



82 | COMMUNITY FORUM



Program Update

ICANN Contractual Compliance



ICANN82 Prep Week
24 February 2025

Agenda

Program Update:

- Introduction
- Enforcement of DNS Abuse Mitigation Requirements
- Enforcement of the Registration Data Access Protocol (RDAP) requirements
- Contractual Compliance Audit
- Support of Policy and Working Groups Efforts and Other Community Initiatives

Questions and Answers

ICANN Contractual Compliance - Introduction

Jamie Hedlund

SVP, Contractual Compliance & U.S. Government Engagement

ICANN Contractual Compliance Program Update

ICANN82 Prep Week

24 February 2025



ICANN Contractual Compliance (“Compliance”) enforces the obligations in ICANN’s agreements with generic top-level domain (gTLD) registry operators and registrars and the community-developed policies incorporated into those agreements. Compliance ensures all obligations are implemented to preserve and enhance the security, stability and resiliency of the Domain Name System (DNS).

- Enforcement actions arise from external complaints, proactive monitoring and audit-related activities.
- Compliance produces, publishes and maintains [metrics and data](#) on complaints received and enforcement actions to help inform community discussions.
- Compliance supports policy and working groups’ efforts by providing data and input regarding enforcement and enforceability of obligations.
- Compliance participates in training and outreach sessions to increase awareness regarding contractual obligations among the community.

Enforcement of DNS Abuse Mitigation Requirements

Rómulo Chacín

Contractual Compliance Analyst

Leticia Castillo

Senior Director, Contractual Compliance

ICANN Contractual Compliance Program Update

ICANN82 Prep Week

24 February 2025



Enforcement of DNS Abuse Mitigation Requirements

On 5 April 2024, Compliance began enforcing the new DNS Abuse requirements applicable to gTLD registry operators and ICANN-accredited registrars.

These requirements added to the prior abuse-related RAA and RA obligations by:

- Including a definition of DNS Abuse for the purpose of the Registrar Accreditation Agreement (RAA) and the Base Registry Agreement (RA):
Malware, botnets, phishing, pharming, and spam (when used as a delivery mechanism for DNS Abuse) as defined in [SAC 115](#).
- Requiring mitigation actions to stop or disrupt well-evidenced DNS Abuse.
- Clarifying that abuse contacts must be readily accessible.
- Requiring the provision of receipt confirmation of abuse reports to reporting parties.

ICANN issued an [Advisory](#) that provides guidance on the interpretation of and compliance with the new requirements.

Enforcement of DNS Abuse Mitigation Requirements

From 5 April 2024 through 5 December 2024, Compliance:

- Initiated 249 DNS Abuse investigations with registrars and registry operators.
- Issued formal Notices of Breach to one [registry operator](#) and one [registrar](#) for failure to comply with DNS Abuse mitigation requirements. A new [Notice of Breach](#) to a registrar was issued on 5 February 2025.
- Resolved 204 DNS Abuse mitigation investigations that resulted in the suspension of over 2,900 domain names and the disabling of over 365 phishing websites.
- Began publishing detailed monthly [reports](#) dedicated to the enforcement of DNS Abuse mitigation requirements.
- Participated in multiple forums and discussions related to raising awareness of DNS Abuse requirements in the RAA and RA.
- Prepared an audit to validate registry operators' compliance with RA requirements, including DNS Abuse.

Enforcement of DNS Abuse Mitigation Requirements

Notices of Breach

- On 16 July 2024, ICANN issued a Notice of Breach to a registry operator for failure to comply with DNS Abuse mitigation requirements in Specification 6, Section 4.2 of the RA.
- On 20 September 2024 and on 5 February 2025, respectively, ICANN issued a Notice of Breach to two registrars for these registrars' failure to comply with DNS Abuse mitigation requirements in Section 3.18.2 of the RAA.
- Per the agreements, Notices of Breach to registrars include a 21-day deadline to cure, while Notices of Breach to registry operators allow a 30-day window to cure the noncompliance.
- The three Notices of Breach continue to be effective. The deadlines to cure have been extended while the contracted parties implement remedial measures.

Enforcement of DNS Abuse Mitigation Requirements

The deadline to cure a Notice of Breach is extended if before the deadline:

- Mitigation actions have been taken on all abusive domain names. No extensions are granted if the abusive domain names identified within the case leading to the Notice of Breach continue to be active and prolonging the exposure of potential victims to the DNS Abuse.
- The registrar or registry operator has presented a remediation plan and demonstrated that the different stages of the plan are being implemented.
- The plan's timelines are reasonable, considering the modifications and enhancements being made in processes, systems, and/or tools.
- ICANN requires additional time to review and, where applicable, test different stages of the plan, communicate feedback, and request further information and/or action.

Enforcement of DNS Abuse Mitigation Requirements

What is Next?

Ongoing Enforcement & Reporting

- Continued processing of complaints, ensuring they are addressed within the established process. Regular reporting on enforcement actions.

Audits & Key Findings

- Ongoing work on the registry audit, with a report to be published upon completion.
- Designing of a new registrar audit round that will incorporate DNS Abuse mitigation requirements.

Facilitating Complaint Submissions

- Advancing initiatives to streamline the complaint submission process for, and exchange of information with, external reporters.

Proactive Investigations & Enforcement

- Designing of an approach to proactively initiate investigations and enforcement actions related to DNS Abuse.

Enforcement of RDAP Requirements

Amanda Rose

Senior Registrar Compliance Lead

ICANN Contractual Compliance Program Update

ICANN82 Prep Week

24 February 2025



RDAP Requirements

As of 3 February 2024 - Registrars and Registry Operators must be in compliance with all RDAP requirements, including:

- [RDAP Response Profile](#) and Technical Implementation Guide
 - Until 21 August 2025, **must** implement **either** Feb-2019 versions or Feb-2024 versions
 - By 21 August 2025, **must** implement Feb-2024 versions
- Service Level Requirements (RAA: [RDDS Specification, §2](#); RA: [Spec 10](#))
- (Registrars only) New [RIS](#) requirement for Registrars (#15) to provide ICANN with 1 Registered Name sponsored by Registrar in any gTLD to be used in monitoring RDAP

28 January 2025 - WHOIS Services Sunset Date

- No longer required to provide WHOIS services*
- If provided, WHOIS services must conform to the requirements within RAA: [RDDS Specification, §1.5](#); RA: [Spec 4, §1.5](#) (base RA)

**A small number of Registry Operators not subject to WHOIS sunset*

RDAP Enforcement

- Compliance enforcement against contracted parties that have not implemented RDAP or whose RDAP implementation is not in conformance with the requirements:
 - **From October 2019 to present**: Compliance has enforced the requirement to implement an RDAP service and registrar base Uniform Resource Locators (URLs).
 - Current information indicates all registry operators have registered URLs.
 - Compliance is following up with registrars that have not yet uploaded their URL to the Naming Services portal (<15).
 - **From June 2023 (following RDAP amendments) to present**: Compliance began enforcing conformance with RDAP Response Profile and Technical Service Guide requirements.
- Compliance has issued 15 formal Notices of Breach including requirements to cure RDAP-related violations. One Notice of Breach escalated to termination of the Registrar's RAA.
- Contracted parties implementing remediation measures are required to provide regular updates on open compliance cases.

Common Issues of Nonconformance

Technical Implementation Guide:

- The 'Content-Type' in the RDAP header is not set to 'application/rdap+JSON'
 - The RDAP service may fail to connect with web-client lookups (such as lookup.icann.org).
 - Testing an RDAP service with just a web browser will not properly account for the correct media types required of RDAP.
- The RDAP service is not available over IPv6.
- The RDAP service is provided over HTTP (RDAP service must be provided over HTTPS **only**).
- The RDAP service is not returning the required HTTP status (200 OK status for sponsored domains and a 404 Not Found status for non-sponsored domains).

Response Profile:

- EPP statuses are not mapped to the required RDAP status.
- Language in the notices required by the Response Profile does not match or is improperly formatted (for example, EPP “Status Codes” notice).
- Required registration data missing from RDAP response.

RDAP Implementation Resources

- [RDAP Conformance Tool](#) - aid for registrars and registry operators to diagnose conformance issues with Feb-2019 RDAP Profile and Technical Implementation Guide (will be updated to accommodate Feb-2024 versions)
- [RDAP Conformance Tool Wiki](#) - resource to explain some of the compliance codes and exit codes from the RDAP Conformance Tool
- [RDAP Guide](#) - resource to aid users, developers and others involved in the efforts of implementing RDAP clients and servers

Contractual Compliance Audit

Joe Restuccia

Contractual Compliance Risk & Audit Senior Specialist



ICANN Contractual Compliance Program Update

ICANN82 Prep Week

24 February 2025

Contractual Compliance Audit - Registry Audit

- In October 2024, Compliance launched a new audit on registry operators' compliance with the Registry Agreement (RA) and ICANN Policies.
 - The audit includes, but is not limited to, the new DNS Abuse mitigation requirements. One, but not sole, criterion for selecting the auditees was ranking across internal and external reports related to DNS Abuse. Selection alone does not mean that auditee is not in compliance.
 - By the end of January 2025, all auditees had submitted the information and documentation requested in the Request for Information (RFI). DNS Abuse related requests were focused on verifying that Registries understood their obligations and had processes in place to address abuse.
 - Compliance is currently reviewing responses, presenting clarifying questions and requesting additional information where needed.
 - Following the completion of the audit, the results of the audit will be included in a publicly available final report that will be published, as ICANN Compliance always does.

Support of Policy, Working Groups & Other Community Initiatives

Jonathan Denison

Senior Director, Contractual Compliance

ICANN Contractual Compliance Program Update

ICANN82 Prep Week

24 February 2025



Policy, Working Groups & Other Initiatives

- Compliance is a regular contributor to the Community's ongoing policy development and research work.
- Compliance's recorded metrics and data help inform community discussions and research on specific topics, such as domain name abuse or obligations related to the renewal of gTLD domain names.
- Compliance provides input on whether proposed policy language and contract provisions are clear and enforceable.
- Compliance allocates subject matter experts to participate in policy development, working group and other initiatives meetings, provide information and feedback on concepts and language, as well as how to implement policy in an effective way once approved.
- Compliance participates in training and outreach sessions to increase awareness regarding contractual obligations among the community.

Policy, Working Groups & Other Initiatives

Compliance has subject matter experts engaged in the following initiatives:

- The Transfer Policy Review PDP
- Rights Protection Mechanisms Implementation Review Team
- The New gTLD Program: Next Round (NxR)
- Registration Data Policy Implementation
- Privacy and Proxy Services Accreditation Implementation (PPSAI)
- ccPDP4 Policy Implementation
- IDNs EPDP Phase 2 Implementation

Compliance maintains a dedicated page with [Metrics and Dashboards](#).

Compliance participates in outreach events to discuss contractual obligations and the compliance process. Recently:

- In February 2025, Compliance participated in a GNSO Council Meeting, where Compliance provided insight into ICANN's enforcement of DNS Abuse mitigation requirements and engaged in dialogue.

Questions & Answers



Questions can be sent to
compliance@icann.org

ICANN Contractual Compliance webforms are available at
<https://www.icann.org/compliance/complaint>

ICANN Contractual Compliance metrics and reporting are available at
<https://compliance-reports.icann.org/compliance.html>

Information about ICANN Contractual Compliance Audit program is
available at
<https://www.icann.org/resources/pages/audits-2012-02-25-en>