ICANN | GAC
Governmental Advisory Committee

ICANN 73 VIRTUAL COMMUNITY FORUM

DNS Abuse Mitigation

Session 10

Contents

Session Objectives

This session aims to continue GAC consideration of ICANN org and ICANN community initiatives to prevent and mitigate DNS Abuse. This includes implementation of the recommendations stemming from the CCT and SSR2 Reviews, discussions following the conclusion of the GNSO's Subsequent New gTLD Procedures PDP WG, proposals by the SSAC for the establishment of a Common Abuse Response Facilitator and a recent study published by the European Commission. This session will also be an opportunity to continue discussing possible concrete proposals by the GAC.

Leadership Proposal for GAC Action

1. **Consider the findings and recommendations of the DNS Abuse Study published by the European Commission**[1] and presented to the GAC Public Safety Working Group prior to ICANN73.[2]

2. **Review progress of ICANN org activities** in relation to DNS Abuse under its DNS Security Threat Mitigation and Contractual Compliance programs, as reported most recently in the Pre-ICANN73 ICANN CEO Briefing to the GAC.[3]

3. **Assess progress in ICANN community discussions and implementation efforts related to** relevant recommendations from the CCT Review Team, SSR2 Review Team, SSAC Working Party on DNS Abuse (SAC115), as well voluntary initiatives by Contracted Parties, in light of relevant GAC Advice in ICANN Montreal and ICANN72 Communiqués.

[1] See European Commission Study on DNS Abuse and its Technical Appendix (31 January 2022)
[2] See https://gac.icann.org/sessions/pre-icann73-pswg-conference-call (17 February 2022) [login required]
[3] See https://gac.icann.org/sessions/icann-org-ceo-pre-icann73-oral-briefing-for-the-gac (16 February 2022) [login required]

Current Status and Recent Developments

Community Discussions and Concrete Steps Taken to Date

- During recent ICANN meetings, **leaders of the GAC Public Safety Working Group have briefed the GAC** on the issue of DNS Abuse[4] 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.
    - The GAC also examined **ongoing or possible initiatives to address DNS Abuse more effectively at the ICANN Board and ICANN org level**[5], 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*."

- **Leaders of the GAC and GNSO Council have discussed specific GAC questions** provided to the GNSO in advance of each ICANN meeting since ICANN70[6]
    - **The GAC has sought updates from the GNSO about Community work it envisions to conduct**, in light of the conclusions of the New gTLD Subsequent Rounds PDP (which refrained from making recommendations on DNS Abuse Mitigation for future New gTLDs only), the SSR2 Review recommendations and SSAC recommendations in SAC115.
    - **GNSO Council leaders recognized the importance of the subject for the ICANN Community** and the long running discussion of this matter, but noted that **further work requires appropriate scoping** as well as developing **a common understanding**, in particular as it relates to the definition of DNS Abuse, its compatibility with ICANN's mission, with **no indication of timeline**[7].
    - On 31 January 2022 the GNSO Council announced the formation of a **GNSO Small Team to consider "*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*

[4] See material of the related GAC plenary session during ICANN66, ICANN68, ICANN69, ICANN70, ICANN71 and ICANN72
[5] See ICANN66 Minutes, ICANN68 GAC Communiqué and Minutes, ICANN69 Communiqué and Minutes, and ICANN70 Communiqué and Minutes, ICANN71 Communiqué and Minutes.
[6] See Messages and Questions to the GNSO Council prior to ICANN70
[7] See ICANN70 Minutes (p.16), ICANN71 Minutes (p.13) and ICANN72 Minutes (p.9)

DNS abuse" and "*Reach[ing] 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."*

- **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 two-third of the gTLD namespace**[8]. 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[9] 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) ,published an article (24 August 2021) discussing mitigation of harm at various layers of the Internet infrastructure. More recently, it has reported developing a Centralized Abuse Reporting Tool (18 Nov. 2021) and issued a Best Practice regarding the identification of malicious registrations (2 Dec. 2021).
-
- **ICANN Org's Multifaceted Response[10] (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

[8] Such provisions include Specification 11 3b which had only been applicable to New gTLDs so far.
[9] See Contracted Parties presentations prior and during the ICANN68 meeting and PSWG briefing to the GAC during ICANN68.
[10] The ICANN CEO published a blog on 20 April 2020 detailing ICANN Org's Multifaceted Response to DNS Abuse

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[11].

- 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 briefed on this matter prior to ICANN68 (12 June 2020) and 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[12]. In October 2021, ICANN org and the Registry Stakeholder Group reported on their agreement in principle[13] 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).
- 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) being currently developing an action plan accordingly.

- **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 Operator focused on DNS Infrastructure abuse which concluded in june 2019[14] , ICANN reported (24 August 2021)

[11] 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

[12] 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).

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

[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)

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
  - 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.

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 (16 Jan. 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.
  - In this report, 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 in particular: 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.
- The DNS Abuse Institute has reported developing a Centralized Abuse Reporting Tool (18 Nov. 2021)

Key Reference Documents

- 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	ICANN73 GAC Session Briefing - DNS Abuse Mitigation
Distribution	GAC Members (before meeting) and Public (after meeting)
Distribution Date	Version 1: 24 February 2022