DNS Abuse Mitigation

Session 5

Contents

Session Objectives

This session aims to continue GAC consideration of ICANN org and ICANN community initiatives to prevent and mitigate DNS Abuse, including outcomes and next steps regarding the new responsibilities domain name registries and registrars at ICANN have to address phishing, malware, botnets, pharming, and spam.

The ICANN80 GAC Plenary Session on DNS Abuse will discuss trends and perspectives on DNS Abuse in Africa and consider what impacts the new obligations for Contracted Parties to disrupt/mitigate DNS abuse in gTLDs may have in the region. Speakers from national regulatory agencies, cybersecurity authorities and african organizations are expected to join the panel.

Leadership Proposal for GAC Action

1. **Discuss trends and perspectives on DNS Abuse in Africa and consider what impacts the new obligations for Contracted Parties to disrupt/mitigate DNS Abuse in gTLDs may have in the region** based on a set of questions proposed by GAC Topic Leads on DNS Abuse:

   DNS Abuse Trends and cases

   1. Can you share any data/information on DNS abuse trends within your country/region and how these have evolved over time?
   2. Do you see any particular pattern of DNS Abuse specific in the African region?
      a. Could you present (if any) an example of such cases?
   3. Could you present (if any) some [criminal] cases pertaining to DNS Abuse in your country (or region) that frustrate you from a government perspective?
      a. Could you present (if any) some cases that drew a strong political attention?
   4. What proportion of such DNS abuse do you see performed leveraging domains registered in African ccTLDs vs. domains registered in gTLDs?

5. Do you see differences in how such DNS abuse is dealt with by ccTLD Registry Operators, as compared to gTLD Registry Operators?

Policy & Solutions

6. To your knowledge, which measures taken by African DNS operators have been the most effective in mitigating DNS abuse?
7. Could you present (if any) example(s) of policy (or regulatory) action against DNS Abuse taken by African ccTLD registry operators?
8. Within the DNS Abuse categories, is there any policy priority in preventing / mitigating DNS Abuse in your country (or region)?
    a. Could you present why, if possible?

Next Steps for the GAC and ICANN

9. What positive impacts do you think that the new ICANN contract provisions will have on DNS abuse activity in the African region?
10. What do you think the GAC should focus on when supporting the ICANN community in reflecting upon DNS abuse? What should be the priorities for the GAC agenda?
11. What improvements do you believe are needed in the detection, reporting, and mitigation of abusive domains? What would be the role of ICANN for those improvements?

2. **Continue considering the scope of desirable policy development to further improve DNS Abuse prevention and mitigation** in light of:

    - Recommendation by the GNSO Small Team on DNS Abuse (7 October 2022) **to initiate a policy development process on malicious registrations**, and potential contractual negotiations on this matter, which should eventually be informed by findings of the Inferential Analysis of Maliciously Registered Domains (INFERMAL) project, to explore the drivers of malicious domain name registrations[1].
    - The GAC's statement in the GAC Comments (17 July 2023) on the proposed Amendments that "*subsequent work with the multistakeholder community on DNS Abuse [...] should include Policy Development Processes (PDPs) to further inform the updated RA and RAA, as well as other work on outstanding issues to address prior to the next application round for New gTLDs.*"
    - The summary report of Public Comments on the new amendments (1 August 2023) in which ICANN org noted "*the ICANN community will have the opportunity to discuss these obligations and determine if further obligations are required […]. **ICANN org and the CPH NT support the comments from the GAC which stated that after the proposed amendments are adopted, work should include Policy Development Processes (PDPs) to further inform the updated Base RA and RAA**.*"
    - ICANN Contractual Compliance's plans to enforce the new amendments, as outlined to the GAC during ICANN79:

[1] See ICANN OCTO Blog "New ICANN Project Explores the Drivers of Malicious Domain Name Registrations" on 25 April 2023

- To conduct specific monitoring and prioritize the processing of complaints submitted by law enforcement and cybersecurity professionals
- To facilitate the submission of valid complaints that provide enough information so that prompt action can be taken
- To Include the new DNS Abuse obligations in the scope of future proactive audits
- To produce a dedicated report on the enforcement of the new DNS Abuse requirements, published monthly starting in June 2024
- To prepare a specific report on the enforcement of the new obligations after 6 months (to be published in Q2 2025)

- **The ICANN Board's indication**, during a GAC/Board interaction on the ICANN79 San Juan Communqué (13 May 2024)[2] that while Compliance reports are expected to contribute to measuring the impact of the DNS Abuse Amendments, **it would be up to a community-led effort, facilitated and supported by ICANN, to determine the specific metrics and data sets that will allow measurement** of such an impact.

[2] See ICANN Board Comments on Issues of Importance in the ICANN79 San Juan Communiqué (9 May 2024)

Current Status and Recent Developments

- **Amendments of the Registry and Registrar Agreements to Enhance DNS Abuse Mitigation Obligations**
    - Since ICANN66, **leaders of the GAC Public Safety Working Group have briefed the GAC** on the issue of DNS Abuse mitigation[3] including **measures available to registries and registrars to prevent DNS Abuse**, in particular the role of registration policies (including identity verification) and pricing strategies as key determinants of levels of abuse in any given TLD; as well as on **possible avenues to address DNS Abuse more effectively at the ICANN Board and ICANN org level**, such as the revisions of ICANN Contracts with registries and registrars, the enforcement of existing requirements, the implementation of relevant CCT and SSR2 Review recommendations, Privacy/Proxy Service Provider policy recommendations, the improvement of accuracy of registration data, and the publication of more detailed domain abuse activity data.
    - In Communiqués in recent years, the GAC highlighted "***the need for improved contract requirements to address the issue of DNS Abuse more effectively*** (ICANN72 GAC Communiqué, 1 Nov. 2021) and proposed that "*Improved contract provisions could focus on the reporting and handling of DNS Abuse and enforcement of related contract requirements*" (The Hague Communiqué, 20 June 2022). The GAC also stressed that ICANN is "*particularly well placed to negotiate improvements to existing contracts*" and "*to receive public input from the ICANN Community*".
    - During ICANN75, the **GNSO Small Team on DNS Abuse**, **discussed "gaps in interpretation and/or enforcement" of the current ICANN contracts** as later reflected in its Recommendations to the GNSO Council (7 Oct. 2022).
    - In the Kuala Lumpur Communiqué (26 September 2022) the **GAC recalled its "*support for 'the development of proposed contract provisions applicable to all gTLDs to improve responses to DNS Abuse'[4], for example those identified in the SSR2 and the CCT reviews"***
    - In December 2022, the Registrar Stakeholder Group (RrSG) and Registry Stakeholder Group (RySG) formally **notified ICANN to initiate negotiations** to respectively "*incorporate baseline contractual requirements to Section 3.18 of the RAA for registrars to disrupt and/or mitigate Domain Name System Abuse"* and "*enhance the DNS Abuse obligations contained in the [Registry Agreement]*". An **ICANN CEO** Blog (18 Jan. 2023) confirmed ongoing work *"to **define baseline obligations to require registries and registrars to mitigate or disrupt DNS abuse**"* expecting that this should "*aid ICANN's Contractual Compliance team in its enforcement efforts with registrars or registries who fail to adequately address DNS abuse*." It also noted this would be an opportunity for the ICANN Community "*to discuss and determine if further obligations are required via a policy development process".*

[3] See material of GAC plenary sessions during ICANN66, ICANN68, ICANN69, ICANN70, ICANN71, ICANN72, ICANN73 and ICANN74.
[4] ICANN70 GAC Communiqué, Section IV.1 p.5

- In the meantime, the GNSO's Business Constituency (**BC**) and Intellectual Property Constituency (**IPC**), and the At Large Advisory Committee (**ALAC**) requested (20 Jan. 2023) that "*community input is appropriately regarded, and to assist ICANN Org in its established role as an advocate for community needs and arbiter of the public interest".* In its response (27 March 2023), the ICANN Board stated that both "*ICANN Board and org have listened carefully to the community over the last several years regarding DNS abuse. Taking* ***this approach to make focused improvements to the Agreements, to add a clear obligation for registries and registrars to mitigate DNS abuse, will be an important building block in a longer journey that envisions potential policy discussions*** *open to the full ICANN community,* ***and potentially future negotiations*** *between the CPH and ICANN org.*"
- In a Pre-ICANN76 GAC Briefing on Contract Negotiation regarding DNS Abuse Mitigation (28 February 2023) [*GAC website login required*] GAC Topic leads **discussed possible improvements to existing contract provisions** towards better clarity and enforceability, **as well as possible areas for new contract provisions** as discussed in the ICANN Community (notably by the CCT and SSR2 Reviews) **including: financial and reputational incentives, thresholds of abuse and compliance triggers, best practices and centralized abuse reporting.**
- During the GAC bilateral meeting with the ICANN Board during ICANN76, **the GAC encouraged the ICANN Board to consider conducting a listening session with the ICANN community** about the negotiations (See p.11 of the ICANN76 GAC Meeting Minutes)
- In the ICANN76 Cancún Communiqué (20 March 2023), the GAC encouraged the ongoing negotiations *"to proceed expeditiously"* and noted that it *"considers that* ***continued efforts in this area will be required, including further improvement of contractual obligations and/or targeted policy development processes prior to the launch of a second round of New generic Top-Level Domains*** *(new gTLDs)."* In addition, the GAC encouraged *"Contracted Parties and ICANN to further consider, inter alia, proactive measures as well as positive incentives for registries and registrars in future work on DNS abuse mitigation or disruption.*"
- In preparation for ICANN77, the **GAC Underserved Regions Working Group** (USRWG) organized two **webinars** to prepare newcomers and underserved regions GAC representatives to contribute to a Comment on the expected amendments of the Registry and Registrar contracts[5].
- **ICANN org initiated a public comment proceeding** on the Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations (29 May 2023) which were subsequently presented in a ICANN77 Prep Week webinar (30 May 2023). Among the various changes proposed to ICANN's contracts, the amendments include a **new requirement to promptly take appropriate mitigation actions against domains for which the contracted party has actionable evidence** demonstrating that the domains are being used for DNS Abuse. In addition to the proposed contract amendments, a draft ICANN

[5] See Pre-ICANN77 GAC Capacity Development Webinar on DNS abuse #1 (4 May 2023) and Webinar #2 (22 May 2023)

Advisory provides detailed explanation of the new provisions and sets expectations as to their interpretation.

- Following its discussions of the proposed amendments during ICANN77[6], GAC Comments (17 July 2023) were submitted in the public comment proceeding:
  - The GAC noted that the amendments are "*timely and relevant and, when adopted, will represent an important first step forward to combat DNS Abuse.*"
  - The GAC stressed "*In light of the ongoing threat that DNS Abuse poses to consumers and the public and private sectors*", that "*it is imperative that the improved contracts are swiftly adopted following the completion of the Public Comment process*"
  - **The GAC expressed support for "*the proposed amendments as a general matter*" but invited *"ICANN org and the CPH NT to consider some specific issues related to the text of the amendments*"**. These include: the DNS Abuse definition; reporting and monitoring by Contracted Parties; consequence for non compliance; providing the ICANN community the ability to monitor how compliance is enforced; the need for the Advisory to be updated from time to time; and the need to address DNS Abuse both inside and outside of ICANN.
  - **The GAC indicated looking forward to "*engaging in subsequent work** with the multistakeholder community on DNS Abuse after the amendments are adopted. T**his work should include Policy Development Processes (PDPs) to further inform the updated RA and RAA, as well as other work on outstanding issues** to address prior to the next application round for New gTLDs."*
- In its Public Comment Summary Report (1 August 2023), **ICANN org indicated that voting by registries and registrars will proceed on the amendments as initially proposed** and noted *"[r]regarding comments that the proposed amendments are insufficient to address the challenge of DNS Abuse": ICANN org acknowledges the comments and reminds the community that the ICANN community will have the opportunity to discuss these obligations and determine if further obligations are required […]. I**CANN org and the CPH [Negotiating Team] support the comments from the GAC which stated that after the proposed amendments are adopted, work should include Policy Development Processes (PDPs) to further inform the updated Base RA and RAA**."*
- Voting by registries and registrars on the amendments started on 9 October 2023 for a duration of 60 days and concluded successfully with 80% of affirmative votes by Registries and 94% approval by Registrars[7] .
- The ICANN Board subsequently resolved to approve the amendments (21 January 2024) and determined that "***no further revisions to the proposed Global Amendments are necessary after taking the public comments** and voting results into account".*
- The Amendment of the Registry Agreement, the Amendment of the Registrar Accreditation Agreement and the related Advisory: Compliance With DNS Abuse

[6] See ICANN77 GAC Capacity Development Workshop on DNS Abuse (Sunday 11 June) and GAC Discussion on DNS Abuse (Wednesday 14 June)

[7] Detailed voting results available at https://www.icann.org/resources/pages/global-amendment-2024-en

Obligations in the Registrar Accreditation Agreement and the Registry Agreement were published on 5 February 2024 and became effective on 5 April 2024[8].

- During the ICANN79 ICANN meeting, ICANN Contractual Compliance outlined its enforcement plans to the GAC. These are expected to include:
  - Specific monitoring of complaints submitted by law enforcement and cybersecurity professionals and prioritization of their processing.
  - Facilitating the submission of valid complaints that provide enough information so that prompt action can be taken.
  - Inclusion of the new DNS Abuse obligations in the scope of future proactive audits
  - A dedicated report on the enforcement of the new DNS Abuse requirements to be published and updated every month, including data such as:
    - Number of complaints received broken down by the type of DNS Abuse;
    - Number of compliance notifications sent to contracted parties under the DNS Abuse requirements;
    - Number of cases resolved with contracted parties and their outcomes, including whether the contracted party took action to stop or to disrupt the DNS Abuse or whether no action was taken because there was no actionable evidence; and
    - Number cases resolved with contracted parties, and their outcomes, that resulted from complaints submitted by law enforcement agencies within the registrar's jurisdiction.
  - By Q2 2025, ICANN Compliance intends to prepare a more detailed report related to the enforcement of the DNS Abuse requirements during the first 6 months in force.
- In the ICANN79 GAC San Juan Communiqué (11 March 2024), the GAC stated that it *"will track reports from ICANN Compliance on DNS Abuse enforcement"* and that "*there remains a general expectation that significant progress occur in advance of the next round of new gTLD applications"*.
- In its ICANN Board Comments on Issues of Importance in the ICANN79 San Juan Communiqué (9 May 2024) regarding the ICANN79 Communiqué, the ICANN Board stated: "***the intent is that Compliance's reports contribute to measuring the impact of the DNS Abuse Amendments****. However,* ***determining the specific metrics and data sets that will allow measurement of such an impact should be a community-led effort, facilitated and supported by ICANN***". It further indicated that "*an ICANN org cross-functional team working on analyzing the information and determining how to approach these efforts.*"
- During the recent Contracted Parties Summit (6-9 May 2024), Contracted Parties discussed the implementation and impact of the Amendments from their perspective. It was reported that the CPH DNS Abuse Subgroup is currently engaging ICANN Compliance on the way the amendments are being enforced.

[8] See notices sent by ICANN org to Registry Operators and Registrars (5 Feb. 2024)

- **Prospects of policy development regarding the prevention and mitigation of DNS Abuse**
    - Per the ICANN69 GAC Communiqué (23 October 2020), "***From the GAC's perspective, the momentum has been increasingly building for concrete action*** *as the Community has progressively engaged in constructive dialogue to advance work on a shared goal, the mitigation of DNS abuse. Beginning with the recommendations from the CCT-RT and the SSR2 RT and continuing through several cross-community sessions and more recent work on a DNS Abuse Framework,* ***the GAC believes there is now a solid expression of broad support for concrete steps to be taken to address the core components of effective DNS abuse mitigation****".*
    - Since prior to the ICANN68 meeting, **the GAC Leadership has sought the establishment, in collaboration with the GNSO Council leadership, of a framework of possible community work and policy development to address DNS Abuse**. During the ICANN72 bilateral meeting between the GAC and the GNSO as reported in the ICANN72 GAC Minutes, the GAC Chair reiterated that DNS Abuse "*is a long standing issue of interest to the GAC and that the GAC is interested in advancing community discussions, driving progress and convergence of views prior to the launch of new gTLDs*" and added that "*the GAC looks forward to agreeing on how to handle community wide discussions on DNS Abuse mitigation (a PDP, CCWG etc)*"
    - On 31 January 2022 the GNSO Council formed a **GNSO Small Team on DNS Abuse** expected to determine "*what policy efforts, if any, the GNSO Council should consider undertaking to support the efforts already underway in the different parts of the community to tackle DNS abuse*".
    - In The Hague Communiqué (20 June 2022), the GAC stated that "***any PDP on DNS Abuse should be narrowly tailored to produce a timely and workable outcome***" to which the ICANN Board responded that it shares this view and is prepared to support the ICANN community in such pursuits[9].
    - **The GNSO Small Team recommended** in a Report to the GNSO Council (7 October 2022): **the initiation of a tightly scoped policy development on malicious registrations** (Rec. 1), **further exploration of the role of bulk registrations play in DNS Abuse** and measures already in place to address it (Rec. 2), **encouraging further work towards easier, better and actionable reporting** of DNS Abuse (Rec. 3), and possible work between Contracted Parties and ICANN Compliance regarding its findings on potential gaps in interpretation and/or enforcement of the current ICANN contracts (Rec. 4). The GNSO Council proceeded with recommended outreach to Contracted Parties regarding Rec. 3 and to Contracted Parties, the DNS Abuse Institute and ICANN Compliance regarding Recommendation 2 (6 January 2023).
    - **Regarding bulk registrations**, the ICANN Compliance response to the GNSO Council (22 February 2023) states that '*ICANN agreements and policies do not contain requirements or limitations related to registering domain names in bulk. As a result,* ***ICANN Contractual***

[9] See https://gac.icann.org/sessions/boardgac-interaction-group-bgig-call-31-august-2022 (31 August 2022) [*prior GAC website login required*]

Compliance does not collect or track information on bulk registrations**, [or] the potential role these may play in Domain Name System (DNS) abuse".* The DNS Abuse Institute's response (24 February 2023) proposed that "research would need to be conducted to determine the scale of any issues related to [Bulk Domain Registration] prior to any policy work**",* and noted the relevance of the Framework on Domain Generating Algorithms Associated with Malware and Botnets developed by the RySG and the GAC PSWG. **The DNS Abuse Institute expressed support for payment-based approaches to fighting DNS abuse,** and **proposed that it would be worth "*to encourage Registrars to investigate all of the domains in a customer account where one is identified as malicious*"**as part of "*sensible and practical options available to registrars that will reduce DNS Abuse [...] right now*", in addition to "*friction at the time of registration*"**.**

- Based on further input received from Contracted Parties[10], **the GNSO Small Team on DNS Abuse concluded**, as part of its Preliminary Findings Preliminary Finding on Bulk Registrations (15 May 2023), that **the topic of bulk registrations "*does not fall within the realm of Consensus Policy at the moment*"** to the extent that:
  - *Complaints from single or multiple registrations are handled uniformly, without clarity on what might constitute bulk registrations warranting targeted reactions.*
  - *The lack of a clear definition did not elicit a clear response.*
  - *Other Know Your Customer tools are deemed more efficient in detecting potential abuse, and should warrant more attention.*
  - *ICANN's recently started Inferential Analysis of Maliciously Registered Domains (INFERMAL) project seems to indicate a willingness from the org. to look into this matter and provide [...] better statistics and intelligence* [on this matter]
- In the Hamburg Communiqué (30 October 2023), the GAC stated its intention "*to engage with the community in discussions on policy efforts around [...] key themes linked to effective implementation of the amendments, such as clarification of key terms from the amendments (i.e. "reasonable", "actionable", "prompt"), and further actions to mitigate DNS Abuse, such as capacity building efforts*".
- During the ICANN79 preparation call between the GNSO Council and GAC Leadership, it was indicated that at the moment, the GNSO Council is not actively considering policy development on DNS Abuse-related issues and that this is currently the subject of discussion within and between stakeholder groups in the GNSO.
- During a bilateral meeting with the GAC in San Juan (6 March 2024), the GNSO Council noted that the GNSO Small Team is currently paused while awaiting for data to be collected from ICANN Compliance on the impact of the amendments, and will resume once further information is provided to determine what if any policy development might be appropriate to address gaps in DNS Abuse mitigation.

[10] See correspondence from the Contracted Parties House (CPH), Registry Stakeholder Group (RySG) and Registrar Stakeholder Group (RrSG)

- **Status and implementation prospects of Specific Reviews recommendations related to DNS Abuse disruption**[11]
    - **The SSR2 Review delivered 63 recommendations** in its Final Report (25 January 2021) with a significant focus on measures to prevent and mitigate DNS Abuse.
        - The GAC considered a Draft SSR2 Review Report (24 January 2020) and endorsed many of the draft recommendations in a GAC Comment (3 April 2020). These were followed by GAC Comments (8 April 2021) on the final recommendations, and subsequent GAC Advice in the ICANN72 Communiqué (1 Nov. 2021) requesting follow-up action and further information on levels of implementation of certain recommendations, to which the ICANN Board responded (16 Jan. 2022), leading to further discussions during ICANN73[12], and communications by ICANN org to the GAC in a letter (18 March 2022) and a follow-up email (12 April 2022).
        - Based on the ICANN Specific Review Quarterly Report (31 March 2024), and based on several ICANN Board resolutions (22 July 2021, 1 May 2022, 16 November 2022 and 10 September 2023): **23 recommendations** are now **approved** (including 14 subject to prioritization for implementation), **38 rejected**, and **1 pending** further information.
        - On 10 September 2023, the **ICANN Board rejected 6 of the 7 Pending Recommendations relating to DNS Abuse** based on assessment by ICANN org - **12.1** (*DNS Abuse Analysis advisory team*), **12.2** (*structure agreements with data providers to allow further sharing of the data*), **12.3** (*publish reports that identify registries and registrars whose domains most contribute to abuse*), **12.4** (*report actions taken by registries and registrars to respond to complaints of illegal and/or malicious conduct*), **13.1** (*central DNS abuse complaint portal mandatory for all gTLDs*), **13.2** (*publish complaints data for third party analysis*) and **14.2** (*provide contracted parties with lists of domains in their portfolios identified as abusive*)
        - **In its discussion of contract negotiations on DNS Abuse, the GAC PSWG discussed**[13] **several SSR2 recommendations that have been rejected** by the ICANN Board per the Board Scorecard (22 July 2021) - **8.1** (*commission a negotiating team that includes abuse and security experts to renegotiate contracted party contracts*), **9.4** (*regular compliance reports enumerating missing tools*), **14.4** (*provide contracted parties 30 days to reduce the fraction of abusive domains below the threshold*) and **14.5** (*consider offering financial incentives*) - **for which the GAC acknowledged** in the GAC ICANN72 Communiqué (1 November 2021) "*the procedural bases for the Board's rejection*" **noting**, nevertheless, ***"the useful substantive aspects of certain rejected recommendations**, including those that aim **to provide ICANN org and ICANN Contractual Compliance with appropriate tools to prevent and mitigate DNS abuse***".

[11] The status of all recommendations may be consulted in the ICANN's Quarterly Reports, the home page of each review, all accessible from https://www.icann.org/resources/reviews/specific-reviews
[12] See ICANN73 GAC Minutes p.13
[13] See PSWG Conference Call on 14 February 2023 [*prior GAC website login required*]

- The **Competition, Consumer Trust & Consumer Choice Review Team's** Final Report (8 Sep. 2018) provided 35 recommendations. In the Montréal Communiqué (6 Nov. 2019), as clarified in subsequent correspondence with the ICANN Board (Jan. 2020), **the GAC advised the ICANN Board "*not to proceed with a new round of gTLDs until after the complete implementation* of the recommendations [...] that were identified as 'prerequisites' [14 recommendations] or as 'high priority' [10 recommendations]."** Following discussions related to the ICANN70 and ICANN71 Communiqués[14], the GAC and ICANN Board agreed on an understanding stated in a GAC/Board BGIG Call (5 October 2021) *[GAC Website Login required]* as "*the GAC would consider follow-up on the substance of the CCT Review recommendations and not the specific recommendations themselves.*"
  Several of the these recommendations were relevant to contract negotiations on DNS Abuse and were discussed by the GAC PSWG[15]:
  - **Recommendation 17** (*collect data about and publicize the chain of parties responsible for domain name registrations)* **was approved and implementation is complete** per its Implementation documentation as of 14 Sep. 2022.
  - **Recommendation 13** (*collect data on impact of registration restrictions* which the GAC noted "*would allow for more informed decision and policy making with regard to future standard registry and registrar contract provisions")* and **Recommendation 20** (*assess mechanisms to report and handle complaints and possibly consider amending future standard Registry Agreements to require registries to more prominently disclose their abuse points of contact and provide more granular information to ICANN*) were approved in part per Board Scorecard of 22 October 2020, and **their implementation is in progress with competition estimated between Q3 2023 and Q2 2024** according to the ICANN Specific Reviews Q1 2023 Quarterly Report (31 March 2023)
  - **Recommendation 14** *(incentives to adopt proactive anti-DNS Abuse measures)* and **Recommendation 15** *(negotiate amendments to include provisions aimed at preventing systemic use of specific registrars or registries for DNS Security Abuse, and establish thresholds of abuse for automatic compliance triggers)* **were rejected by the ICANN Board** (resolution of 10 September 2023)

- The **RDS-WHOIS2 Review recommendations LE.1 and LE.2** which sought "*regular data gathering through surveys and studies to inform a future assessment of the effectiveness of RDS (WHOIS) in meeting the needs of law enforcement*" and "*conducting comparable surveys and/or studies with other RDS (WHOIS) users working with law enforcement on a regular basis*" are now **considered to be "*implemented to the extent possible*"** in connection with work of EPDP Phase 2 and 2A as well as the SSAD ODP, per the Implementation Documentation (11 October 2022)

[14] See Communiqué clarification discussions and eventual Board responses to the GAC's Follow-up on Previous Advice in the ICANN70 Communiqué and ICANN71 Communiqué: ICANN70 Clarification call (21 April 2021) and Board response (12 May 2021), and ICANN71 Clarification call (29 July 2021) and Board response (12 September 2021).
[15] See PSWG Conference Call on 14 February 2023 [*GAC website login required*]

- **Measures and initiatives to mitigate DNS Abuse by Registries and Registrars**
  - On 27 March 2020, ICANN org executed the proposed amendment of the .COM Registry Agreement which **extends contractual provisions to facilitate the detection and reporting of DNS Abuse to three-quarters of the gTLD namespace**[16]. Additionally, a binding Letter of Intent between ICANN org and Verisign lays out a cooperation framework to develop best practices and potential new contractual obligations, as well as measures to help measure and mitigate DNS security threats.
  - **In the context of the COVID-19 crisis Contracted Parties and Public Safety stakeholders** reported[17] on their collaboration to facilitate reports, their review and their referral to relevant jurisdiction through the adoption of a standardized form and the establishment of single point of contacts for relevant authorities. These efforts built on working relations established between law enforcement and registrars as well as the publication by the **Registrar Stakeholder Group** of a Guide to Registrar Abuse Reporting during ICANN67. This guide was updated (Jan. 2022) and endorsed by the **Registry Stakeholder Group**.
  - **Public Interest Registry (PIR)**, Registry Operator of .ORG and several New gTLDs launched the **DNS Abuse Institute** (17 February 2021). This initiative was presented to the GAC PSWG (3 March 2021). In the ICANN70 Communiqué, the GAC welcomed the launch of the DNS Abuse Institute and "*encouraged[d] community efforts to cooperatively tackle DNS Abuse in a holistic manner*". The DNS Abuse Institute has since released a Roadmap (14 June 2021), regularly discusses best practices, and developed an initiative to measure the use of the DNS for phishing and malware activities. During ICANN74, the GAC invited the DNS Abuse Institute to present Net Beacon (formerly known as the **Centralized Abuse Reporting Tool**), which it indicated it is developing in response to SAC115 and SSR2 Recommendation 13.1, and consistent with CCT-RT Recommendation 20. In advance of ICANN79, the DNS Abuse Institute published an analysis of GAC Communiqués and Community Activity on DNS Abuse (8 February 2024) in which it discusses the GAC's positions, related Community activity and "current gaps".
  - **Several actors of the DNS Industry are actively seeking to contribute to the measurement of DNS Abuse** and of the effect the recently approved Amendments of the Registry Agreement and the Registrar Accreditation Agreements will have:
    - During ICANN78, the **DNS Abuse Institute** presented to the GAC its Compass project and methodology which aims to provide a rigorous and transparent approach to measuring DNS Abuse, and currently produces monthly abuse reports that discuss trends across the industry and specific registrars and registries that either have high or low rates of DNS Abuse. Based on its measurements, the DNS Abuse Institute reports that 80% of DNS Abuse gets mitigated within 30 days. It expects that

[16] Such provisions include Specification 11 3b which had only been applicable to New gTLDs so far. As of March 2022, .COM totaled 161.3 million domains names registrations, which, excluding the 133.4 million ccTLD domains out of the 350.5 million domains across all TLDs, represent a 74% share of all gTLD domain registrations (see Verisign Domain Name Industry Brief of June 2022)

[17] See Contracted Parties presentations prior and during the ICANN68 meeting and PSWG briefing to the GAC during ICANN68.

mitigation trends should evolve favorably in the future thanks to the amendments of the ICANN's contracts.

  - **CleanDNS**, a service provider managing DNS Abuse on behalf of registrars, registries and hosting providers, discussed with the GAC, during ICANN78 and ICANN79, the importance of well evidenced reports of DNS Abuse, which need to be communicated to the most appropriate party (registry, registrar, hosting provider or registrant), to ensure that the time to mitigate the abuse is as short as possible so that victimization can be minimized.

- During the recent Contracted Parties Summit (6-9 May 2024), ICANN and Contracted Parties held a "Combatting DNS Abuse workshop" which discussed amongst other topics" "Most pressing concerns and challenges on DNS Abuse", "Case Studies and Lessons Learnt from Challenging DNS Abuse Reports". Recording of the open sessions are available at https://cpsummit2024.sched.com/.
-

- **ICANN Org's multifaceted Response[18] (now part of the DNS Security Threat Mitigation Program) and contractual enforcement**
  - ICANN org presented (22 July 2021) its DNS Security Threat Mitigation Program which aims to provide visibility and clarity over various DNS security threats related initiatives and projects, and allows for the formation and execution of a centralized strategy.
  - **ICANN's Office of the CTO** (OCTO) **and its Security Stability and Resiliency Team** (SSR) conduct research and maintain ICANN's expertise in DNS security for the benefit of the Community. It is engaged in cyber threats intelligence and incident response fora, and develops systems and tools to assist in identification, analysis and reporting DNS Abuse[19].
    - In response to the COVID-19 crisis, OCTO developed the **Domain Name Security Threat Information Collection and Reporting (DNSTICR)** tool to help identify domain names used for COVID-19-related abuse and share data with appropriate parties. The GAC was initially briefed on this matter prior to ICANN68 (12 June 2020) and GAC Members have been invited to contribute to the linguistic diversity of the tool.
    - Through its **Domain Abuse Activity Reporting (DAAR) platform**, ICANN has reported monthly since January 2018 on domain name registration and security threats behavior observed in the DNS[20]. In October 2021, ICANN org and the Registry Stakeholder Group reported on their agreement in principle[21] to leverage Registry-held registration data to provide registrar-level information in DAAR as recognized by the GAC in a letter to ICANN (21 February 2022). These changes were

[18] See ICANN CEO blog on 20 April 2020 detailing ICANN Org's Multifaceted Response to DNS Abuse
[19] During a GAC call on DNS Abuse Matters (24 February 2021), ICANN org provided updates on OCTO's DNS Abuse-related Activities, which included a discussion the definition of DNS Security Threats and DNS Abuse, Contracted Parties obligations, and updates on DAAR, DNSTICR, DSFI, KINDNS, and OCTO's efforts in the area of training and capacity building throughout the world
[20] Several stakeholders and ICANN initiatives have commented on the limitations of DAAR, in particular a letter from the M3AAWG to ICANN org (5 April 2019) and the Draft Report of the SSR2 Review Team (24 January 2020). The Registry Stakeholder Group who had also expressed concerns made recommendations in a correspondence to ICANN's CTO (9 September 2020).
[21] See RySG letter to ICANN (22 October 2021) and ICANN Blog (28 October 2021)

included in the Proposed Amendments to the Base gTLD RA and RAA to Add RDAP Contract Obligations (6 September 2022) which the GAC welcomed in its Comments (16 November 2022). These amendments were recently approved by the ICANN Board (30 April 2023) and are expected to become effective by 3 February 2024.

- OCTO supported the **DNS Security Facilitation Initiative Technical Study Group**, launched in May 2020 as part of the implementation of the FY21-25 Strategic Plan, to *"explore ideas around what ICANN can and should be doing to increase the level of collaboration and engagement with DNS ecosystem stakeholders to improve the security profile for the DNS"*. Its Final report (15 October 2021) was released after 18 months of deliberations. ICANN org indicated to the GAC (16 Feb. 2022) developing an action plan accordingly. The implementation process and a wiki page to track progress was introduced to the community on 20 April 2022. During ICANN74, the GAC discussed the value of prioritizing recommendation E5 for the establishment of a **threat and incident information sharing platform** among relevant stakeholders in the ICANN community[22].
- A new project to be supervised by ICANN OCTO, Inferential Analysis of Maliciously Registered Domains (INFERMAL), aims to **systematically analyze the preferences of cyberattackers, including the use of domain names of certain registrars over others**, and possible measures to mitigate malicious activities across top-level domains (TLDs). This project is stemming in part from evidence gathered in the Statistical Analysis of DNS Abuse in gTLDs (9 August 2017)[23], suggesting that malicious actors may prefer registrars that provide low registration prices, accept specific payment methods, offer free application programming interfaces (APIs) for bulk registrations or avoid registrars that require certain information in the purchasing process.
  In a pre-ICANN78 update (25 October 2023), it was indicated that the research team was planning "*to perform an analysis of identified security measures that help mitigate DNS abuse"* and intended to "*summarize a study on how quickly abusive domain names are suspended after operators are notified about the abuse*". It expected that a final report "*in the form of a research paper*" will be shared by September 2024 and that "*best practices to effectively mitigate abuse*" will be proposed.

- **Regarding Contractual Compliance enforcement** in its blog (20 April 2020), the ICANN CEO recalled: "*ICANN Compliance enforces the contractual obligations set forth in ICANN's policies and agreements, including the Registry Agreement (RA) and the Registrar Accreditation Agreement (RAA). ICANN Compliance also works closely with OCTO to identify DNS security threats [...] and associate those threats with the sponsoring contracted parties. ICANN Compliance uses data collected in audits [...] to assess whether registries and registrars are adhering to their DNS security threat obligations. Outside of*

[22] Recommendation E5 *Incident Response* of the DSFI-TSG Final Report *(13 Oct. 2021)*: "*ICANN org should, together with relevant parties, encourage the development and deployment of a formalized incident-response process across the DNS industry that allows for interaction with others in the ecosystem. Such an effort should include incident-response handling as well as the protected sharing of threat and incident information"*

[23] This study was conducted as part of the CCT Review and a GAC Comment (19 Sept. 2017) was submitted on this report.

audits, ICANN Compliance will leverage data collected by OCTO and others to proactively engage with registries and registrars responsible for a disproportionate amount of DNS security threats. Where constructive engagement fails, ICANN Compliance will not hesitate to take enforcement action against those who refuse to comply with DNS security threat-related obligations.".

- Following a prior **Contractual Compliance audit** of Registry Operators focused on DNS Infrastructure abuse which concluded in June 2019[24] , ICANN reported (24 August 2021) on the results of the audit on **Registrars' Compliance with DNS Abuse Obligations**: 126 registrars audited (managing over 90% of all registered domains in gTLDs); 111 registrars not fully compliant with requirements related to the receiving and handling of DNS abuse reports (RAA Sections 3.18.1 – 3.18.3); and 92 registrars took actions to become fully compliant.
- On 9 March 2022, ICANN announced its rolling out of new reporting enhancing the visibility of complaint volumes and trends.
- **A new round of audits for** 28 gTLD Registry Operators[25] running gTLDs that have not previously been audited in a standard full-scope audit, and which were found to have the highest abuse score as reported by publicly available Reputation Blocklists (excluding Spam), was announced on 13 April 2022 and concluded with the publication of the Audit Report on 16 September 2022. The GAC discussed the findings during its plenary session on DNS Abuse during ICANN75 (20 Sep. 2022).
- As part of ICANN78 Prep Week (9 October 2023, Contractual Compliance reported on its actions resulting from complaints[26], as well as on its Audit Program, including:
  - Completion of a Registrar Audit (22 June 2023) of 15 Registrars "*representing 7 registrar families comprising 619 registrars*" based in 8 countries, totalling 83 million domain names under management (see list on p.17). 40% of auditees were able to resolve "initial findings" while 53% were not and "*are implementing necessary changes*" to resolve outstanding deficiencies (see pp. 10-14).
  - **Launch of a new Registry Compliance Audit** (August 2023) involving 19 Registry Operators, not previously audited, with a DAAR abuse score greater than 0%.

[24] See ICANN blog Contractual Compliance: Addressing Domain Name System (DNS) Infrastructure Abuse (8 November 2018) and Contractual Compliance Report on Registry Operator Audit for Addressing DNS Security Threats (17 September 2019)

[25] .africa .app .art .bar .best .blog .buzz .cat .cloud .club .com .coop .gift .icu .ink .istanbul .moe .one .ooo .org .ren .ryukyu .tel .tirol .xin 我爱你 (Xn--6qq986b3xl) .닷컴 (Xn--mk1bu44c) .Рус (Xn--p1acf)

[26] See ICANN78 Compliance Update Slides pp. 9-10 and https://features.icann.org/compliance for more detailed reporting

- **Survey of DNS Abuse Mitigation efforts in ccTLDs by the ccNSO DNS Abuse Standing Committee (DASC)**
    - Work plans of the GAC Public Safety Working Group (PSWG) have included consideration of DNS Abuse mitigation practices by ccTLDs to inform elevated contractual standards in the gTLD space. In particular, the most recent 2023-2024 PSWG Work Plan includes Work Item 1.3 to "*Review and identify ccTLD Best Practices for adoption in the gTLD space*":
        - *Review and assess ccTLD best practices in mitigating security threats such as abuse prediction and registrant validation and verification policies, with a view to identify possible practical and implementable approaches and consider how they may inform elevated contractual standards in the gTLD space.*
    - Previously, operators of ccTLDs around the world briefed the GAC in a Pre-ICANN69 webinar (4 June 2020) on the lessons they learned from their operations during the COVID-19 crisis.
    - In March 2022, the ccNSO established a DNS Abuse Standing Committee (DASC) to "*raise understanding and awareness of the issues pertaining to DNS Abuse, promote open and constructive dialogue, and ultimately to assist ccTLD Managers in their efforts to mitigate the impact of DNS Abuse"*, noting that "*In keeping with the nature of the ccNSO, the purpose of the Committee is not to formulate any policy or standards, recognising that policy development in this area is out of scope of the ccNSO policy remit.*"
    - During the ICANN76 GAC Capacity Development Workshop (11 March 2023), the DASC presented to the GAC its initial findings following a survey it conducted between September and November 2022 covering about 100 ccTLDs, on their practices for mitigating DNS Abuse. The presentation discussed quantitative results regarding:
        - methods used to mitigate DNS Abuse (registration policies, complaint procedures, other tools) and actions taken when DNS Abuse is detected (notices to registrants, suspension, deletion);
        - collaboration with national CERTs, Law Enforcement and Trusted Notifiers;
        - public reporting of DNS Abuse.
    - The results of this survey were further discussed in ccNSO session during ICANN77 focussing on quantitative results related to verifications of registration data, their scope, timing, methods and consequences; as well as the connection between pricing policies and levels of DNS Abuse.
    - During the final presentation of the survey's results, in a Pre-ICANN78 DASC webinar on 28 September 2023 (see recording and slides), the DASC focussed on the quantitative distribution of DNS Abuse trends and mitigation practices based on features of ccTLDs (including region, governance model, size of domain portfolio, etc.).
    - During ICANN78, the ccNSO DASC joined the GAC plenary discussion on DNS Abuse Mitigation and discussed next steps in studying measurements of DNS Abuse and mitigation tools in ccTLDs.

Key Reference Documents

- ICANN Board Comments on Issues of Importance in the ICANN79 San Juan Communiqué (9 May 2024)
- Contracted Parties Summit (6-9 May 2024) and recordings of the open sessions.
- Amendment of the Registry Agreement, Amendment of the Registrar Accreditation Agreement and related Advisory: Compliance With DNS Abuse Obligations in the Registrar Accreditation Agreement and the Registry Agreement (published on 5 February 2024 and to become effective on 5 April 2024).
- ICANN Board resolution (21 January 2024) approving the Amendments of the Registry and Registrar Agreements regarding DNS Abuse
- ICANN Board Resolution (10 September 2023) based on ICANN org assessment of pending CCT and SSR2 Review pertaining to DNS Abuse Mitigation
- ICANN org Public Comment Summary Report (1 August 2023) on Public Comment proceeding related to the proposed Amendments of the Registry and Registrar Agreements regarding DNS Abuse
- GAC Comments (17 July 2023) on the proposed Amendments of the Registry and Registrar Agreements regarding DNS Abuse
- Contractual Compliance November 2022 Round Registrar Audit Report (22 June 2023)
- Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations (29 May 2023)
- Inferential Analysis of Maliciously Registered Domains (INFERMAL) announcement (25 April 2023)
- GNSO Small Team on DNS Abuse Report to the GNSO Council (7 October 2022)
- The Last Four years in Retrospect: A Brief Review of DNS Abuse by ICANN org (22 March 2022)
- European Commission Study on DNS Abuse and its Technical Appendix (31 January 2022)
- SSR2 Review FInal Report (25 January 2021) and related GAC Comments (8 April 2021)
- SSAC SAC115 Report (19 March 2021), a proposal for an Interoperable Approach to Addressing Abuse Handling in the DNS

Document Administration

Title	ICANN80 GAC Session Briefing - DNS Abuse Mitigation
Distribution	GAC Members (before meeting) and Public (after meeting)
Distribution Date	Version 1: 27 May 2024