive such reports on, or conspiculously and readily accessible from, the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time). Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse. For the purposes of this Agreement, "DNS Abuse" means malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse listed in this Section) as those terms are defined in Section 2.1 of SAC115 (<https://www.icann.org/en/system/files/files/sac-115-en.pdf>).

3.18.2 When Registrar has actionable evidence that a Registered Name sponsored by Registrar is being used for DNS Abuse, Registrar must promptly take the appropriate mitigation action(s) that are reasonably necessary to stop, or otherwise disrupt, the Registered Name from being used for DNS Abuse. Action(s) may vary depending on the circumstances, taking into account the cause and severity of the harm from the DNS Abuse and the possibility of associated collateral damage.

~~3.18.2~~3.18.3 Registrar shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which Registrar is established or maintains a physical office. Well-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report. In responding to any such reports, Registrar will not be required to take any action in contravention of applicable law.

ATTACHMENT 4

RA Amendments

4. **Abuse Mitigation**

4.1. **Abuse Contact**. Registry Operator shall provide to ICANN and publish on its website its accurate contact details including a valid email address or webform and mailing address as well as a primary contact for handling ~~inquiries~~reports related to malicious conduct in the TLD, including DNS Abuse, and will provide ICANN with prompt notice of any changes to such contact details. Upon receipt of such reports, Registry Operator shall provide the reporter with confirmation that it has received the report.

For the purposes of this Agreement, "DNS Abuse" is defined as malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse listed in this Section) as those terms are defined in Section 2.1 of SAC115 (<https://www.icann.org/en/system/files/files/sac-115-en.pdf>).

4.2. **DNS Abuse Mitigation**. Where a Registry Operator reasonably determines, based on actionable evidence, that a registered domain name in the TLD is being used for DNS Abuse, Registry Operator must promptly take the appropriate mitigation action(s) that are reasonably necessary to contribute to stopping, or otherwise disrupting, the domain name from being used for DNS Abuse. Such action(s) shall, at a minimum, include: (i) the referral of the domains being used for the DNS Abuse, along with relevant evidence, to the sponsoring registrar; or (ii) the taking of direct action, by the Registry Operator, where the Registry Operator deems appropriate. Action(s) may vary depending on the circumstances of each case, taking into account the severity of the harm from the DNS Abuse and the possibility of associated collateral damage.

~~4.2~~4.3. **Malicious Use of Orphan Glue Records**. Registry Operator shall take action to remove orphan glue records (as defined at https://www.icann.org/en/committees/security/sac048.pdf) when provided with evidence in written form that such records are present in connection with malicious conduct.

ATTACHMENT 5

Resources

- Webinar 1: Pre-ICANN77 GAC Capacity Development Webinar on DNS abuse #1 - 4 May 2023
- Webinar 2: Pre-ICANN77 GAC Capacity Development Webinar on DNS abuse #2 - 22 May 2023
- GAC Statement on DNS Abuse
- ICANN77 Policy Briefing, DNS Abuse excerpt (requires GAC login)
- Internet & Jurisdiction slides from ICANN76 on DNS Abuse
- Contracted Party House's Framework to Address DNS Abuse