



81

ANNUAL
GENERAL
MEETING



Program Update

ICANN Contractual Compliance



ICANN81 Prep Week
28 October 2024

Agenda

Program Update:

- Introduction
- Enforcement of DNS Abuse and Abuse 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

ICANN81 Prep Week

28 October 2024



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 Abuse & DNS Abuse Requirements

Leticia Castillo

Senior Director, Contractual Compliance



ICANN Contractual Compliance Program Update

ICANN81 Prep Week

28 October 2024

Enforcement of DNS Abuse 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 Requirements

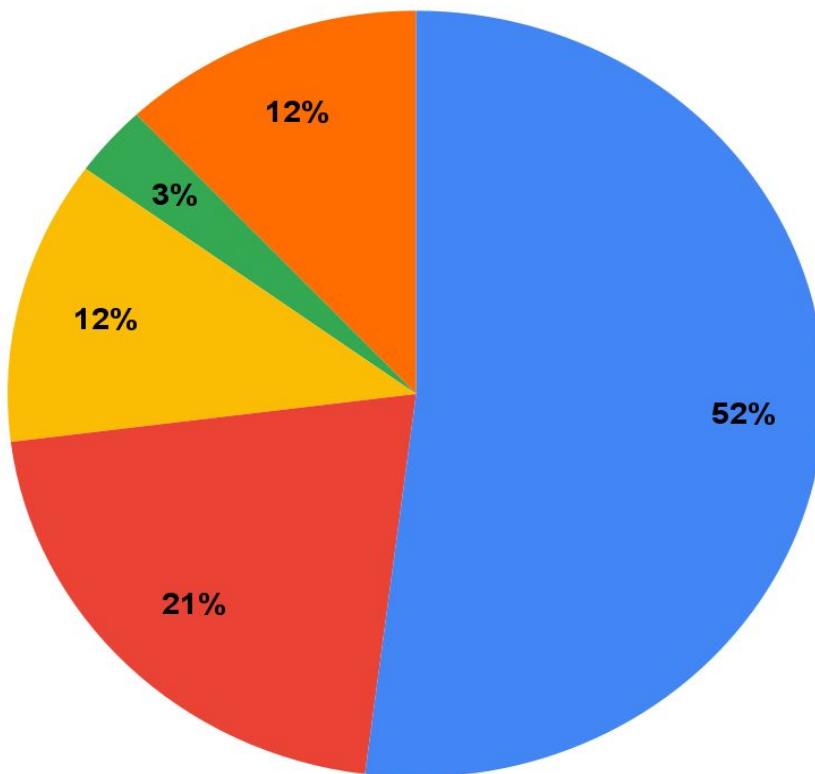
From 5 April 2024 through 5 October 2024, Compliance:

- Initiated 192 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.
- Resolved 154 DNS Abuse mitigation investigations that resulted in the suspension of over 2,700 domain names and the disabling of over 350 phishing websites.
- Begun 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 Requirements

Top Reasons for Resolving Investigations with Registrars - DNS Abuse (Cases Resolved: 151)

- The registrar took action to stop the DNS abuse by suspending the domain name.
- The registrar did not find actionable evidence of the DNS abuse.
- The registrar took action to disrupt the DNS abuse.
- The registrar took other action to stop the DNS abuse (e.g., DNS redirection/sinkholing).
- All others

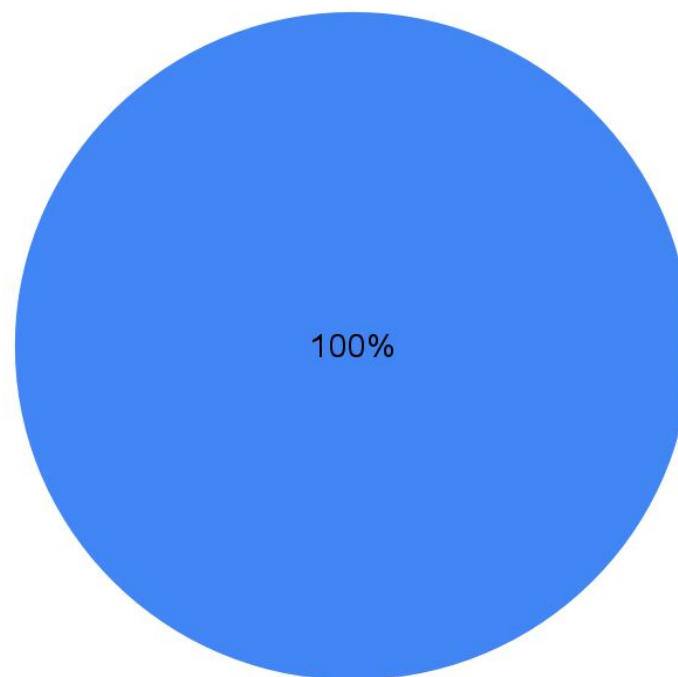


Percentages are rounded to the nearest whole number.

Enforcement of DNS Abuse Requirements

Top Reasons for Resolving Investigations with Registry Operators - DNS Abuse (Cases Resolved: 3)

- The registry operator took action to contribute to stopping the DNS abuse by suspending the domain names.



A fourth resolved case was limited to the display of DNS Abuse contact was also resolved during the reporting period as the relevant registry operator remediated the issue.

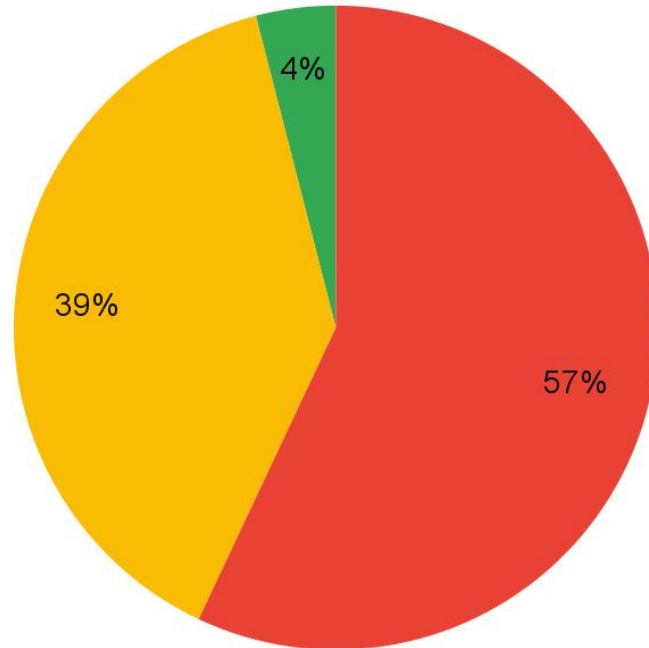
Enforcement of Other Abuse Obligations

RAA 3.18.1 requires registrars to take reasonable and prompt step to investigate and respond appropriately to reports of abuse. This requirement continues to be in force and enforced.

Details about related cases resolved from 5 April 2024 through 5 October 2024:

Top Reasons for Resolving Investigations with Registrars - Other Types of Abuse (Cases Resolved: 247)

- The registrar investigated the report and suspended the domain name(s).
- The registrar investigated and responded to the abuse report without suspending the domain name(s).
- All others



Enforcement of RDAP Requirements

Amanda Rose

Senior Registrar Compliance Lead

ICANN Contractual Compliance Program Update

ICANN81 Prep Week

28 October 2024



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 Port 43 WHOIS and RDAP

28 January 2025 - WHOIS 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](#)

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 (<20).
 - **From June 2023 (following RDAP amendments) to present:** Compliance began enforcing conformance with RDAP Response Profile and Technical Service Guide requirements.
- 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 are 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

Yan Agranonik

Senior Manager, Contractual Compliance Risk & Audit



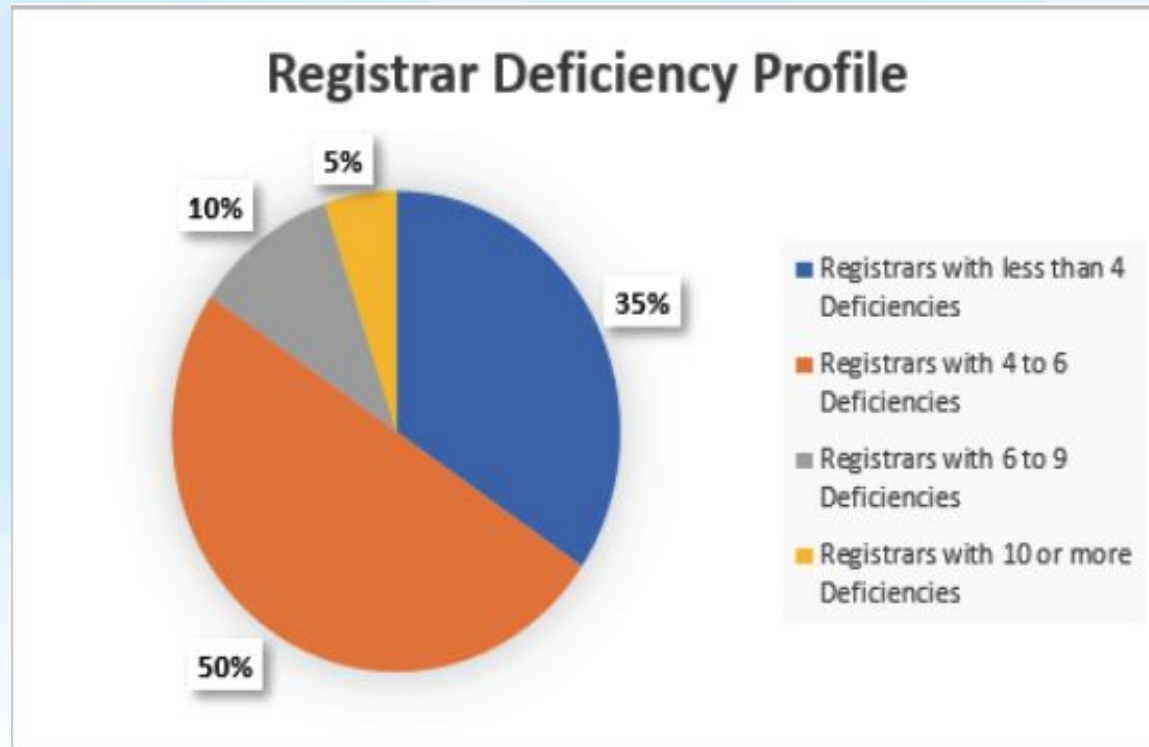
ICANN Contractual Compliance Program Update

ICANN81 Prep Week

28 October 2024

Contractual Compliance Audit - Registrar Audit

- From January through July 2024, Compliance conducted an audit on registrars' compliance with the Registrar Accreditation Agreement and ICANN Policies.
 - Sixty-two (62) registrars were selected for this audit which entailed the review of over 4,000 documents in 17 different languages.
 - The consolidated [report](#) was published in August. Key statistics:



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 the sole, criterion for selecting the auditees is higher DNS abuse rankings.
 - Following the completion of the audit, a report including key findings and auditees will be published.

Information about ICANN Contractual Compliance Audit Program is available at:

<https://www.icann.org/resources/pages/audits-2012-02-25-en>

Support of Policy, Working Groups & Other Community Initiatives

Jonathan Denison

Senior Director, Contractual Compliance

ICANN Contractual Compliance Program Update

ICANN81 Prep Week

20 February 2024



Policy, Working Groups & Other Initiatives Support

- 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 Support

Compliance has subject matter experts engaged in the following initiatives:

- The Transfer Policy Review PDP
- IDN Guidelines
- Rights Protection Mechanisms Implementation Review Team
- Registration Data Request Service (RDRS)
- The New gTLD Program: Next Round (NxR)
- Registration Data Policy Implementation
- Privacy and Proxy Services Accreditation Implementation (PPSAI)
- ccPDP4 Policy Implementation

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

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

- In October 2024, in partnership with the GSE and GDS teams, Compliance participated in an outreach session with Turkish Contracted Parties, where Compliance discussed Abuse requirements, RDAP implementation, interaction with Compliance, the RDRS, and other topics.

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>