DNS Abuse Negotiation: CPH Outreach Session

13 June 2023

Agenda

- Welcome
- Background and Scope of Amendment Discussions
- Review of the DNS Abuse Contract Amendments
- DNS Abuse Mitigation
- The Global Amendment Procedures
- Q&A

Public Comment Period now live!

- Proposed changes to the RAA, Section 3.18
- Proposed changes to the RA, Specification 6, Section 4 and Specification 11 3(b)

A supporting document: Draft ICANN Advisory which helps provide expectations for compliance with the proposed obligations

DNS Abuse Contract Amendments

Background

How did we get here?

The Contracted Parties:

- → appreciating an absence of strong ‘enforceable’ obligations to mitigate or disrupt DNS Abuse in the RA and RRA;
- → paying all due regard to the substantial ICANN Community discussion and stakeholder inputs seeking stronger DNS Abuse response;
- → building off of 10+ years of work, both within and outside the ICANN sphere in refining DNS Abuse approaches in the gTLD space;
- → accepting that policy development alone may struggle with the current contractual language;

used the opportunity afforded to us, by the GNSO Small Team on DNS Abuse, resolved to take firm practical steps to evolve our approach to DNS Abuse.

How did we get here?

Contracted Parties proposed a 2 stage process:

Step 1 : Contractual Changes

- Needed to be meaningful & enforceable: raise the floor
- Expediently close the gap: create obligation to mitigate DNS Abuse
- Scope: DNS Abuse as previously defined by CPH, No Registration Data disclosure topics, no pass through obligations

Step 2: Community Driven Process

- Acknowledging how vital the work of the Multistakeholder Policy Development Process, the full involvement of the ICANN Community in shaping homogeneous policy expectations on DNS Abuse was established as a key step in this effort.
- A strong scaffold of enforceable contractual obligations, was a prerequisite to ensure enhanced and consistent ICANN compliance enforcement opportunities.
- Enhance ICANN policy with community driven, targeted and distinct policy development processes.
- PDPs must be grounded with clear practical goals in support of DNS Abuse disruption and mitigation.

Guiding Principles in the Resulting Amendments

- Focus on the target outcome of stopping or disrupting the use of gTLD domain names for DNS Abuse
- Registrars and Registries must take prompt action to mitigate when domain name(s) is being used for DNS Abuse
- DNS Abuse is highly contextual: the circumstances of each case are critical to determining the best approach to mitigate
- Registrars and Registries need discretion for what action to take
  - Proportionality and collateral damage must be taken into consideration
- Recognize the different roles between Registrars and Registries

DNS Abuse Amendments

Registrar Obligations

Existing RAA DNS Abuse Contractual Obligations

- **Under Section 3.18 of the RAA, registrars are required to:**
  - Take reasonable and prompt steps to investigate and respond appropriately to abuse reports.
  - Maintain a dedicated point of contact (monitored 24/7) for reports of illegal activity filed by law enforcement, consumer protection, quasi-governmental or similar authorities within the registrar's jurisdiction. Review well-founded reports submitted by these authorities within 24 hours.
  - Publicly display abuse contact information and abuse report handling procedures.
  - Maintain records related to the receipt of and response to abuse reports and provide these records to ICANN upon reasonable notice.

Proposed Registrar Obligations

- Adds to existing obligations in RAA Section 3.18
- Clarifies Registrar's abuse contacts are readily accessible
- Adds a requirement for registrar to provide confirmation of receipt of an abuse report
- Adds a definition of DNS Abuse for purpose of the agreement
- Adds new section 3.18.2 - obligation to take mitigation action to stop or disrupt DNS Abuse.

Proposed RAA Obligations: Reporting Abuse to a Registrar

Requirements to clarify abuse contacts are readily accessible on the home page and to produce receipt confirmation for reporters upon receipt of abuse reports. (RAA 3.18.1)

- **Where to report abuse**

  The registrar must publish an email address or web form that is readily accessible on the homepage of the registrar's website. Web forms must not require a login to submit abuse reports.

- **Registrar Must Provide a Confirmation of Receipt of a Report of Abuse**

  At a minimum, the receipt confirmation must identify the registrar, the reported Registered Name(s), and the date the report was submitted.

- **Contacts for Law Enforcement Agencies**

  No changes made. The requirements related to contacts dedicated to receiving reports from Law Enforcement Agencies (LEA) and other authorities within the registrar's jurisdiction previously described in Section 3.18.2 of the RAA are now in RAA Section 3.18.3;

Proposed RAA Obligations: Definition of DNS Abuse

A definition of DNS Abuse for purposes of the RA and RAA.

For the purpose of the RAA, RA, and draft Advisory, *DNS Abuse* means:

- Malware
- Botnets
- Phishing
- Pharming
- Spam, when spam serves as a delivery mechanism for the other forms of DNS Abuse listed

As those terms are defined in Section 2.1 of SAC115.

Proposed RAA Obligations: Take Mitigating Actions

New: 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.

DNS Abuse Amendments

Registry Obligations

Existing RA DNS Abuse Contractual Obligations

- **Under Section 4, Specification 6 of the RA, registry operators are required to:**
  - Publish and provision to ICANN, contact details for handling inquiries related to malicious conduct in the TLD.
  - Remove orphan glue records when used in connection with malicious conduct.

Existing RA DNS Abuse Contractual Obligations

- **Under Section 3(a) and 3(b), Specification 11 of the RA, registry operators are required to:**
  - Include a provision in their agreement with registrars to prohibit registrants from engaging in certain activities, and requiring consequences for the registrants for such activities, including suspension of the domain.
  - Periodically conduct a technical analysis to assess whether domains in their gTLD are being used to perpetrate security threats.
  - Maintain statistical reports on the number of security threats identified, including the actions taken as a result of the periodic security checks, and to provide copies of these reports to ICANN upon request.

Proposed RA Obligations: Reporting Abuse to a Registry

Requirements Relating to the Publication and Maintenance of Abuse Contacts (Base RA Specification 6 Section 4.1).

- **Where to Report Abuse**
  The registry operator must publish an email address or web form, a mailing address, and a primary contact for handling such reports.

  A registry operator's homepage which clearly displays a link to a "Report Abuse'' or a "Contact Us" page (which clearly includes the abuse contact) where submission of reports is unimpeded will be deemed compliant.

- **Registry Must Provide a Confirmation of Receipt of a Report of Abuse**
  At a minimum, the receipt confirmation must identify the registry operator, the reported Registered Name(s), and the date on which the report was submitted.

.

Proposed RA Obligations: Definition of DNS Abuse

A definition of DNS Abuse for purposes of the RA and RAA.

For the purpose of the RAA, RA, and draft Advisory, *DNS Abuse* means:

- Malware
- Botnets
- Phishing
- Pharming
- Spam, when spam serves as a delivery mechanism for the other forms of DNS Abuse listed

As those terms are defined in Section 2.1 of SAC115.

Proposed RA Obligations: Take Mitigating Action

New Specification 6 Section 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.

Proposed RA Obligations: Update to Spec 11 3(b)

Specification 11 3(b) - replaces the term "security threats" with the defined term DNS Abuse.

- Clarifies the technical analysis is done to assess whether domains in their gTLD are being used to perpetrate DNS Abuse
- Clarifies the statistical reports are for identified DNS Abuse
- More clearly defines what is to be analyzed and reported

DNS Abuse Mitigation Techniques and Considerations

Mitigation Actions to Stop or Disrupt DNS Abuse

- Mitigation is not a one size fits all approach
- Available actions for Registrars and Registries:
  - **Suspend** the Domain Name: Stops the name from resolving, disables associated services such as email; reversible
    - Client Hold (Registrar) / Server Hold (Registry)
  - **Contact the Registrant or Hosting Provider**: Inform them of issue, support them to remediate; particularly for cases of “compromised websites”
  - **Delete** the Domain Name from the zone: Stops the name from resolving, disables associated services such as email
  - **Lock** the Domain Name: Prevents transfering, changing details, or deleting
  - **Redirect**: changing the nameservers, usually to log traffic and identify & help victims
  - **Escalation** of actionable evidence to a party more proximate to the abuse (e.g. registry escalation to registrar in cases of compromise so as to prevent collateral damage)

Compromised Domains and Collateral Damage

- **Collateral damage** is an important consideration when acting at the DNS level, even when dealing with DNS Abuse.
- This is particularly important when an otherwise legitimate or benign domain name is used as a vector for DNS Abuse without the knowledge or consent of the registrant. This is often referred to as a "**compromised domain**."
- In these compromise situations, direct suspension of the domain may not be the appropriate mitigation, as suspension will cut off access to all legitimate content as well as render any associated email and other services with the domain inaccessible.
- This is also the case when the DNS Abuse is associated with a **third-level or subdomain**. Registrars and registries can only act at the second-level domain level. If the second-level name is suspended, all third-level domains would be suspended as well.
- In these situations, a registrar might elect to provide notification to the registrant, site operator, and/or web host.

Expectations and Enforcement

Draft Advisory

ICANN Advisory

The draft ICANN Advisory would come into effect if the proposed amendments are approved. The draft Advisory:

- Describes the new requirements and provide clarity on the implementation and enforcement of such requirements.
- Expands upon terms like *mitigation actions*, *stop,* and *disrupt*, and describe (with examples) how the appropriateness and promptness of the actions may vary depending on the circumstances of each specific instance of DNS Abuse.
- Provides details regarding the review ICANN Contractual Compliance will conduct before initiating a case with a contracted party under the new requirements, and expectations for contracted parties' actions and responses to compliance cases.

How Will ICANN Contractual Compliance Enforce the Proposed New Obligations?

- ICANN Contractual Compliance will enforce the new requirements through the processing of external complaints, proactive monitoring, and audit activities.

- ICANN Contractual Compliance will review all available information and records relevant to a specific case and domain names(s) to determine whether to initiate a compliance case under the new requirements with a registrar or registry operator.

- When initiating a compliance case with a registrar or registry operator, ICANN Contractual Compliance will provide an itemized list of all the information and records needed to assess compliance. This will include an explanation of and supporting records related to:
  - How and why the registrar or registry operator determined that the evidence obtained was not actionable, where applicable.
  - The specific mitigation actions taken, and how these actions were prompt and reasonably necessary to stop or to disrupt or to contribute to stopping or disrupting, as it pertains to the specific circumstances of the case (including any applicable explanation relating to disproportionality of actions at the DNS level and collateral damage).

Next Steps: The Global Amendment Procedures

Global Amendment Procedure

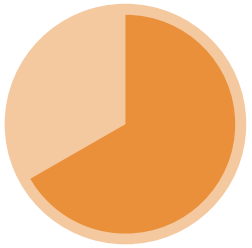
Utilizing the Global Amendment procedures to update both the RA and RAA

- The same process was used for the:
  - 2017 Global Amendment to the Base RA
  - 2023 Global Amendments to the Base RA and 2013 RAA for Registration Data Access Protocol (RDAP)
- For registries that are not a party to the Base RA, additional steps will be required including additional negotiation with those registries to include the proposed changes into the respective registry agreements.
  - Both .COM & .NET (proposed) have provision to adopt the result of global amendment for DNS Abuse via the LOI

Registry Operator Voting Approval Thresholds

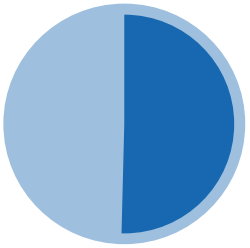
Registry Operator Approval - Voting results must reach the following two (2) thresholds as defined by base RA Section 7.6 (j) (ii):

1. The affirmative approval of **Applicable Registry Operators whose payments to ICANN accounted for two-thirds of the total amount of fees paid**, pursuant to the Registry Agreement, the immediately previous calendar year.



+

2. The affirmative approval of a **majority (over 50%)** of the Applicable Registry Operators at the time such approval is obtained.

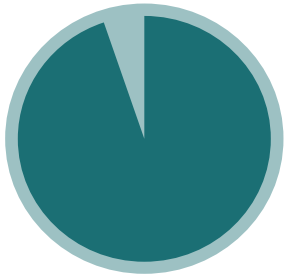


Registrar Voting Approval Thresholds

Registrar Approval - voting result must reach the following threshold as defined by Section 1.18.1 of the Registrar Accreditation Agreement (RAA):

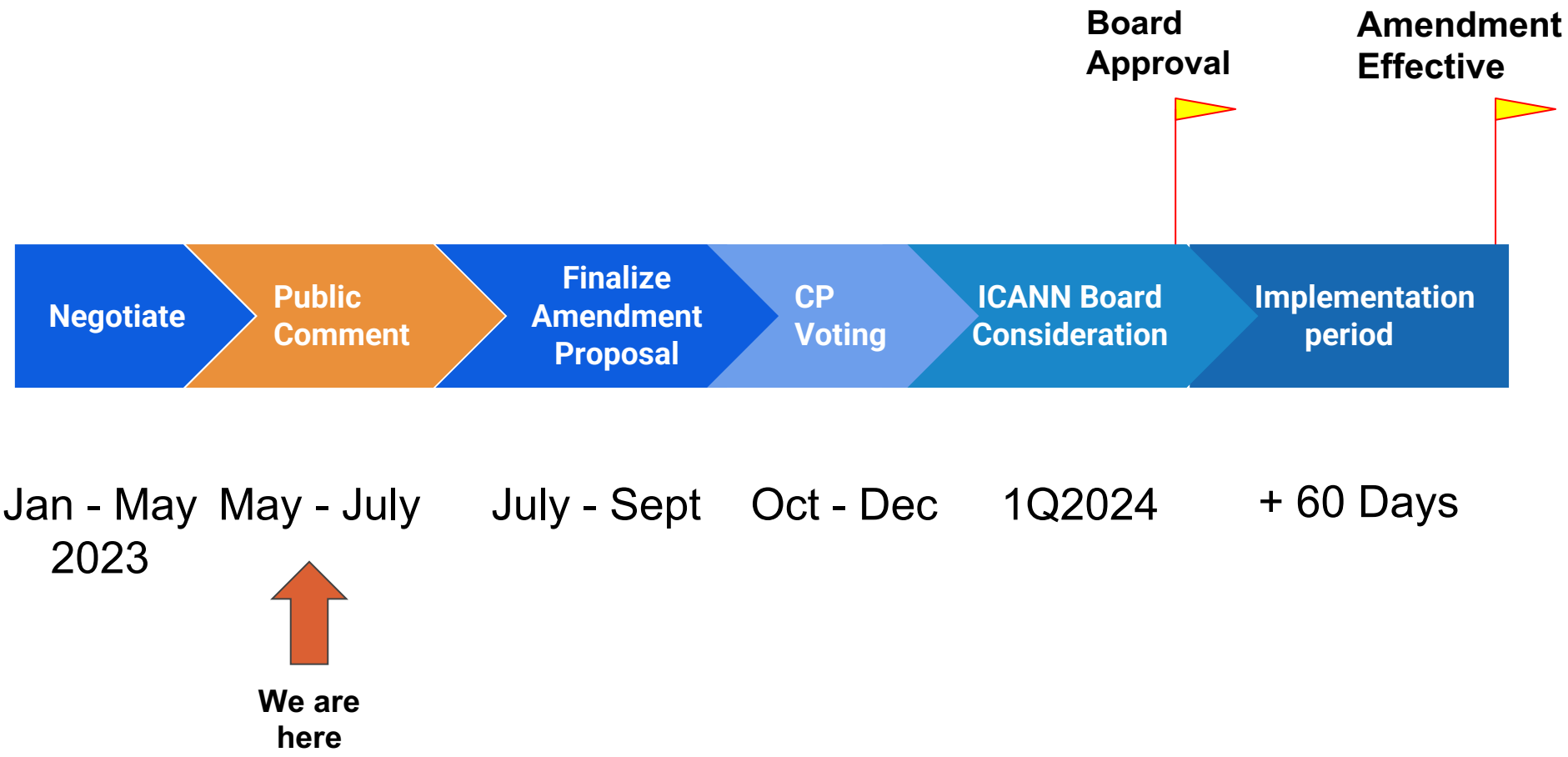
- The affirmative approval of **Applicable Registrars accounting for 90% of the total registered domain names under management (TDUMs)* as calculated** pursuant to Section 1.18.1:

  The DUM count for the 5th largest applicable registrar family will replace the DUM count for the top four (4) registrar families - **meaning more applicable registrars overall must vote in the affirmative to reach the 90% threshold.*



- The final calculation for registrar voting weight will be based on the most recent Per-Registrar Transactions Report available prior to the conclusion of the voting period.

DNS Abuse Proposed Amendments Procedure Timeline



Q&A