ICANN | GAC
Governmental Advisory Committee

ICANN 75 ANNUAL GENERAL KUALA LUMPUR

DNS Abuse Mitigation

Session 6

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 processes to better mitigate DNS Abuse.

Leadership Proposal for GAC Action

1. **Review progress of ICANN org activities** in relation to DNS Abuse under its DNS Security Threat Mitigation (e.g. DAAR, DNSTICR, and capacity development/training) and Contractual Compliance programs, including recent updates to the GAC during the recent Board GAC Interaction Group Call (31 August) and the expected Pre-ICANN75 Briefing to the GAC by ICANN org[1]

2. **Assess progress in ICANN community discussions and implementation efforts related to** DNS Abuse including deliberations of the GNSO Small Team on DNS Abuse which recently indicated preparing to share a draft report "around ICANN75[2]".

[1] See https://gac.icann.org/sessions/boardgac-interaction-group-bgig-call-31-august-2022 (31 August 2022) and https://gac.icann.org/sessions/icann-org-preicann75-oral-briefing-to-the-gac (6 September 2022) [login required]
[2] See Draft Minutes of GNSO Council meeting on 25 August 2022.

Current Status and Recent Developments

- Since ICANN66, **leaders of the GAC Public Safety Working Group have briefed the GAC** on the issue of DNS Abuse[3] consistent with the PSWG Work Plan 2020-2021 and its Strategic Goal #1 to Develop DNS Abuse and Cybercrime Mitigation Capabilities.
    - The GAC reviewed **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[4].
    - The GAC also was briefed on **ongoing and possible initiatives to address DNS Abuse more effectively at the ICANN Board and ICANN org level**, including: revisions of ICANN Contracts with registries and registrars, enforcement of existing requirements, implementation of relevant CCT and SSR2 Review recommendations, Privacy/Proxy Service Provider policy recommendations, improvement of accuracy of registration data, and publication of more detailed domain abuse activity data.
    - In the ICANN72 Communiqué (1 Nov. 2021), the GAC highlighted "***the need for improved contract requirements to address the issue of DNS Abuse more effectively***. *In this regard, ICANN's role under the Bylaws includes duly taking into account the public policy concerns of governments and public authorities and acting for the benefit of the public. The Bylaws also authorize ICANN to negotiate agreements, including Public Interest Commitments, in service of its Mission. Hence, ICANN is particularly well placed to negotiate improvements to existing contracts to more effectively curb DNS Abuse, as informed by the GAC and other stakeholders advocating in the public interest*."
    - During ICANN73, the GAC considered a DNS Abuse Study published by the European Commission (see the Report and its Technical Appendix, 31 January 2022) and mentionned in the ICANN73 GAC Communiqué that this study: "*provides many valuable case studies, clarifies the different actors in the Internet ecosystem, and provides recommendations on how the different actors (e.g., registries, registrars, resellers, hosting providers, registrants, etc.) can respond to DNS abuse that takes place within the different layers of the DNS system".* The same Communiqué stated that "*not all harmful or illegal activities covered by the study fall into ICANN's remit*," although it noted the GAC could remain an "*important venue for governments*" to continue discussing DNS abuse.
    - During ICANN74, the GAC discussed ICANN's report The Last Four years in Retrospect: A brief Review of DNS Abuse Trends (22 March 2022) It was noted that it is too early to draw conclusions on trends at this stage given difficulties in discerning actual trends for important threats such as malware distribution, phishing and botnet. The importance of complementing these considerations with human and economic harm being caused by DNS Abuse was stressed, with the goal to provide a holistic picture of trends, support a better understanding of driving factors, and set appropriate incentives for effective action across the industry. In the ICANN74 The Hague Communiqué (20 June 2022), the GAC

[3] See material of the related GAC plenary session during ICANN66, ICANN68, ICANN69, ICANN70, ICANN71, ICANN72, ICANN73 and ICANN74.

[4] See in particular discussion of preventative measures available to Registries and Registrars during ICANN66 and the experience of identity verification as implemented in the .DK ccTLD during ICANN69.

called for "*more detailed breakdowns of the type of DNS Abuse measured; and availability of raw aggregate data.*"

- During ICANN74, the GAC invited the DNS Abuse Institute to present its recently launched **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 the ICANN74 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[5] that it shares this view and is prepared to support the ICANN community in such pursuits.

- **The GNSO Council Small Team on DNS Abuse** is expected to report on its findings "around" ICANN75 regarding "*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*"
  - On 31 January 2022 the GNSO Council announced the formation of this **GNSO Small Team** which was expected to "*Reach out to others in the community that have been vocal on the topic (such as the Governmental Advisory Committee [...]) to better understand what its expectations are of the GNSO and if/how it expects further policy work to contribute (or not) to the already ongoing initiatives.*"
  - In the GAC response (4 April 2022) to the GNSO's request for community input on DNS Abuse policy making, the GAC Chair recalled the importance of this "*long-standing issue of interest to the GAC"* and the GAC's interest *"in advancing community discussions, driving progress and convergence of views prior to the launch of future New gTLDs*". In light of the fact that "*ongoing community efforts may produce beneficial initiatives and outcomes which may obviate the need for a PDP*", the letter suggested that "*At this time [...] pursuing a PDP scoping exercise may be premature*". Other community responses from the ALAC, the SSAC, the BC, RySG and DNS Abuse Institute are available in the section "Next Steps regarding DNS Abuse" on the GNSO Small Teams workspace.

- **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**[6]. 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.

[5] See https://gac.icann.org/sessions/boardgac-interaction-group-bgig-call-31-august-2022 (31 August 2022) [login required]
[6] 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)

- **In the context of the COVID-19 crisis Contracted Parties and Public Safety stakeholders** reported[7] 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 (17 February 2021) the **DNS Abuse Institute**. 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), discussed mitigation of harm at various layers of the Internet infrastructure (24 August 2021) and issued a Best Practice regarding the identification of malicious registrations (2 Dec. 2021). During ICANN74, The DNS Abuse Institute was invited to present its recently launched **Net Beacon** (formerly known as the **Centralized Abuse Reporting Tool**), which it is developing in response to SAC115 and SSR2 Recommendation 13.1, and consistent with CCT-RT Recommendation 20.

- **ICANN Org's Multifaceted Response[8] (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[9].
    - 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.

[7] See Contracted Parties presentations prior and during the ICANN68 meeting and PSWG briefing to the GAC during ICANN68.
[8] The ICANN CEO published a blog on 20 April 2020 detailing ICANN Org's Multifaceted Response to DNS Abuse
[9] 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, Domain Abuse Activity Reporting (DAAR), Domain Name Security Threat Information, Collection, & Reporting (DNSTICR), the status of the Domain Security Facilitation Initiative (DSFI), the new Knowledge-sharing and Instantiating Norms for Domain Name Security (KINDNS) initiative, and a review of OCTO's efforts in the area of training and capacity building throughout the world

- 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[10]. In October 2021, ICANN org and the Registry Stakeholder Group reported on their agreement in principle[11] to leverage Registry-held registration data to provide registrar-level information in DAAR as recognized by the GAC in a recent letter to ICANN (21 February 2022). The ICANN Board confirmed that this will be reflected in contractual amendments that are expected to be published before or shortly after ICANN75[12]. ICANN org's DAAR Report for July 2022 indicated that: "*reporting about registrar portfolios requires domain name registration data to identify which domains are sponsored by which registrars. A system that can collect and analyze the necessary registrar data on a daily basis remains under development. We hope to add registrar reporting in future reports".*
- 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[13].

- **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.".*

[10] 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).

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

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

[13] 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"*

- Following a prior **Contractual Compliance audit** of Registry Operators focused on DNS Infrastructure abuse which concluded in June 2019[14] , 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)
  - 92 registrars took actions to become fully compliant, 19 are implementing changes
- **A new round of audits for selected registries** was announced on 13 April 2022. It will concern 28 gTLD Registry Operators 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). This audit is expected to be completed before Q3 2022
- During the Pre-ICANN73 ICANN CEO Briefing to the GAC (16 February 2022), ICANN Contractual Compliance reviewed the DNS Abuse obligations in ICANN Agreements and presented the outcome of a sample of 3378 complaints regarding the handling of abuse reports by registrars, leading to 456 compliance inquiries, and 1 breach notice.
- On 9 March 2022, ICANN announced its rolling out of new reporting enhancing the visibility of complaint volumes and trends.
- As part of ICANN75 Prep Week, Contractual Compliance is expected to update the Community (6 September 2022) on recent developments, and possibly on progress of its latest round of registry audits referenced above.

[14] 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)

Community Recommendations for Future Work

- **SSR2 Review Recommendations**
  - The SSR2 Review Team delivered a Draft Report (24 January 2020) with a significant focus on measures to prevent and mitigate DNS Abuse. The GAC Comment (3 April 2020) endorsed many of the recommendations, including for improving Domain Abuse Activity Reporting (DAAR) and strengthening compliance mechanisms.
  - The Final Report (25 January 2021) was considered by the GAC during ICANN70 in preparation for the eventual submission of GAC Comments (8 April 2021) as part of the Public Comments proceeding.
  - The ICANN Board took action (22 July 2021) on the Review Team's 63 Final Recommendations (25 Jan. 2021). An ICANN org blog summarized actions taken:
    - 13 recommendations were approved (pending planning of their implementation),
    - 16 recommendations were rejected (incl. 6 that could not be approved in full),
    - 34 recommendations are pending further information and analysis.
  - In the ICANN72 Communiqué (1 Nov. 2021), the GAC advised the ICANN Board to:
    - *Undertake as a matter of priority the follow-up actions needed to support the swift implementation of the Board's scorecard [...] and*
    - *Provide further information on the diverging interpretation by the Board and SSR2 Review Team of the level of implementation of certain recommendations.*
  - The ICANN Board provided additional information in its response to the ICANN72 Communiqué (16 Jan. 2022). This was a topic of further discussion between the GAC and the ICANN Board during ICANN73[15], and subject to subsequent communications by ICANN org to the GAC in a letter (18 March 2022) and a follow-up email (12 April 2022).

- **The Working Party on DNS Abuse of the Security and Stability Advisory Committee (SSAC)** released its Report published as SAC115 (19 March 2021) which proposes an Interoperable Approach to Addressing Abuse Handling in the DNS.
  - The **SSAC proposes a general framework of best practices and processes** to streamline reporting of DNS abuse and abuse on the Internet in general, discussing: Primary Point of Responsibility for Abuse Resolution, Evidentiary Standards, Escalation Paths, Reasonable Timeframes for Action and Availability and Quality of Contact Information.
  - **The key proposal**, which the SSAC recommends should be examined and further refined by the ICANN Community in collaboration with the extended DNS infrastructure community, **is the creation of a "Common Abuse Response Facilitator"** as a wholly independent non-governmental, not-for-profit organization that would act as a facilitator for the entire DNS ecosystem, including ICANN contracted parties, hosting providers, Internet Service Providers (ISPs), and Content Delivery Networks (CDNs) to streamline abuse reporting and minimize abuse victimization.

[15] see ICANN73 GAC Minutes p.13

- As noted above, the DNS Abuse Institute has taken steps since SAC115 to create a common abuse reporting platform, the Net Beacon reporting tool (June 2022). NetBeacon's features were presented to the GAC by the DNS Abuse Institute during ICANN74.

Key Reference Documents

- 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 (22 March 2022)
- European Commission Study on DNS Abuse and its Technical Appendix (31 January 2022)
- SSR2 Review FInal Report (25 January 2021) and Scorecard of Board Action (22 July 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

Further Information

GAC Policy Background Document on DNS Abuse Mitigation
https://gac.icann.org/briefing-materials/public/gac-policy-background-dns-abuse-mitigation.pdf

Document Administration

Title	ICANN75 GAC Session Briefing - DNS Abuse Mitigation
Distribution	GAC Members (before meeting) and Public (after meeting)
Distribution Date	Version 1: 2 September 2022