ICANN 79 | COMMUNITY FORUM

Enforcement of the DNS Abuse Requirements in the RAA and the Base RA

ICANN79 Community Forum

ICANN Contractual Compliance

02 - 07 March 2024
Centro de Convenciones de Puerto Rico

Agenda

- Requirements in effect before and after 5 April 2024 in the Registrar Accreditation Agreement (RAA)
- Requirements in effect before and after 5 April 2024 in the Base Registry Agreement (RA)
- ICANN Contractual Compliance's Enforcement of DNS Abuse Requirements.
  - Team and System Readiness.
  - Process.
- ICANN Contractual Compliance's Reporting on the Enforcement of DNS Abuse Requirements.

Requirements in effect before and after 5 April 2024 – RAA

EXISTING RAA OBLIGATIONS (RAA 3.18)

- 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 and other 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.

VS

RAA OBLIGATIONS AFTER 5 APRIL 2024 (RAA 3.18)

- Take prompt and appropriate mitigation action to stop or disrupt the Registered Name from being used for *DNS Abuse* when the registrar has actionable evidence.
- 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 and other 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. Registrars may use a webform instead of email to collect abuse reports. Registrars must confirm receipt of an abuse report.
- Maintain records related to the receipt of and response to abuse reports and provide these records to ICANN upon reasonable notice

Requirements in effect before and after 5 April 2024 – Base RA

EXISTING BASE RA OBLIGATIONS

- Publish and provision to ICANN contact details for handling inquiries related to malicious conduct in the top-level domain (TLD). Specification 6
- Remove orphan glue records when used in connection with malicious conduct. Specification 6
- 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. Specification 11. 3(a)
- Periodically conduct a technical analysis to assess whether domains in their gTLD are being used to perpetrate security threats. Specification 11.3(b)
- 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. Specification 11.3(b)

VS

BASE RA OBLIGATIONS AFTER 5 APRIL 2024

- Take prompt and appropriate mitigation action to contribute to stopping or disrupting the Registered Name from being used for *DNS Abuse* when the registry has actionable evidence. Specification 6
- Publish and provision to ICANN contact details for handling inquiries related to maliciuos conduct in the TLD, including DNS Abuse. Registries may use a webform instead of email to collect abuse reports. Registries must confirm receipt of a DNS Abuse report. Specification 6
- Remove orphan glue records when used in connection with malicious conduct. Specification 6
- 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. Specification 11. 3(a)
- Periodically conduct a technical analysis to assess whether domains in their gTLD are being used to perpetrate DNS Abuse. Specification 11.3(b)
- Maintain statistical reports on the number of identified DNS Abuse, including the actions taken as a result of the periodic security checks, and to provide copies of these reports to ICANN upon request. Specification 11.3(b)

Enforcement of DNS Abuse Requirements - Team & System Readiness

ICANN Contractual Compliance is taking multiple actions to prepare:

- A dedicated team of processors who are structured for expertise and training across multiple areas of the ICANN policies and agreements
- An internal, robust, knowledge base and training materials that will include a library of cases illustrating different scenarios linked to compliant and noncompliant actions
- Dedicated webforms to receive complaints from external users
- A case processing system equipped to process and monitor complaints, and to capture granular data to report to the community on the complaints received and related enforcement action

Enforcement of DNS Abuse Requirements - Process

- As explained in the Advisory, ICANN Contractual Compliance will process complaints alleging DNS Abuse through ICANN's established compliance process.
  - Once valid complaint triggers the process to request the contracted party to provide evidence of compliance
  - The process comprises two stages: an informal and a formal resolution stage.
  - The process may result in the termination or suspension of the accreditation of a noncompliant registrar, or the termination of the RA of a noncompliant registry operator.

- ICANN Contractual Compliance will continue validating compliance across all ICANN policies and agreements through proactive monitoring and an established Audit Program.
  - Compliance with DNS Abuse obligations will be included in the Audit Program. The Program generally entails two audit rounds per year.

- ICANN Contractual Compliance will use the data and experience garnered through the enforcing of the DNS Abuse requirements to continue participating in ICANN's multifaceted efforts to help combat DNS Abuse, including through the provision of data and information.

Reporting on the Enforcement of DNS Abuse Obligations

- ICANN Contractual Compliance maintains a dedicated page with Metrics and Dashboards. Audit reports including scope, testing approach, and key results are also published.

- The introduction of data related to the enforcement of the new DNS Abuse requirements in Compliance's metrics and reporting publications will include the number of:

  - Complaints received broken-down by type of DNS Abuse: Phishing; Malware; Botnets; Pharming; and Spam as a delivery mechanism for the other forms of DNS Abuse.`

  - Cases resolved with contracted parties (CPs) and their outcome, including:
    - Whether the CP took mitigation actions to stop or to disrupt,
    - What type of action was taken; or
    - Whether no action was taken due to lack of actionable evidence.

  - Cases resolved with CPs that were submitted by law enforcement and other authorities within the jurisdiction in which registrar is established or maintains a physical office.

- ICANN Contractual Compliance will continue reporting on existing abuse-related obligations.

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg