

---

## DNS Abuse Mitigation

### Session 7

---

#### Contents

Session Objective	p.1	Leadership Proposal for GAC Action	p.1	Current Status and Recent Developments	p.2	Key Reference Documents	p.7
-------------------	-----	------------------------------------	-----	--	-----	-------------------------	-----

#### 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 recent developments, including the new Abuse Reporting Tool (NetBeacon) developed in response to recommendation made by SSAC and possibly the outcome of a GNSO Small Team currently considering what policy efforts should be undertaken in this area. This session will also be an opportunity to continue discussing possible efforts by the GAC to engage with stakeholder groups to improve ICANN contract provisions and their enforcement as it relates to mitigating 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 and Contractual Compliance programs, as reported most recently in the Pre-ICANN74 ICANN org Briefing to the GAC.<sup>1</sup>
- 2. Assess progress in ICANN community discussions and implementation efforts related to DNS Abuse** including deliberations of the GNSO Small Team on DNS Abuse<sup>2</sup>, and NetBeacon (formerly Centralized Abuse Reporting Tool) by the DNS Abuse Institute<sup>3</sup>.

---

<sup>1</sup> See <https://gac.icann.org/sessions/icann-org-preicann74-oral-briefing-for-the-gac> (31 May 2022) [login required]

<sup>2</sup> *idem*

<sup>3</sup> See [https://dnsabuseinstitute.org/centralized\\_abuse\\_reporting\\_update/](https://dnsabuseinstitute.org/centralized_abuse_reporting_update/) (5 April 2022)

## 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<sup>4</sup> 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**<sup>5</sup>, 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 noted 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 GNSO Council Small Team on DNS Abuse** is [expected](#) to report on its findings after ICANN74 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** 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*

---

<sup>4</sup> See material of the related GAC plenary session during [ICANN66](#), [ICANN68](#), [ICANN69](#), [ICANN70](#), [ICANN71](#) and ICANN72

<sup>5</sup> See [ICANN66 Minutes](#), [ICANN68 GAC Communiqué](#) and [Minutes](#), [ICANN69 Communiqué](#) and [Minutes](#), and [ICANN70 Communiqué](#) and [Minutes](#), [ICANN71 Communiqué](#) and [Minutes](#).

*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 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”*.
- Among other community responses, that of [PIR’s DNS Abuse Institute](#) (22 April) was made public and received a [response from the ICANN CEO](#) (9 May), who highlighted PIR’s *“innovative”* suggestion of *“tightly focused PDPs”* as well as ICANN’s [Brief Review of DNS Abuse Trends](#) (22 March)

- **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**<sup>6</sup>. 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<sup>7</sup> 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](#) or CART (18 Nov. 2021), issued a [Best Practice regarding the identification of malicious registrations](#) (2 Dec. 2021) and published an update on its CART initiative which it is renaming [NetBeacon](#) (4 April 2022).

---

<sup>6</sup> Such provisions include [Specification 11.3b](#) which had only been applicable to New gTLDs so far.

<sup>7</sup> See Contracted Parties presentations [prior](#) and [during the ICANN68 meeting](#) and [PSWG briefing to the GAC](#) during ICANN68.

- **ICANN Org’s Multifaceted Response<sup>8</sup> (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<sup>9</sup>.
    - 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<sup>10</sup>. In October 2021, ICANN org and the Registry Stakeholder Group reported on their agreement in principle<sup>11</sup> 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. The [implementation process](#) and a [wiki page](#) to track progress was introduced to the community on 20 April 2022.
  - **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*

<sup>8</sup> The ICANN CEO published a blog on 20 April 2020 detailing ICANN Org’s [Multifaceted Response to DNS Abuse](#)

<sup>9</sup> 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

<sup>10</sup> 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).

<sup>11</sup> See RySG letter to ICANN (22 October 2021) and ICANN Blog (28 October 2021)

*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<sup>12</sup>, 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 audit 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.
- **Regarding trends in DNS Abuse**, ICANN org conducted a retrospective study of DNS Abuse Trends: [The Last Four years in Retrospect: A Brief Review of DNS Abuse](#) (22 March 2022) which was referenced during the GAC introductory Webinar on [ICANN’s Role in Making and Enforcing Policies That Apply Globally to the DNS](#) (16 May 2022).

---

<sup>12</sup> 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<sup>13</sup>, 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.
- The DNS Abuse Institute has reported developing a [Centralized Abuse Reporting Tool](#) (18 Nov. 2021) on which the GAC is expected to be briefed during ICANN74.

---

<sup>13</sup>see [ICANN73 GAC Minutes](#) p.13

## 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

<b>Title</b>	ICANN74 GAC Session Briefing - DNS Abuse Mitigation
<b>Distribution</b>	GAC Members and Public (before meeting)
<b>Distribution Date</b>	Version 1: 3 June 2022