ICANN | GAC
Governmental Advisory Committee

ICANN 70
VIRTUAL COMMUNITY FORUM

DNS Abuse Mitigation

Sessions 8, 16

Contents

Session Objectives

The GAC will consider recent ICANN Community developments, including the conclusion of the SSR2 Review and that of the Subsequent Procedures PDP to determine next steps in ensuring appropriate measures are taken to prevent and mitigate DNS Abuse in gTLD, including through consideration of concrete proposals for the improvement of contractual provisions and their enforcement.

Background

Malicious activity on the Internet threatens and affects domain name registrants and end-users by leveraging vulnerabilities in all aspects of the Internet and DNS ecosystems (protocols, computer systems, personal and commercial transactions, domain registration processes, etc). These activities can threaten the security, stability and resiliency of DNS infrastructures, and that of the DNS as a whole.

These threats and malicious activities are generally referred to as "DNS Abuse" within the ICANN Community. DNS Abuse is generally understood as including all or part of activities such as Phishing, Malware, Botnets, Distributed Denial of Service Attacks (DDoS), Spam, and the distribution of illegal materials. However, it should be noted that even the exact definition of "DNS Abuse" is a subject of active debate.

While stakeholders in the ICANN Community generally appear to agree that DNS abuse is an issue and should be addressed, there are differences of opinion as to the extent of responsibilities of relevant parties. For instance, Registries and Registrars are concerned with taking on more contractual obligations (which may affect their business models), and argue that their tools to mitigate abuse are limited and may not be appropriate (some abuse may need to be addressed by hosting providers and some registry/registrar action may result in collateral damage and liability exposure).

Notable ICANN Community efforts to address DNS Abuse to date have had varying degree of success:

- ICANN's **Generic Names Supporting Organization (GNSO)** set up the Registration Abuse Policies Working Group in 2008. It identified a set of specific issues but did not deliver policy outcomes, nor did a subsequent discussion of non-binding best practices for Registries and Registrars (including workshops during ICANN41 and ICANN42).
- **As part of the New gTLD Program,** ICANN Org adopted of a series of new requirements[1] per its memorandum on Mitigating Malicious Conduct (3 October 2009). ICANN's Report on New gTLD Program Safeguards (18 July 2016) assessed their effectiveness in preparation for the bylaws-mandated Competition, Consumer Choice and Consumer Trust (CCT) Review which delivered its recommendations on 8 September 2018.
- Prior to the creation of the GAC's Public Safety Working Group (PSWG), **representatives of Law Enforcement Agencies (LEA)** played a leading role in the **negotiation of the 2013 Registrar Accreditation Agreement**[2], as well as in the development of GAC Advice related to Security Threats which led to new provisions in the Base New gTLD Agreement that outlined responsibilities of registries[3].

[1] Vetting registry operators, requiring demonstrated plan for DNSSEC deployment, prohibiting wildcarding, removing orphan glue records when a name server entry is removed from the zone, requiring the maintenance of thick WHOIS records, centralization of zone-file access, requiring documented registry level abuse contacts and procedures

[2] See Law Enforcement Due Diligence Recommendations (Oct. 2019) and the 12 Law Enforcement recommendations (1 March 2012)

[3] These provisions were later complemented by a non-binding Framework for Registry Operators to Respond to Security Threats (20 October 2017) agreed upon between ICANN Org, Registries and the GAC PSWG.

- **More recently, the ICANN Organization,** through its **Office of the CTO** has developed ICANN's Domain Abuse Activity Reporting (DAAR) which supports monthly Abuse Reports and monitoring of trends as reported most recently to the GAC (24 February 2021). The monitoring and reporting of DNS Abuse has actively been supported both by the GAC and Review Teams, which have recommended improvements. It is expected that such tools create transparency and help identify sources of problems, which could then be addressed through compliance or - where needed - informed new policy.

Issues

Past initiatives have not yet resulted in an effective reduction of DNS abuse; rather, it is clear that much remains to be done. Despite ICANN Community attention and existing industry best practices to mitigate DNS Abuse, GAC-led community engagements as well as the Review Teams have highlighted persistent trends of abuse, commercial practices conducive to abuse and evidence that there is "*scope for the development and enhancement of current mitigation measures and safeguards*" as well as potential for future policy development[4].

Additionally, concerns with the ability to effectively mitigate DNS Abuse have been heightened in law enforcement, cybersecurity, consumer protection and intellectual protection circles[5] as a consequence of the entry into force of the European Union General Data Protection Regulation (GDPR) and ensuing efforts to change the WHOIS system - a key crime and abuse investigation tool - to comply with the GDPR. More recently, the COVID-19 global health emergency proved an illustration of existing challenges as pandemic-related domains registrations spiked.

ICANN's Advisory Committees, in particular the GAC, SSAC and ALAC, and various affected third parties have been calling upon ICANN org and the ICANN Community, to take further action[6].

[4] See GAC comment (19 September 2017) on the Final Report of the Statistical Analysis of DNS Abuse in gTLDs.

[5] See Section III.2 and IV.2 in the GAC Barcelona Communiqué (25 October 2018) pointing to surveys of impact on law enforcement in section 5.3.1 of the Draft Report of the RDS Review Team (31 August 2018) and in a publication from the Anti-Phishing and Messaging Malware and Mobile Anti-Abuse Working Groups (18 October 2018)

[6] See DNS Abuse and Consumer Safeguards discussion during the GDD Summit (7-8 May 2019)

Such further action would require that the ICANN community come to some form of consensus around a number of open questions.

Discussions of abuse mitigation and potential policy work in the ICANN Community generally revolve around:

- **The definition of DNS Abuse**: What constitutes abuse considering the purview of ICANN and its contracts with Registries and Registrars ?
- **The detection and reporting of DNS Abuse:** How to ensure that DNS Abuse is detected and known to relevant stakeholders, including consumers and Internet users ?
- **The prevention and mitigation of DNS Abuse**: What tools and procedures can ICANN org, industry actors and interested stakeholders use to reduce the occurence of abuse and respond appropriately when it does occur ? Who is responsible for which parts of the puzzle, and how can different actors best cooperate?

The GAC, in its efforts to improve security and stability for the benefit of Internet users overall, might wish to be actively involved in advancing the discussion on these issues so that progress can be made towards more effective abuse prevention and mitigation.

Leadership Proposal for GAC Action

1. **Consider the Recommendations of the Security Stability and Resiliency Review (SSR2)** in their FInal Report (25 January 2021), with a **view to providing GAC Comments prior to** ICANN Board's formal consideration due before 25 July 2021.

2. **Consider new contributions to the Definition of DNS Abuse** to reflect the threats landscape as experienced by law enforcement agencies, consistent with the GAC Statement on DNS Abuse (18 September 2019), in complement to the definition adopted by Contracted parties (October 2020) after the emergence of an industry-led Framework to Address Abuse (17 October 2019).

3. **Deliberate on possible next steps,** including through **concrete proposals to improve policies and/or improve contract provisions and their enforcement**[7] for addressing public policy issues related to DNS Abuse as identified through various Community efforts and GAC contributions:

    a. **The CCT Review Recommendations** per its Final Report (8 Sept. 2018), considering:
        - The ICANN Board action (1 March 2019) on all 35 recommendations and its subsequent adoption (26 January 2020) of an implementation plan proposed for the 6 recommendations it had accepted (6 September 2019);
        - GAC input in Comments on the Draft Report (19 May 2017), Comments on the Statistical Analysis of DNS Abuse in gTLDs (19 September 2017), Comments on additional Draft Recommendations (15 January 2018), Comments on the CCT Review Final Report (11 December 2018), Comments on the implementation plan (21 October 2019);
        - GAC Advice in the Montréal Communiqué (6 November 2019) *not to proceed with a new round of gTLDs until after the complete implementation of the recommendations in the Competition, Consumer Trust and Consumer Choice Review that were identified as "prerequisites" or as "high priority"*
        - Board Clarifying Questions (16 December 2019) regarding the GAC Montreal Advice – including topic of CCT Review and Subsequent Rounds of new gTLDs and the definition of "complete implementation"
        - GAC Response to Board Clarifying Questions (22 January 2020)
        - Board Reply to GAC Response to Clarifying Questions (11 February 2020) referring to its decision (26 January 2020) neither to accept nor reject the advice.

    b. **The GNSO Policy Development Process Working Group on New gTLD Subsequent Procedures** which determined in its Final Report (1 February 2021) that "*this PDP Working Group is not making any recommendations with respect to mitigating domain name abuse other than stating that any such future effort must apply to both existing and new gTLDs (and potentially ccTLDs)"* despite relevant recommendations on DNS

[7] Per GAC ICANN69 Communiqué Section IV.2: "*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";* and ICANN69 GAC Minutes: Section 2.2 "*Action Points: GAC PSWG to consider developing a concrete proposal regarding DNS Abuse Mitigation steps to prepare GAC for further discussions at ICANN70 (per GAC Wrap up Session discussion).*"

Abuse addressed to it by the CCT Review Team[8]. The GAC expressed its serious concerns with this decision in the GAC Comments (29 September 2020) on the Draft Final Report of this PDG WG, and its expectation of the GNSO Council to take swift action on this matter.

c. **Implementation and enforcement of key contractual obligations** in the Registry and Registrar Agreements, in particular:
   - **Specification 11 of the New gTLD Registry Agreement** and the related GAC Safeguard Advice in the Beijing Communiqué (11 April 2013), considering the conclusions of the Registry Operator Audit for Addressing DNS Security Threats (17 September 2019) and discussion in the GAC/ICANN Questions & Answers (30 May 2017), in the GAC Comments on the CCT Draft Report (19 May 2017) and in the GAC Comments on the SSR2 Draft Report (3 April 2020)
   - **The WHOIS Accuracy Program Specification** of the 2013 Registrar Accreditation Agreement which includes provisions for the verification, validation and accuracy of domain registration data, as discussed in the GAC Comment on the RDS-WHOIS2 Review Final Report (23 December 2019), and the **Registrar's Abuse Contact and Duty to Investigate Reports of Abuse** (Section 3.18) which is currently subject of a Contractual Compliance Audit launched for 153 selected registrars (15 January 2021). Both of these topics were also discussed in the GAC/ICANN Questions & Answers (30 May 2017) following GAC Advice in the Hyderabad Communiqué (8 November 2016)

d. **Community discussions of DNS Abuse and the effectiveness of related contract provisions**, both in terms of enforcement and enforceability:
   - **ICANN meeting sessions**: pre-ICANN66 webinar (15 October 2019), ICANN66 At-Large Session on End User Concerns (3 November 2019), ICANN66 Cross Community Session on DNS Abuse (6 November 2019), the ICANN67 At-Large Session on Contract Compliance (9 March 2020, the ICANN68 ALAC Session on Public Interest Commitments and the associated Dispute Resolution Procedure (22 June 2020), the ICANN68 Board GNSO Council Meeting which discussed possible Next Steps regarding DNS Abuse (14 June 2020) and the ICANN69 Plenary Session on DNS Abuse Issues (20 October 2020)
   - **Correspondence between the ICANN Board and the Business and Intellectual Property Constituencies** of the GNSO, including: the BC Statement Regarding Community Discussion on DNS Abuse (28 October 2019), a BC letter to the ICANN Board (9 December 2019), and subsequent response (12 February 2020); followed by a letter from the IPC to the ICANN Board (24 April 2020)

e. **Implementation of proactive anti-abuse measures by ccTLD Operators** that could inform gTLD registry practices such as those presented by the .EU and .DK ccTLDs[9]

[8] See Sub Pro PDP WG Final Report Recommendation 9.15 (p. 42) and related ICANN Board action on the CCT recommendations.
[9] See in particular a EURid presentation (28 January 2016) and .DK presentation during ICANN64 (12 March 2018)

f. **The RDS-WHOIS2 Review Recommendations** as detailed in its Final Report (8 October 2019) that are relevant to the legitimate use of WHOIS as a key crime and abuse investigation tool, considering GAC Comments (23 December 2019) and the ICANN Board Action to date (25 Feb. 2020)

4. **Consider and continue monitoring progress of key DNS Abuse Mitigation Efforts** in the ICANN Community to inform and promote elevated standards in practices and contracts:
   a. **Expected SSAC Proposals** for standardization of strategies and processes to address DNS Abuse identification and mitigation in the Report of its DNS Abuse Work Party to be release prior to ICANN70
   b. **Implementation of voluntary measures by gTLD Registrars and Registries** per the industry-led Framework to Address Abuse and ongoing discussion in the Internet & Jurisdiction Policy Network[10]
   c. **Improvements of ICANN's Domain Abuse Activity Reporting (DAAR)** as previously discussed by Registries, the GAC and SSAC, ad ICANN's Office of the CTO[11]
   d. 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** (including Specification 11 3b) **to two-third of the gTLD namespace** (they had only been applicable to New gTLDs so far). 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. **Consider public policy aspects of DNS over HTTPS (DoH)** in light of recent developments in the implementation of Encrypted DNS technologies, consistent with requests from GAC Members during ICANN69 and ongoing work by the GAC's Public Safety Working Group (PSWG) according to its Work Plan 2020-2021.

[10] The Internet and Jurisdiction Policy Network recently announced (22 February 2021) the launch of a toolkit on DNS Level Action to Address Abuses, which it is planning to present during a conference on Thursday 18 March.
[11] See most recently the RySG DAAR Working Group Report (9 September 2020), a response by ICANN's CTO (30 September 2020) and the OCTO update to the GAC (24 February 2021)

Relevant Developments

Overview of recent developments

- **During recent ICANN meetings**, GAC PSWG leaders provided detailed briefings to the GAC on the issue of DNS Abuse (see material of the GAC ICANN66 Session, ICANN68 Sessions and ICANN68 GAC Briefing on DNS Abuse, as well the ICANN69 PSWG Update to the GAC).
    - 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 a 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 (see ICANN66 Minutes, ICANN68 GAC Communiqué and Minutes as well ICANN69 Communiqué and Minutes).
    - The PSWG Work Plan 2020-2021 includes all these areas as part of its Strategic Goal #1 to Develop DNS Abuse and Cybercrime Mitigation Capabilities.

- **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 and in particular those pertaining to improving Domain Abuse Activity Reporting (DAAR) and the strengthening of compliance mechanisms.
    - The Final Report (25 January 2021) is now open for Public Comments (Closing 8 April 2021). The structure of the report was changed significantly. GAC Topics leads are currently reviewing the report and will be proposing a Draft Comment for GAC consideration.

- **The Working Party on DNS Abuse of the Security and Stability Advisory Committee (SSAC)** is expected to Report on its activities and findings prior to ICANN70
    - During the ICANN66 meeting, the SSAC reported to the PSWG its initiation of a Working Party on DNS Abuse, in which **a representative of the PSWG has taken part**.
    - Since then, the SSAC has signaled its intention not to declare a definition of DNS Abuse. Instead, the Work Party is expected to focus on roles of appropriate parties, building on Community perspectives and existing Frameworks. The Work Party's goal is to produce a report that outlines potential efforts to standardize community strategies and processes surrounding abuse identification and mitigation.

- **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** (including Specification 11 3b) **to two-third of the gTLD namespace** (they had only been applicable to New gTLDs so far). 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 presented their actions and lessons learned** prior and during the ICANN68 meeting while PSWG stakeholders reported ongoing efforts in collaboration with EU Members-States, Europol, ccTLD and registrars to facilitate reports, their review and their referral to relevant jurisdiction through the adoption of a standardized form to report domain/content related to COVID-19 and the establishment of single point of contacts for relevant authorities. These efforts build 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 reported during ICANN67.
- **Public Interest Registry (PIR)**, Registry Operator of .ORG and several New gTLDs launched (17 February 2021) the **DNS Abuse Institute** which stated objective is "*to bring together leaders in the anti-abuse space to: fund research, publish recommended practices, share data, and provide tools to identify and report DNS Abuse*". This initiative was presented to the GAC PSWG (3 March 2021) in advance of a webinar to be held by the Institute on the State of DNS Abuse on 16 March 2021.

- **ICANN Org's Multifaceted Response and Contractual Enforcement**
  - The ICANN CEO published a blog on 20 April 2020 detailing ICANN Org's Multifaceted Response to DNS Abuse
  - **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 a variety of cyber threats intelligence and incident response fora including the Forum of Incident Response and Security Teams (FIRST), the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), the Anti-Phishing Working Group (APWG), the US National Cyber-Forensics and Training Alliance (NCFTA) and the recent COVID-19 Cyber Threat Coalition (CTC) and Intelligence League (CTI).
    It is also developing systems and tools to assist in identification, analysis and reporting DNS Abuse:
    - 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), as was the ICANN Community during the ICANN68 meeting.
    - 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. It also monitor trends through its Identifier Technologies Health Indicators (ITHI). 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 tSSR2 Review Team (24 January 2020) which the GAC supported (see below). The Registry

Stakeholder Group who had also expressed their concerns with DAAR and was know to be working with ICANN in its evolution, recently made recommendations in a correspondence to ICANN's CTO (9 September 2020)

- ICANN OCTO also supports the recently launched (6 May 2020) **DNS Security Facilitation Initiative Technical Study Group**, 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"*. Recommendations are expected by May 2021.
- 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.
- **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 complaints.

Focus: Definition of DNS Abuse

As highlighted most recently during the GDD Summit (7-9 May 2019), there is **no Community-wide agreement on what constitutes 'DNS Abuse'**, in part due to concerns of some stakeholders with ICANN overstepping its mandate, impacts on the rights of users, and impact on the bottom line of contracted parties.[12]

There is, however, according the CCT Review Team, a **consensus on what constitutes 'DNS Security Abuse' or 'DNS Security Abuse of DNS infrastructure'** understood as including "*more technical forms of malicious activity*", such as malware, phishing, and botnets, as well a spam "*when used as a delivery method for other forms of abuse.*" [13]

The ICANN Contractual Compliance Department has referred to 'Abuse of DNS Infrastructure' and 'Security Threats' in its communications about audits of Registries and Registrars regarding their implementation of contractual provisions in the New gTLD Registry Agreement (Specification 11 3b) regarding "*security threats such as pharming, phishing, malware, and botnets*"[14] - and in the Registrar Accreditation Agreement (Section 3.18) - which refers to "*abuse contacts*" and "*abuse reports*" without providing a definition of the term 'abuse' specifically, but including 'Illegal Activity" within its scope.

From a GAC perspective, the definition of 'Security Threats' in the New gTLD Registry Agreement is in fact the transcription of the **definition given in the 'Security Checks' GAC Safeguards Advice** applicable to all New gTLDs in the Beijing Communiqué (11 April 2013).

Following the Board resolution (1 March 2019) directing ICANN org to "*facilitat[e] community efforts to develop a definition of 'abuse' to inform further action on this recommendation.*"[15].

During a pre-ICANN66 webinar on 15 October 2019 **PSWG and Contracted Parties discussed current issues and industry practices**. In preparation for this webinar, the Registry Stakeholder Group had issued an Open Letter (19 August 2019) discussing the registries views on the definition of DNS Abuse, the limited options registries have to take action on security threats and theirs concerns with ICANN's Domain Abuse Activity Reporting.

In response, the GAC issued a Statement on DNS Abuse (18 September), followed by the Business Constituency (28 October). In its Statement, the GAC recognised the CCT Review Team's definition of DNS Abuse as the "*intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names",* which in technical terms

---

[12] Indeed, the definition of Abuse Mitigation may carry consequences in terms of the scope of activity overseen by ICANN policies and contracts. While governments and other stakeholders are concerned with the impact of DNS abuse on the public interest, including the safety of the public and the infringement of intellectual property rights, registries and registrars are concerned with restrictions on their commercial activities, ability to compete, increased operating costs and liability for consequences registrants may incur when action is taken on abusive domains. Non-commercial stakeholders on their part are concerned with the infringement of freedom of speech and privacy rights of registrants and Internet users, and share with contracted parties concerns about ICANN overstepping its mission.

[13] See p.88 of the CCT Review Final Report (8 September 2018) as highlighted more recently in the GAC Statement on DNS Abuse (18 September 2019)

[14] The Advisory, New gTLD Registry Agreement Specification 11 (3)(b) (8 June 2017) provides a definition of 'Security Threats' as including "*pharming, phishing, malware, botnets, and other types of security threats.*"

[15] See p.5 of scorecard of Board Action on the Final CCT Recommendations

may take the form of Security Threats such as "*malware, phishing, and botnets, as well as spam when used as a delivery method for these forms of abuse*". The GAC recognised that the New gTLD Registry Agreement reflects this understanding in its Specification 11, in particular section 3a[16] and 3b[17].

Following the publication of the GAC Statement on DNS Abuse (18 September 2019) a set of **leading gTLD registries and registrars proposed a voluntary** Framework to Address Abuse (17 October 2019). Notably, this Framework includes in the scope of possible action by its adopters certain forms of "Website Content Abuse", which it considers "so egregious that the contracted party should act when provided with specific and credible notice". Since its publication and discussion during ICANN66, the list of signatories of this Framework has expanded to include other leading registrars and registries services providers, as well as a number of smaller industry players.

On 18 June 2020, the chairs of the **Registry and Registrar Stakeholder Groups** (collectively known as the Contracted Parties House of the GNSO, or CPH) shared with Community leaders that they **adopted a** definition of DNS Abuse mirroring exactly that of the industry-led Framework to Address Abuse:

> *DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam when it serves as a delivery mechanism for the other forms of DNS Abuse* [referencing the Internet and Jurisdiction Policy Network's Operational Approaches, Norms, Criteria, Mechanisms for definitions for each of these activities].

This definition **appears to confirm what the CCT Review Team called an existing consensus on "DNS Security Abuse** or DNS Security Abuse of DNS infrastructure" (CCT Final Report p. 8.) and **comports with the GAC's illustrative definition of "Security Threats"** in the 'Security Checks' GAC Safeguard Advice applicable to all New gTLDs of the Beijing Communiqué (11 April 2013) incorporated in the gTLD Registry Agreement under Specification 11 3.b.

[16] Specification 11 3a provides that "*Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.*"

[17] Specification 11 3b provides that "R*egistry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.*"

Focus: DNS Abuse Safeguards in Registries and Registrars Contracts

Building on the Law Enforcement Due Diligence Recommendations (October 2009), the GAC sought the **inclusion of DNS Abuse Mitigation Safeguards in ICANN's contracts** with Registries and Registrars:

- The 2013 Registrar Accreditation Agreement (17 September 2013) was approved by the ICANN Board (27 June 2013) after the inclusion of provisions addressing the 12 Law Enforcement recommendations (1 March 2012)
- The New gTLD Registry Agreement was approved by the ICANN Board (2 July 2013) after the inclusion of provisions in line with the GAC Safeguards Advice in the Beijing Communiqué (11 April 2013), consistent with the ICANN Board Proposal for Implementation of GAC Safeguards Applicable to All New gTLDs (19 June 2013)

After the first few years of operations of New gTLDs, during the ICANN57 meeting, **the GAC identified a number of provisions and related safeguards for which it could not assess effectiveness**. As a consequence, in its Hyderabad Communiqué (8 November 2016) the GAC sought clarifications on their implementation from the ICANN Board. This led to a dialogue between the GAC and the ICANN org, follow-up questions in the GAC Copenhagen Communiqué (15 March 2017) and a set of draft responses (30 May 2017) which were discussed in a conference call between the GAC and the ICANN CEO (15 June 2017). A number of questions remained open and new questions were identified as reflected in a subsequent working document (17 July 2017).

Among the outstanding topics of interest to the GAC, an Advisory, New gTLD Registry Agreement Specification 11 (3)(b) was published on 8 June 2017 in response to questions from some registry operators seeking guidance on how to ensure compliance with Section 3b of Specification 11 of the New gTLD Registry Agreement. **The Advisory offers one voluntary approach registry operators may adopt** to perform technical analyses to assess security threats and produce statistical reports as required by Specification 11 3(b).

As part of regular **audits conducted by the ICANN Contractual Department**, a targeted audit of 20 gTLDs on their "*process, procedures, and handling of DNS infrastructure*", between March and September 2018, revealed that "*there were incomplete analyses and security reports for 13 top-level domains (TLDs), as well as a lack of standardized or documented abuse handling procedures and no action being taken on identified threats.*"[18] Shortly thereafter, in November 2018, a DNS Infrastructure Abuse Audit of nearly all gTLDs was launched to "*ensure that the contracted parties uphold their contractual obligations with respect to DNS infrastructure abuse and security threats*". In its report of the latest audit (17 September 2019), ICANN concluded that:

- the vast majority of registry operators are committed to addressing DNS security threats.
- The prevalence of DNS security threats is concentrated in a relatively small number of registry operators.

[18] As reported in the blog post of 8 November 2018, Contractual Compliance: Addressing DNS Infrastructure Abuse: https://www.icann.org/news/blog/contractual-compliance-addressing-domain-name-system-dns-infrastructure-abuse

- Some Registry Operators interpret the contractual language of Specification 11 3(b) in a way that makes it difficult to form a judgment as to whether their efforts to mitigate DNS security threats are compliant and effective.

Contacted parties have taken issue with these audits as exceeding the scope of their contractual obligations.[19] ICANN org indicated that it will initiate an audit of registrars focusing on DNS security threats.

Focus: Non-Binding Framework for Registries to Respond to Security Threats

As part of the New gTLD Program, the ICANN Board resolved (25 June 2013) to include the so-called "security checks" (Beijing Communiqué GAC Safeguards Advice) into Specification 11 of the New gTLD Registry Agreement. However, because it determined that these provisions lacked implementation details, it decided to solicit community participation to develop a framework for "*Registry Operators to respond to identified security risks that pose an actual risk of harm (…)*". In July 2015, ICANN formed a Drafting Team composed of volunteers from Registries, Registrars and the GAC (including members of the PSWG) who developed the Framework for Registry Operator to Respond to Security Threats published on 20 October 2017, after undergoing public comment.

This framework is a voluntary and non-binding instrument designed to articulate guidance as to the ways registries may respond to identified security threats, including reports from Law Enforcement. It introduces a 24h maximum window for responding to High Priority requests (imminent threat to human life, critical infrastructure or child exploitation) from "*legitimate and credible origin*" such as a "*national law enforcement authority or public safety agency of suitable jurisdiction*".

Per its recommendation 19, the CCT Review Team deferred the task of conducting an assessment of the effectiveness of the Framework to a subsequent review[20] as the Framework had not been in existence for a long enough period of time to assess its effectiveness.

[19] See correspondence from the RySG (2 November 2019) to which ICANN org responded (8 November), and in comments posted on the announcement page (15 November): registries have taken issues with the audit questions as threatening enforcement action exceeding the scope of their contractual obligations [in particular underSpecification 11 3b] and indicated their reluctance to "*share with ICANN org and the community relevant information regarding our ongoing efforts to combat DNS Abuse […] as part of an ICANN Compliance effort that goes beyond what is allowed under the Registry Agreement*"

[20] CCT Review recommendation 19: *The next CCT should review the "Framework for Registry Operator to Respond to Security Threats" and assess whether the framework is a sufficiently clear and effective mechanism to mitigate abuse by providing for systemic and specified actions in response to security threats*

Focus: Consideration of the CCT Review Recommendations on DNS Abuse

Based on its analysis of the DNS Abuse landscape,[21] including consideration of ICANN's Report on New gTLD Program Safeguards (15 March 2016) and the independent Statistical Analysis of DNS Abuse (9 August 2017), the CCT Review Team recommended, in relation to DNS Abuse:

- The inclusion of **provisions in Registry Agreements to incentivize the adoption of proactive anti-abuse measures** (Recommendation 14)
- The inclusion of contractual provisions aimed at **preventing systemic use of specific registrars or registries** for DNS Security Abuse, including thresholds of abuse at which compliance inquiries are automatically triggered and consider a possible DNS Abuse Dispute Resolution Policy (DADRP) if the community determines that ICANN org itself is ill-suited or unable to enforce such provisions (Recommendation 15)

The ICANN Board resolved (1 March 2019) to place these recommendations in "Pending" Status, as it directed ICANN org to "*facilitat[e] community efforts to develop a definition of 'abuse' to inform further action on this recommendation.*"[22]

In light of Advice in the GAC Montréal Communiqué (6 November 2019) for the ICANN Board *"not to proceed with a new round of gTLDs until after the complete implementation of the recommendations [...] identified as "prerequisites" or as "high priority*", and the Board response to this advice (26 January 2020), the PSWG continues to monitor the consideration of key CCT-RT recommendations (6 September 2018) aimed at: the adoption of contractual provisions to incentivize proactive anti-abuse measures (Rec. 14) and to prevent systemic use of registrars or registries for DNS Abuse (Rec. 15); the improvement of research on DNS Abuse (Rec. 16); the improvement of WHOIS Accuracy (Rec. 18); and effectiveness of contractual compliance complaints handling (Rec. 20).

The GAC PSWG is also considering the Board resolution to proceed with ICANN's implementation plan (23 August 2019) for CCT Recommendations that were accepted in the Scorecard of ICANN Board Action (1 March 2019). The GAC had commented (21 October 2019) on this plan and highlighted some shortcomings regarding important recommendations to combat DNS Abuse, including the publication of the chain of parties responsible for gTLD domain name registrations (Rec. 17), more detailed information on contractual compliance complaints (Rec. 21), security measures commensurate with the offering of services that involve the gathering of sensitive health and financial information (Rec. 22).

Following the adoption by the Contracted Parties of a definition of the DNS Abuse the **GAC sought clarification from the ICANN Board during ICANN68** (see material of GAC/Board meeting on 24 June 2020), in connection with implementation of CCT-RT Rec. 14 (*ICANN to negotiate contractual provisions providing financial incentives for contracted parties to adopt proactive anti-abuse measures*), as to the status and plan regarding the facilitation of community efforts to develop a definition of 'abuse' and to inform further Board action on this recommendation. The GAC recorded in its ICANN68 Minutes that "*the Board will continue to support community dialogue as it*

[21] See Section 9 on Safeguards (p.88) in the CCT REview Final Report (8 September 2018)
[22] See p.5 of scorecard of Board Action on the Final CCT Recommendations

has been doing by facilitating regional and cross-community discussions, by conducting research and developing tools to help inform community discussions, and by providing speakers when requested".

During the ICANN68 meeting, the PSWG noted with ALAC stakeholders that progress on both implementation of accepted CCT-RT recommendation and consideration of pending recommendation is unclear. Unsatisfaction was also expressed at a communication (29 April 2020) of the **GNSO Policy Development Process Working Group on New gTLD Subsequent Procedures** that it is "*not planning to make any recommendations with respect to mitigating domain name abuse other than stating that any such future effort must apply to both existing and new gTLDs (and potentially ccTLDs)".* This is despite relevant recommendations addressed to it by the CCT Review Team, further supported by ICANN Board Action on these recommendations, as well as GAC Montréal Communiqué Advice (6 November 2019) and further GAC input as recorded in the GAC ICANN67 Communiqué (16 March 2020).

In its Final Report (1 February 2021), the GNSO Policy Development Process Working Group on New gTLD Subsequent Procedures confirmed its decision[23]. The GAC expressed its serious concerns on this matter in the GAC Comments (29 September 2020) on the Draft Final Report of this PDP WG, and its expectation of the GNSO Council to take swift action on this matter.

Focus: Discussion GNSO policy development on DNS Abuse Mitigation

Following the initial decision by the New gTLD Subsequent Procedures PDP WG not to make any recommendation in the area of DNS Abuse for future New gTLD contracts, the **GNSO Council discussed** in its meeting on 21 March 2020 **the possibility of initiating a Cross Community Working Group (CCWG)** on matters of DNS Abuse and possibly a subsequent GNSO PDP should new contractual requirements be needed.

It did not discuss an informal proposal by the GAC Leadership (12 May 2020) to consider a Birds of a feather discussion among relevant experts, including ccTLD operators, to scope any future policy effort.

As of 18 February 2021, this matter is still identified as "Unplanned" in the GNSO Council Action/Decision Radar, with the GNSO Council "*to determine next steps, if any, on DNS Abuse*". The GAC Leadership and relevant Topic leads are due to discuss this matter during a pre-ICANN70 GAC/GNSO Leadership call (8 March 2021), in preparation for the ICANN70 GAC meeting with the GNSO (24 March 2021).

[23] See Sub Pro PDP WG Final Report Recommendation 9.15 (p. 42)

Focus: Domain Abuse Activity Reporting (DAAR)

ICANN org's Domain Abuse Activity Reporting Project emerged as a research project concurrently to the GAC and PSWG engagement of the ICANN Board and Community on the effectiveness of DNS Abuse mitigation, between the ICANN57 (Nov. 2016) and ICANN60 meetings (Nov. 2017).[24]

The stated purpose of DAAR is to "*report security threat activity to the ICANN community, which can then use the data to facilitate informed policy decisions*". This is achieved since January 2018 by the publication of monthly reports, based on the compilation of TLD registration data with information from a large set of high-confidence reputation and security threat data feeds.[25]

As such, DAAR is contributing to the requirement identified by the GAC for publication of "*reliable and detailed data on DNS Abuse*" in the GAC Abu Dhabi Communiqué (1 November 2017). However, as highlighted in a letter from the M3AAWG[26] to ICANN org (5 April 2019), by not including security threat information on a per registrar per TLD basis, DAAR is still falling short of expectation from the GAC PSWG Members and their cybersecurity partners that it provides actionable information.

Recently, registries reported in an Open Letter (19 August 2019) interacting with ICANN's Office of the CTO "*to analyze DAAR with a view to recommending enhancements to OCTO to ensure DAAR better serves its intended purpose and provides the ICANN community with a valuable resource*". While registries recognized that "*some members of the community may rely on data provided in ICANN's Domain Abuse Activity Reporting - or DAAR - to support claims of systemic or widespread DNS Abuse*" they believe that "*the tool has significant limitations, cannot be relied upon to accurately and reliably report evidence of security threats, and does not yet achieve its objectives*".

The Registry stakeholder group reported on its work in its DAAR Working Group Report (9 September 2020), in response to which the ICANN CTO (30 September 2020): "*the majority of recommendations in the letter emphasize improving communication around the data that are exported from the DAAR system, as that communication is seen by the Working Group as potentially unclear, both in terms of the DAAR's current methodology documentation as well as in the DAAR monthly reports. While most of the recommendations focus on specific changes in the report, some (such as recommendation 3 which asks for measuring of the "persistence" of reported abusive activity) may require longer-term investigation and analysis.*"

During the OCTO update to the GAC (24 February 2021), the ICANN CTO discussed future plans in the development of DAAR: adding more ccTLDs to the scope of DAAR, continuing to work with the RySG DAAR Working Group, and exploring solutions to overcome challenges with accessing WHOIS data to build Registrar level metrics including: daily WHOIS queries only for blocklisted domains, random sampling of domains or getting approval to use data from Bulk Registration Data Access (BRDA).

---

[24] See cross-community sessions led by the GAC PSWG during ICANN57 (Nov. 2016), ICANN58 (March 2017) and ICANN60 (October 2017), as well as questions to the ICANN Board regarding the effectiveness of DNS Abuse Safeguards in Hyderabad Communiqué (8 November 2016), follow-up questions in the GAC Copenhagen Communiqué (15 March 2017) and a set of draft responses (30 May 2017) by ICANN org.

[25] For more information, see https://www.icann.org/octo-ssr/daar-faqs

[26] Messaging, Malware and Mobile Anti-Abuse Working Group

Current Positions

The current positions of the GAC are listed below in reverse chronological order:

- GAC ICANN69 Communiqué (23 October 2020) noting the GAC's belief that "*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"* in light of increasing momentum and constructive dialogue in the ICANN Community (see Section IV.2 p.6).
- GAC ICANN68 Communiqué (27 June 2020) noting "*that new efforts to tackle DNS abuse should not replace, but rather complement, existing initiatives to improve accuracy of registration data, such as the Accuracy Reporting System, and to implement policy on privacy and proxy services, which are currently on hold*" (see Section IV.3 p.7)
- GAC Comment (3 April 2020) on the SSR2 Review Team Draft Report
- GAC Comment on the RDS-WHOIS2 Review Final Recommendations (23 December 2019)
- GAC Statement on DNS Abuse (18 September 2019)
- GAC Comments on the CCT Review Final Report (11 December 2018)
- GAC Comment (16 January 2018) on New Sections of the CCT Review Team Draft Report (27 November 2017)
- GAC Comment on the Statistical Analysis of DNS Abuse in gTLDs (19 September 2017)
- GAC Comment on New gTLD Program Safeguards Against DNS Abuse Report (21 May 2016)
- GAC Barcelona Communiqué (25 October 2018) in particular sections III.2 GAC Public Safety Working Group (p.3) and IV.2 WHOIS and Data Protection Legislation (p.5)
- GAC Copenhagen Communiqué (15 March 2017) including Abuse Mitigation Advice requesting responses to the GAC Follow-up Scorecard to Annex 1 of GAC Hyderabad Communiqué (pp. 11-32)
- GAC Hyderabad Communiqué (8 November 2016) including Abuse Mitigation Advice requesting responses to Annex 1 - Questions to the ICANN Board on DNS Abuse Mitigation by ICANN and Contracted Parties (pp.14-17)
- GAC Beijing Communiqué (11 April 2013), in particular the 'Security Checks' Safeguards Applicable to all NewgTLDs (p.7)
- GAC Dakar Communiqué (27 Octobre 2011) section III. Law Enforcement (LEA) Recommendations
- GAC Nairobi Communiqué (10 March 2010) section VI. Law Enforcement Due Diligence Recommendations
- LEA Recommendations Regarding Amendments to the Registrar Agreement (1 March 2012)
- Law Enforcement Due Diligence Recommendations (Oct. 2009)

Key Reference Documents

- GAC Documentation on DNS Abuse
  - GAC ICANN68 Briefing on DNS Abuse (18 June 2020)
  - GAC Questions on Abuse Mitigation and ICANN Draft Answers (30 May 2017) per Advice in the GAC Hyderabad Communiqué (8 November 2016) and Follow-up in GAC Copenhagen Communiqué (15 March 2017)
- Definition of DNS Abuse (including Industry Stakeholders Perspective)
  - Contracted parties definition of DNS Abuse (October 2020)
  - Framework to Address Abuse (17 October 2019)
  - GAC Statement on DNS Abuse (18 September 2019)
- SSR2 Review FInal Report (25 January 2021
- RDS-WHOIS2 Review
  - Scorecard of ICANN Board Action (25 February 2020) on the Final RDS-WHOIS2 Review Recommendations
  - Final RDS-WHOIS2 Review Recommendations (3 September 2019)
- Competition, Consumer Choice and Consumer Trust Review
  - CCT Review Final Report and Recommendations (8 September 2018), in particular Section 9 on Safeguards (p.88)
  - Scorecard of ICANN Board Action on the Final CCT Recommendations (1 March 2019)
  - Statistical Analysis of DNS Abuse in gTLDs (9 August 2017)

Document Administration

Meeting	ICANN70 Virtual Community Forum, 22-25 March 2021
Title	DNS Abuse Mitigation
Distribution	GAC Members (before meeting) and Public (after meeting)
Distribution Date	Version 1: 11 March 2021