
DNS Abuse Mitigation

Session 3

Contents

Session Objective	p.1	Leadership Proposal for GAC Action	p.1	Current Status and Recent Developments	p.2	Key Reference Documents	p.5
-------------------	-----	------------------------------------	-----	--	-----	-------------------------	-----

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, and recent proposals by the SSAC for the establishment of a Common Abuse Response Facilitator. This session will also be an opportunity to continue discussing possible concrete proposals by the GAC.

Leadership Proposal for GAC Action

1. **Consider the ICANN Board's [Resolution](#) and [Scorecard](#) (22 July 2021) on the Recommendations of the Security Stability and Resiliency Review (SSR2) in their [Final Report](#) (25 January 2021) on which the GAC had submitted [Comments](#) (8 April 2021)¹.**
2. **Consider the results of ICANN's Audit on Registrars' compliance with DNS Abuse obligations as reported in a [announcement](#) and [report](#) (24 August 2021).**
3. **Consider the SSAC proposal for an [Interoperable Approach to Addressing Abuse Handling in the DNS](#) (19 March 2021) including the proposed creation of a "Common Abuse Response Facilitator" as an independent non-governmental, not-for-profit organization that would act as a facilitator for the entire DNS ecosystem to streamline abuse reporting and minimize abuse victimization.**

¹ See also on the ICANN org blog [Board Action and Next Steps on the SSR2 Review](#) (26 July 2021) which summarizes the Board's action.

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 Abuse² 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 level³, including revisions of ICANN Contracts with registries and registrars, enforcement of existing requirements, implementation of relevant CCT and SSR2 Review recommendations and Privacy/Proxy Service Provider policy recommendations, improvement of accuracy of registration data, and publication of more detailed domain abuse activity data.
- **Leaders of the GAC and GNSO Council have discussed specific GAC questions provided to the GNSO in advance of each ICANN meeting since ICANN70⁴**
 - **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 recommendation on DNS Abuse Mitigation for future New gTLDs only), the SSR2 Review recommendations and SSAC recommendations in SAC115.
 - As recorded in the GAC Minutes for [ICANN70](#) (p.16) and [ICANN71](#) (p.13), **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,.
 - In terms of steps expected to be taken by the GNSO, GNSO Council leaders have indicated that **consultations with Contracted Parties** would be conducted and **could lead to developing options for further work**. Per the [GNSO Council's Action/Decision Radar](#) (as of 23 September 2021) "*next steps, if any on DNS Abuse*" remain to be determined.
- **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 namespace⁵**. Additionally, a binding [Letter of Intent](#) between ICANN org and Verisign lays out a cooperation framework to

² See material of the related GAC plenary session during [ICANN66](#), [ICANN68](#), [ICANN69](#), [ICANN70](#) and [ICANN71](#)

³ See [ICANN66 Minutes](#), [ICANN68 GAC Communiqué](#) and [Minutes](#), [ICANN69 Communiqué](#) and [Minutes](#), and [ICANN70 Communiqué](#) and [Minutes](#), [ICANN71 Communiqué](#) and [Minutes](#).

⁴ See [Messages and Questions to the GNSO Council](#) prior to ICANN70

⁵ Such provisions include [Specification 11 3b](#) which had only been applicable to New gTLDs so far.

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** reported⁶ 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 and well as the publication by the **Registrar Stakeholder Group** of a [Guide to Registrar Abuse Reporting](#) during ICANN67.
- **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) and published an [article](#) (24 August 2021) discussing mitigation of harm at various layers of the Internet infrastructure.

- **ICANN Org’s Multifaceted Response⁷ and Contractual Enforcement**

- **ICANN’s Office of the CTO (OCTO) and its Security Stability and Resiliency Team (SSR)** conduct research and maintains 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 Abuse⁸.
 - 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 DNS⁹.
 - OCTO supports 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*”. A progress report was provided at the [4th DNS Symposium](#) (24 May 2021) and is expected [prior to ICANN72](#).

⁶ See Contracted Parties presentations [prior](#) and [during the ICANN68 meeting](#) and [PSWG briefing to the GAC](#) during ICANN68.

⁷ The ICANN CEO published a blog on 20 April 2020 detailing ICANN Org’s [Multifaceted Response to DNS Abuse](#)

⁸ 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

⁹ 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).

- **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.”*

The blog also provided a sense of volumes of complaints, resources allocated to their processing and statistics on resolution of these complaints¹⁰.

- Following a prior **Contractual Compliance audit** of Registry Operator focused on DNS Infrastructure abuse which concluded in June 2019¹¹, 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
- ICANN org [presented](#) (22 July 2021) its [DNS Security Threat Mitigation Program](#) which aims to provide visibility and clarity over the org’s various DNS security threats related initiatives and projects, and allows for the formation and execution of a centralized strategy.

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](#).

¹⁰ Regular Contractual Compliance reporting is available at: <https://www.icann.org/resources/compliance-reporting-performance>

¹¹ 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)

- The ICANN Board [took action](#) (22 July 2021) on the Review Team’s 63 Final Recommendations (25 Jan. 2021). An associated ICANN org [blog](#) summarized the types of actions taken as follows:
 - 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.
- **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.

Key Reference Documents

- 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	ICANN72 GAC Session Briefing - DNS Abuse Mitigation
Distribution	GAC Members (before meeting) and Public (after meeting)
Distribution Date	Version 1: 12 October 2021