ICANN | GAC
Governmental Advisory Committee

ICANN 77
WASHINGTON, D.C.

DNS Abuse Mitigation

Session 8

Contents

Session Objectives

This session aims to continue GAC consideration of ICANN org and ICANN community initiatives to prevent and mitigate DNS Abuse. The GAC will be briefed on relevant developments and continue discussing possible efforts by the GAC to engage with the broader ICANN community to support enhanced contract provisions and possible policy development to better mitigate DNS Abuse.

Leadership Proposal for GAC Action

1. **Consider the development of a GAC Comment on the proposed Amendments of the Registry and Registrar Agreements regarding DNS Abuse taking into account discussions during the Pre-ICANN77 GAC Capacity Development Workshop** (to be held on Sunday 11 June), **input from the GAC Public Safety Working Group (PSWG), as well as input from the ICANN community more broadly.** The proposed amendments were recently published following negotiations between ICANN and Contracted Parties since late 2022[1]. In The Hague Communiqué (20 June 2022) the GAC stated that "*ICANN org is particularly well placed to receive public policy input from the ICANN community and negotiate updates to the standard Registry and Registrar Agreements.*"

2. **Discuss the scope of desirable policy development to improve DNS Abuse prevention and mitigation**, following the 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 recently launched Inferential Analysis of Maliciously Registered Domains (INFERMAL) project, to explore the drivers of malicious domain name registrations[2].

[1] See ICANN CEO Blog "ICANN and Contracted Parties Negotiate About Improved DNS Abuse Requirements" on 18 January 2023 and Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations public comment proceeding (29 May 2023)
[2] See ICANN OCTO Blog "New ICANN Project Explores the Drivers of Malicious Domain Name Registrations" on 25 April 2023

3. **Consider the status of Review Recommendations related to the mitigation of DNS Abuse** in particular in the CCT Review Final Report (8 September 2018) and the SSR2 Review Final Report (25 January 2021).

Current Status and Recent Developments

- **Proposed 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 recent Communiqués, 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 November 2022, the Registry and Registrar Stakeholder Groups signaled their **willingness to "*pursue possible enhancements to the DNS Abuse obligations** contained in [their] respective agreements with ICANN*", to which ICANN org responded (30 Nov. 2022) that it "*aligned on the proposed guideposts outlined in [the] letter for any negotiations*". These *guideposts* were provided in the Contracted Parties correspondence to ICANN as follows:
        - *The focus of the new provisions will be on DNS Abuse as set forth in the existing ICANN*

[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

contracts, and reinforced by the GNSO Small Team on DNS Abuse;
  - *The amendments will not include matters pertaining to website content abuses nor access to registration data; and*
  - *Any new provisions [...] will not seek to impose pass-through requirements on either group.*

- 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]*".
- A recent **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".* **The ICANN CEO aims "*to share drafts with the community before ICANN77*".**
- 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 preparation for an update by Contracted Parties on the ongoing negotiations, 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.**
- 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 future GAC Comment on the expected amendments of the Registry and Registrar contracts:
  - Pre-ICANN77 GAC Capacity Development Webinar on DNS abuse #1 (4 May 2023) discussed:
    - When to address abuse at the DNS level
    - An Overview and concrete examples of malware, botnets, phishing, pharming and spam
    - ICANN's Role
    - The Roles of Registrars and Registries
    - The GAC's Role
  - Pre-ICANN77 GAC Capacity Development Webinar on DNS abuse #2 (22 May 2023) discussed:
    - Overview of Contract Negotiations and Public Comment Process
    - Development of GAC Public Comment – Process and Timeline
- **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 expected to be 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 Advisory provides detailed explanation of the new provisions and sets expectations as to their interpretation.
- During ICANN77, **the GAC is expected to discuss these amendments** in at least two settings **towards preparing a GAC Comment** (which will be due by 13 July 2023):
  - Pre-ICANN77 GAC Capacity Development Workshop on DNS Abuse (Sunday 11 June)
  - GAC Discussion on DNS Abuse (Wednesday 14 June)

- **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 GAC response (4 April 2022) to the GNSO's request for community input on DNS Abuse policy making, the GAC Chair suggested that in light of the fact that "*ongoing community efforts may produce beneficial initiatives and outcomes which may obviate the need for a PDP*", "*At this time [...] pursuing a PDP scoping exercise may be premature*".
    - 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[5].
    - **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).

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

- **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 Compliance does not collect or track information on bulk registrations****, 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[6], **the GNSO Small Team on DNS Abuse concluded**, as part of its Preliminary Findings Preliminary Finding on Bulk Registrations (15 May 2023), that ***"this 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]

[6] 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**[7]
    - **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[8], and communications by ICANN org to the GAC in a letter (18 March 2022) and a follow-up email (12 April 2022).
        - To date, per the latest ICANN Specific Review Quarterly Report (21 February 2023), based on 3 ICANN Board resolutions (22 July 2021, 1 May 2022 and 16 November 2022): **23 recommendations** are now **approved** (including 14 subject to prioritization for implementation), **30 rejected**, and **10 pending** further Board consideration.
        - **7 Pending Recommendations relating to DNS Abuse** - **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*) - **are tentatively expected to be considered by the ICANN Board in Q3 2023**. In the relevant Board Scorecard (22 July 2021), the ICANN Board acknowledged "*the extensive community and ICANN org efforts currently going on around DNS security threats*" and directed ICANN org "*to evaluate how this grouping of recommendations, along with other recommendations that pertain to DNS security threats should be considered in a coordinated way*" and inform the Board's decision on next steps.
        - **In its recent discussion of ongoing contract negotiations on DNS Abuse, the GAC PSWG discussed**[9] **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***

[7] The status of all recommendations may be consulted in the ICANN Specific Reviews Q1 2023 Quarterly Report (31 March 2023) starting p.28, along with further documentation at: https://www.icann.org/resources/reviews/specific-reviews/whois

[8] See ICANN73 GAC Minutes p.13

[9] See PSWG Conference Call on 14 February 2023 [*GAC website login required*]

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".

- 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]."* Several of the these recommendations are relevant to contract negotiations on DNS Abuse and were discussed recently by the GAC PSWG[10]:
  - **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)* which were placed **in pending status** per Board Scorecard of 1 Mar. 2019 in consideration of ongoing community discussions on DNS abuse, **are tentatively expected to be considered by the ICANN Board in Q3 2023.** In the meantime, ICANN org is processing these recommendations along with other relevant Specific Reviews recommendations and advice to the Board.
- 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 "*conducting comparable surveys and/or studies with other RDS (WHOIS) users working with law enforcement on a regular basis*" are now **considered to "*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)

[10] 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**[11]. 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[12] 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.

- **ICANN Org's multifaceted Response[13] (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[14].

[11] 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)
[12] See Contracted Parties presentations prior and during the ICANN68 meeting and PSWG briefing to the GAC during ICANN68.
[13] See ICANN CEO blog on 20 April 2020 detailing ICANN Org's Multifaceted Response to DNS Abuse
[14] 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

- 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[15]. In October 2021, ICANN org and the Registry Stakeholder Group reported on their agreement in principle[16] 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 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), and which are expected to undergo a 60-day voting period before ICANN Board consideration.
- 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[17].
- 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)[18], 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.

---

[15] 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).

[16] See RySG letter to ICANN (22 October 2021) and ICANN Blog (28 October 2021)

[17] 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*"

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

- **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 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[19] , 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[20] 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 September 2022).
  - As part of ICANN76 Prep Week, Contractual Compliance reported on its activities (28 February 2023)

[19] 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)

[20] .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)

Key Reference Documents

- 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)
- ICANN Specific Reviews Q1 2023 Quarterly Report (31 March 2023)
- ICANN Specific Reviews Q4 2022 Quarterly Report (21 February 2023)
- RySG – RrSG Communication on DNS Abuse Disruption/Mitigation Obligations (4 November 2022)
- GNSO Small Team on DNS Abuse Report to the GNSO Council (7 October 2022)
- GAC Response to GNSO Request for Community Input on DNS Abuse Policy Making (4 April 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)
- ICANN announcement and report (24 August 2021) of the Audit on Registrars' Compliance with DNS Abuse obligations.
- SSAC SAC115 Report (19 March 2021), a proposal for an Interoperable Approach to Addressing Abuse Handling in the DNS

Document Administration

Title	ICANN77 GAC Session Briefing - DNS Abuse Mitigation
Distribution	GAC Members (before meeting) and Public (after meeting)
Distribution Date	Version 1: 31 May 2023