ICANN | GAC
Governmental Advisory Committee

ICANN 69 VIRTUAL ANNUAL GENERAL

Public Safety Working Group (PSWG) Update

Session 5 - PSWG Update to the GAC

Contents

Session Objective

The GAC Public Safety Working Group (PSWG) will provide an update on its work consistent with its strategic goals to mitigate DNS Abuse and cybercrime, preserve and improve access to domain registration data (and its accuracy) and ensure effective PSWG operations and stakeholders relations.

Background

Since 2003, representatives from law enforcement and consumer protection agencies around the world have been involved in Internet policy deliberations at ICANN and through the Regional Internet Registries (AfriNIC, APNIC, ARIN, LACNIC and RIPE NCC).

While public safety agencies at ICANN initially focused on the need for open and accurate WHOIS information for international law enforcement investigations, the work quickly grew to include the prevention and response to the exploitation of domain registrations for malicious or criminal purposes (also known as "DNS Abuse").

Through their early work with the GAC and the ICANN Community, public safety agencies have made important contributions that continue to shape ICANN policy deliberations and contracted parties obligations to this day. Such contribution include:

- **Recognition of the legitimate uses of WHOIS**, as reflected in the GAC Principles Regarding gTLD WHOIS Services within the GAC Lisbon Communiqué (28 March 2007). These principles are regularly referenced by the GAC when providing input (as in the recent GAC Comments on the RDS-WHOIS2 Review Recommendations, 23 December 2019) or Advice to the ICANN Board (see rationale of Advice in the GAC San Juan Communiqué, 15 March 2018);
- **Due Diligence Recommendations for ICANN**[1] which were endorsed in the GAC Brussels Communiqué (25 June 2010) and eventually led to contractual amendments in the 2013 Registrar Accreditation Agreement (RAA) adopted by the ICANN Board on 27 June 2013; and
- **Introduction of New gTLD GAC Safeguards** in the GAC Beijing Communiqué {11 April 2013) which led to specific Public Interest Commitment provisions in Specification 11 of the New gTLD Registry Agreement

In the GAC Singapore Communiqué (11 February 2015), the GAC agreed to establish a Working Group on Public Safety and Law Enforcement. During the ICANN53 meeting in Buenos Aires, the GAC endorsed the Terms of Reference of the Public Safety Working Group (PSWG) whose focus was to be "*those aspects of ICANN's policies and procedures that implicate the safety of the public*"

Issues

As reflected in its current Work Plan 2020-2021 endorsed by the GAC on 16 March 2020, the PSWG is seeking to:

- **Develop DNS Abuse and Cybercrime Mitigation Capabilities** (Strategic goal #1), that is developing capabilities of the ICANN and Law Enforcement communities to prevent and mitigate abuse involving the DNS as a key resource
- **Preserve and Improve Domain Name Registration Data Effectiveness** (Strategic goal #2), that is ensuring continued accessibility and improved accuracy of domain registration information that is consistent with applicable privacy regulatory frameworks

[1] See Law Enforcement Due Diligence Recommendations (Oct. 2009)

Leadership Proposal for GAC Action during ICANN69

1. **Consider recent developments in the ICANN Community** related to both DNS Abuse Mitigation and Access to gTLD Registration Data and their impact on members' law enforcement and consumer protection organizations.

2. **Deliberate on possible next steps for addressing overarching public policy issues related to DNS Abuse** as identified in previous GAC contributions, and **in particular consider following-up** with the GNSO Council, ALAC, ccNSO and possibly the ICANN Board **on possible avenues to address CCT Review Recommendations on DNS Abuse before the launch of subsequent rounds of New gTLDs** consistent with the GAC Montréal Communiqué Advice (6 November 2019).

3. **Discuss the status** of consideration and implementation **of recommendations pertaining to DNS Abuse issued by the CCT and RDS-WHOIS2 Reviews,** in light of ICANN Board Action as reported in:
    a. Board Action Scorecard on CCT Review Recommendations (1 March 2019)
    b. Board Action scorecard on RDS-WHOIS2 Review Recommendations (25 Feb. 2020)

4. **Consider progress of key DNS Abuse Mitigation Efforts more generally, in the ICANN Community** and in particular by Contracted Parties, ccTLD Operators and ICANN org, including with a view to promote elevated standards in practices and contracts:
    a. **Implementation of voluntary measures by gTLD Registrars and Registries** per the industry-led Framework to Address Abuse
    b. **Implementation of proactive anti-abuse measures by ccTLD Operators** that could inform gTLD registry practices
    c. **Contractual Compliance Audit of Registrars** regarding DNS Security Threats which was expected to follow the conclusion of a similar audit of Registries
    d. Improvements of ICANN's Domain Abuse Activity Reporting (DAAR) as previously discussed by Registries, the GAC and SSAC

5. **GAC Members to consider encouraging their relevant public safety agencies** (criminal and civil law enforcement, and consumer protection agencies), to share their experience, challenges and successes in the DNS space, and join the work of the PSWG where their operational experience, expertise and policy concerns are needed. The Working Group relies on the continued engagement of its stakeholders and continues to seek volunteers to contribute to and to take on a leading role in shepherding PSWG work.

Relevant Developments

DNS Abuse Mitigation

Per its Statement on DNS Abuse (18 September 2019), 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 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[2] and 3b[3].

In its efforts to *continuously assess whether ICANN has responsive and timely mechanisms to develop and enforce ICANN contractual obligations with gTLD registries and registrars*[4], the PSWG has focused on the following activities related to the mitigation of DNS Abuse:

- **During recent ICANN meetings**, PSWG leaders provided detailed briefings to the GAC on the issue of DNS Abuse (see ICANN66 Session and ICANN68 Sessions material). 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 ICANN68 Minutes for additional information). The PSWG Work Plan includes all these areas as part of Strategic Goal #2 to Develop DNS Abuse and Cybercrime Mitigation Capabilities. This briefing includes updates in several of these areas.
- **Competition, Consumer Trust and Consumer Choice Review recommendations**
    - 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).

[2] 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."*

[3] 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."*

[4] See Objectives of the PSWG in its Terms of Reference

- The 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 (see more on this topic below) 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 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 recent 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)

- **Discussion of possible GNSO policy development on DNS Abuse Mitigation**
  - Following the New gTLD Subsequent Procedures PDP WG decision 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 24 September 2020, this matter is identified as "Unplanned" in the GNSO Council Action/Decision Radar.

- **Adoption of measures to mitigate DNS Abuse by Registries and Registrars**
  - 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.
  - On 3 January 2020, ICANN org announced a proposed amendment of the .COM Registry Agreement which would **extend 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.

- **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.
  - **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.

  - Since the ICANN66 meeting, several sessions were dedicated to **Community discussion of the effectiveness of enforcement as well as the enforceability of current contract provisions** related to DNS Abuse, including:
    - ICANN66 Cross Community Session on DNS Abuse (6 November 2020)
    - ICANN67 At-Large Session on Contract Compliance (9 March 2020)
    - ICANN68 ALAC Session on Public Interest Commitments and the associated Dispute Resolution Procedure (22 June 2020)
  - PSWG Leaders are following **correspondence being exchanged** on these enforcement and enforceability matters, **between the ICANN Board and the Business and Intellectual Property Constituencies** of the GNSO:
    - BC Statement Regarding Community Discussion on DNS Abuse (28 October 2019)
    - Letter from the BC to the ICANN Board (9 December 2019)
    - Response from the ICANN Board Chairman to the BC Chair (12 February 2020)
    - Letter from the IPC to the ICANN Board (24 April 2020)
    - Response from the ICANN Board Chairman to the IPC Chair acknowledging the questions and pointing to a future meeting after ICANN68 (10 June 2020)

- **The Working Party on DNS Abuse of the Security and Stability Advisory Committee (SSAC)** is expected to Report on its activities and findings
  - 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.

- **Security Stability and Resiliency 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. Final recommendations of the SSR2 RT are now expected by October 2020 (according to a blog on 1 June 2020). A pre-ICANN69 progress update webinar is planned on 7 October 2020 at 1500 UTC.

- A number of DNS Abuse-related recommendations fall in the scope of the PSWG Work Plan and are consistent with CCT-RT Recommendations as well as previous GAC input regarding the definition of DNS Abuse, limitations of Domain Abuse Activity Reporting (DAAR), new contractual provisions, effectiveness of contractual compliance enforcement. Several recommendations point to new work streams also identified in the PSWG Work Plan 2020-2021 such as the inclusion of ccTLDs in DNS Abuse mitigation efforts, and the investigation of the security implication of DNS encryption technologies (DNS over HTTPS, or DoH).

- **Two particular current policy issues** are of interest to the PSWG as it relates to mitigating DNS Abuse: **Accreditation of Privacy/Proxy Services** and the **Accuracy of gTLD Registration Data**
  - The PSWG continues to seek the implementation of **accreditation of Privacy/Proxy Services** providers with an appropriate law enforcement disclosure framework in line with GNSO policy recommendations dating back to 2013. During ICANN68, law enforcement representatives reported to the GAC being impaired in identifying perpetrators of COVID-19 related abuse in 65% of cases because of non-disclosure of registration data protected by a privacy/proxy service. In the GAC Comments on the RDS-WHOIS2 Review Team Final Report (23 December 2019), the GAC recalled that the correlation between the use of privacy/proxy service and DNS Abuse is established, and reminded of its GAC Kobe Communiqué and GAC Montréal Communiqué advice to the ICANN Board to consider restarting this implementation. Most recently, the ICANN Board responded (25 February 2020) to a letter from the Coalition for Online Accountability (31 October 2019) referring to an ongoing ICANN review of the impact of EPDP policy recommendations on the PPSAI policy recommendation and implementation work completed to date.
  - **Accuracy of gTLD Registration data** is a policy area of high impact for the mitigation of DNS Abuse that the PSWG is pursuing. In its Comments on the RDS-WHOIS2 Review Team Final Report (23 December 2019), the GAC recalled its concerns regarding this systemic issue that negatively affects the security and stability of the DNS, noted that in its view registration data accuracy is not solely a responsibility of registrants, and concluded that enforcement of registrar contractual obligation by ICANN is critical and necessitates proactive monitoring of registration data at scale. This matter is currently discussed in the context of ongoing and future GNSO policy development, discussed in the next section of this briefing, and as well as in the ICANN69 GAC Briefing on WHOIS and Data Protection.

WHOIS: Accessibility and Accuracy of Domain Registration Data

Efforts by ICANN to bring WHOIS in compliance with the EU General Data Protection Regulation (GDPR) have created impediments for law enforcement and consumer protection agencies to access WHOIS data, which is a critical investigative tool for law enforcement. These impediments on investigations[5] have compounded existing challenges with the permanent and growing security threat environment and adversely impact Law Enforcement's ability to conduct investigations, notify victims in a timely manner, and disrupt ongoing criminal activity. This was recognized in the GAC Barcelona Communiqué (25 October 2018) and in a GAC letter to the ICANN Board (24 April 2019) prior to its adoption of recommendations from Phase 1 of the Expedited Policy Development Process (EPDP) on gTLD Registration Data.

This part of the briefing provides an update on PSWG activities to ensure continued accessibility and improved accuracy of domain registration information, consistent with applicable privacy regulatory frameworks and GAC consensus positions, and in support of the *ability of public safety organizations to investigate, prevent, attribute, and disrupt unlawful activity, abuse, consumer fraud, deception or malfeasance, and/or violations of national law*[6].

Since ICANN66, PSWG representatives have engaged in various aspects of the work of the EPDP, in support of the GAC Small Group and its representatives on the EPDP Team, as well as various other ICANN processes with continued relevance:

- **Requirement for Contracted Parties to provide Reasonable Access** to non-public gTLD registration data: the PSWG is considering the ICANN Board response (26 January 2020) to the Advice in the GAC Montréal Communiqué (6 November 2019) and the subsequent clarification (20 January 2020) provided by the GAC which aimed to ensure that while new policy is being developed, interim mechanisms are effective and their deficiencies addressed. As anticipated by the Board in response to GAC Advice, ICANN Contractual Compliance has deployed new complaint forms and is now reporting data[7] for alleged violations of the Temporary Specification on gTLD Registration Data since 1 February 2020.
- **Implementation of EPDP Phase 1 Recommendations**: while Phase 2 of the EPDP recently concluded and next steps remains a current focus of ICANN Community attention[8], the PSWG is also following and contributing to the implementation of the EPDP Phase 1 Policy recommendations. In particular, in light of previous GAC advice, last in the GAC Montréal Communiqué, PSWG representatives seek to ensure that the implementation is done in a timely manner that is consistent with the policy recommendations.

[5] See survey of Law enforcement agencies conducted by the RDS-WHOIS2 Review Team in section 5.2.1 of its Final Report (2 September 2019)
[6] Per Objectives in the PSWG Terms of Reference
[7] See ICANN Contractual Compliance Dashboard for August 2020 under headers "[Registry/Registrar] Complaints with Evidence of Alleged Violation of the Temporary Specification - 1 February 2020 to Date" and "[Registry/Registrar] Inquiries/Notices Related to Temporary Specification Sent and Closed in August 2020
[8] See ICANN69 GAC Briefing on WHOIS and Data Protection Policy

- **Standardized System for Access and Disclosure (SSAD) to non-public gTLD registration data** proposed in the Final Report of EPDP Phase 2 (7 February 2020)
    - PSWG participants have contributed case experience and expertise to inform positions and contributions of the GAC Representatives in the EPDP Team, in particular regarding the GAC Accreditation Principles (21 January 2020), automation of responses to law enforcement requests in jurisdiction, and Service Level Agreements for responses to urgent request and most recently the GAC Minority Statement on the EPDP Phase 2 Final Report (24 August 2020).
    - The PSWG continues to track progress of discussions in the GNSO Council regarding the so-called "Priority 2" Items not addressed in Phase 2 of the EPDP which include policy areas that have direct impact on DNS Abuse, such as the Accuracy of WHOIS information, and the accreditation of Privacy/Proxy Services providers.

- **RDS-WHOIS2 Review Team Recommendations**: following ICANN's report (6 February 2020) of the Public Comment period on the final recommendations of this Bylaw-mandated review, which included a contribution from the GAC (23 December 2019), the ICANN Board adopted a set of Board actions (25 February 2020).
  The GAC had highlighted the importance of several objectives and activities called for by the RDS-WHOIS2 Review Team (in which PSWG participants represented the GAC):
    - Establishing a Strategic Foresight Function for Regulatory and Legislative Developments affecting ICANN in furtherance of a new strategic goal adopted by ICANN in its 2021-2025 Strategic Plan. This recommendation was accepted by the Board
    - Proactive Compliance Enforcement and Reporting of WHOIS Data Accuracy, which the GAC argued must continue at scale and despite current impediments, given the importance of accuracy requirements for preventing and mitigating DNS Abuse, and the extent of estimated nature of inaccuracies. This recommendation is placed in pending status, to be considered by the ICANN Board upon completion of EPDP Phase 2
    - Accreditation of Privacy/Proxy Services and Validation of Registration Data Using Them, which was subject of Follow-up on GAC Advice in the GAC Montréal Communiqué (6 November 2019), in response to which (26 January 2020) the ICANN Board pointed to impact analysis being conducted by ICANN org in the context of the EPDP Phase 1 Implementation. This recommendation was also placed in pending status, to be considered by the ICANN Board upon completion of EPDP Phase 2

Current Positions

- GAC Minority Statement on the EPDP Phase 2 Final Report (24 August 2020)
- GAC Comments on the RDS-WHOIS2 Review Recommendations (23 December 2019)
- GAC Montréal Communiqué (6 November 2019)
- GAC Statement on DNS Abuse (18 September 2019)

Key Reference Documents

- PSWG Work Plan 2020-2021 (16 March 2020)
- ICANN66 GAC Briefing on DNS Abuse (30 October 2019)

Further Information

- ICANN68 Briefing on DNS Abuse (18 June 2020)
- ICANN69 GAC Briefing on WHOIS and Data Protection Policy (24 September 2020)

Document Administration

Meeting	ICANN69 Virtual Annual General Meeting, 13-22 October 2020
Title	PSWG Update
Distribution	GAC Members (before the meeting) and Public (after the meeting)
Distribution Date	Version 1: 24 September 2020