

---

## Public Safety Working Group (PSWG) Update

### Session 9

---

#### Contents

Background	2
Issues	2
Leadership Proposal for GAC Action	2
Relevant Developments	2
Current Positions	2
Key Reference Documents	2
Further Information	2

[Annex](#): PSWG Work Plan 2020-2021 For GAC Endorsement

#### Session Objective

PSWG Leaders to provide an update on developments since ICANN66, in particular in the area of DNS Abuse, and discuss Next Steps for the GAC, including endorsement of the PSWG Work Plan for 2020-2021

## 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<sup>1</sup>** 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 [Work Plan 2020-2021](#) (in annex to this briefing), consistent with the [previous work plan](#) endorsed by the GAC on 14 March 2018, 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

---

<sup>1</sup> See [Law Enforcement Due Diligence Recommendations](#) (Oct. 2009)

## Leadership Proposal for GAC Action during ICANN67

1. **Endorse the PSWG Work Plan 2020-2021** (in annex to this briefing), which will continue to guide PSWG work and enable tracking progress in the fulfilment of the PSWG's mandate
2. **GAC Members to consider encouraging their relevant public safety agencies** (criminal and civil law enforcement, and consumer protection agencies), to join the work of the PSWG by sharing operational experience, expertise as well as any policy concerns. 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<sup>2</sup> and 3b<sup>3</sup>.

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*<sup>4</sup>, the PSWG has focused on the following activities related to the mitigation of DNS Abuse:

- **During the ICANN66 meeting**, PSWG leaders provided a [detailed briefing to the GAC](#) on the issue of DNS Abuse and recent work in this regard. 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](#) 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.

---

<sup>2</sup> 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."*

<sup>3</sup> Specification 11 3b provides that *"Registry 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."*

<sup>4</sup> Per Objectives in the PSWG [Terms of Reference](#)

- **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 recent [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 PSWG is also considering the recent 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).

- **Security Stability and Resiliency Review Recommendations:** the PSWG is currently considering the [Draft Report](#) (24 January 2020) of the SSR2 Review Team.

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).

- **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). Since its publication and discussion during ICANN66, the [list of signatories](#) has expanded to include other leading registrars and registries services providers, as well as a number of smaller industry players.
- On 3 January 2020, ICANN org announced a [proposed amendment of the .COM Registry Agreement](#) which would extend to two-third of the gTLD namespace contractual provisions to facilitate the detection and reporting of DNS Abuse (including [Specification 11 3b](#)), which so far had only been applicable to New gTLDs. 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 wells measures to help measure and mitigate DNS security threats.

## 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<sup>5</sup> 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*<sup>6</sup>.

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.
- **Implementation of EPDP Phase 1 Recommendations:** while Phase 2 of the EPDP is ongoing a current focus of ICANN Community attention<sup>7</sup>, 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.
- **Standardized System for Access and Disclosure (SSAD) to non-public gTLD registration data** proposed in the [Initial 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 (see GAC Summary of Initial Report in Annex to the [ICANN67 Briefing on WHOIS and Data Protection](#) for more details).

---

<sup>5</sup> 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)

<sup>6</sup> Per Objectives in the PSWG [Terms of Reference](#)

<sup>7</sup> See [ICANN67 GAC Briefing on WHOIS and Data Protection Policy](#) (17 February 2020)

- The PSWG continues to track progress of some of the so-called [“Priority 2” Items](#) of 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 Comments](#) (23 December 2019) on the RDS-WHOIS2 Review Recommendations
- [GAC Montréal Communiqué](#) (6 November 2019)
- [GAC Statement on DNS Abuse](#) (18 September 2019)

## Key Reference Documents

- [PSWG Work Plan 2020-2021](#) for GAC Endorsement (7 February 2020) - Also in Annex
- [ICANN66 GAC Briefing on DNS Abuse](#) (30 October 2019)

## Further Information

- [ICANN67 GAC Briefing on WHOIS and Data Protection Policy](#) (17 February 2020)

## Document Administration

<b>Meeting</b>	ICANN67 Cancún, 7-12 March 2020
<b>Title</b>	PSWG Update to the GAC
<b>Distribution</b>	GAC Members (before meeting) and Public (after meeting)
<b>Distribution Date</b>	Version 2: 4 March 2020

**STRATEGIC GOAL 1 - PRESERVE AND IMPROVE DOMAIN REGISTRATION DATA EFFECTIVENESS**

Ensure continued accessibility and improved accuracy of domain registration information that is consistent with applicable privacy regulatory frameworks

	Work Item	Description	Topic Lead
1.1	<b>Swift Implementation of New gTLD Registration Data Policy</b> (EPDP Phase 1)	Monitor and contribute to the implementation of the EPDP Phase 1 policy recommendations, including via participation in the Implementation Review Team.	Laureen Kapin (US FTC)
1.2	<b>Effective Interim Mechanisms for Reasonable Access to Non-Public WHOIS Data</b> (EPDP Phase 1 Rec. 18)	Ensure that the interim requirements for Registries and Registrars to provide reasonable access to non-public registration data is implemented in a consistent and efficient way, that meets the investigative needs of law enforcement agencies, other public authorities, cybersecurity practitioners and other legitimate third parties. Where needs are not met, ensure there are adequate mechanisms in place to report complaints and enforce compliance.	Laureen Kapin (US FTC)
1.3	<b>Swift Implementation of a Standardized System for Access and Disclosure to Non-Public gTLD Registration Data</b> (EPDP Phase 2)	Monitor and contribute to policy development and subsequent implementation efforts towards the timely delivery of the future Standardized System for Access and Disclosure (SSAD) to non-public gTLD Registration Data that is compliant with relevant data protection law.	Chris Lewis-Evans (UK NCA)
1.4	<b>Accreditation of Public Authorities into Future Systems for Access to gTLD Domain Registration Data</b>	Support implementation by ICANN and relevant authorities at national/territory level, of the GAC-approved Accreditation Principles for Public Authorities to access any future Standardized System for Access and Disclosure of Non-Public Data.	Chris Lewis-Evans (UK NCA)
1.5	<b>Long Term Access to Non-Public Domain Registration Data for Law Enforcement and Cybersecurity Practitioners</b>	Ensure that the evolving needs of law enforcement and their cybersecurity partners are met through all relevant policies, systems and mechanisms available or envisioned, including through evolutions and improvements where necessary.	Chris Lewis-Evans (UK NCA)
1.6	<b>Improve gTLD Registration Data Accuracy</b>	Pursue and monitor efforts aimed at improving the overall accuracy of WHOIS data based on regular assessments and reporting of inaccuracy, appropriate compliance enforcement and implementation of industry best practices.	Tjabbe Bos (European Commission)



	Work Item	Description	Topic Lead
1.7	<b>Public Access to Legal Persons Registration Data</b> (Legal vs. Natural)	Monitor and contribute to efforts, including implementation of EPDP Phase 1 Recommendation 17, to assess the feasibility of public availability of non-personal information of legal entities involved in gTLD domain registrations. Follow-up on relevant GAC Advice to revisit the interim redaction of such data, which is not required under applicable data protection law.	Laureen Kapin (US FTC)
1.8	<b>Seek Reverse Lookup Capabilities for Law Enforcement Investigations</b>	Pursue the development and implementation of appropriate policies, processes and technologies, in the DNS ecosystem, to enable law enforcement to identify all assets controlled by nefarious individuals and entities under investigation.	Gabriel Andrews (US FBI)
1.9	<b>Implementation of the Privacy/Proxy Services Accreditation Policy</b>	Seek to resume and contribute to the implementation of an accreditation framework for Privacy/Proxy services providers, with appropriate disclosure requirements ensuring effective access by law enforcement to shielded registrant information.	TBD
1.10	<b>Collection and Publication of The Chain of Parties Responsible For gTLD Domain Name Registrations</b>	Monitor and pursue the implementation of CCT Review recommendation 17, including the collection and publication of registrars' reseller information, through relevant policy development processes and contractual negotiations between ICANN and contracted parties, as appropriate.	TBD
1.11	<b>Performance of ICANN's Mission in Relation to Domain Registration Data Services</b>	Monitor ICANN's performance in relation to its key bylaw responsibilities regarding accuracy, access and protection of gTLD registration data. Pursue implementation of relevant recommendations of the bylaws-mandated WHOIS-RDS Reviews.	Cathrin Bauer-Bulst (European Commission)

**STRATEGIC GOAL 2 - DEVELOP DNS ABUSE AND CYBERCRIME MITIGATION CAPABILITIES**

Develop capabilities of the ICANN and Law Enforcement communities to prevent and mitigate abuse involving the DNS as a key resource

	<b>Work Item</b>	<b>Description</b>	<b>Topic Lead</b>
<b>2.1</b>	<b>Implementation of CCT Review Recommendations for Subsequent Rounds of New gTLDs</b>	Monitor and contribute to the consideration and implementation of recommendations issued by the Competition, Consumer Trust and Consumer Choice Review Team as they relate to public safety and consumer protection.	Laureen Kapin (US FTC)
<b>2.2</b>	<b>Seek and Support Improved Registries Prevention and Response to Security Threats</b>	Improve proactive steps registries may take against Security Threats and supporting registration practices such as Domain Generated by Algorithms (DGA). Assess effectiveness of Specification 11 3b, its related Advisory and the Security Framework for Registries to Respond to Security Threats in implementing the GAC Beijing Communique Safeguards Advice.	Gabriel Andrews (US FBI)
<b>2.3</b>	<b>Seek and Support Registrars Adoption of Proactive Anti-Abuse Measures</b>	Seek elevation of contractual standards and practices including: registrant validation (for the entire resale chain), certification and consideration of bulk registrants as legal entities, and removal of DGA service offerings. Encourage and monitor adoption of voluntary frameworks aimed at addressing DNS Abuse.	Gabriel Andrews (US FBI)
<b>2.4</b>	<b>Survey and Review ccTLD Best Practices for adoption in the gTLD space</b>	Survey and review ccTLD best practices in mitigating security threats such as abuse prediction, registrant validation and verification policies, with a view to promote their adoption and to elevate contractual standards in the gTLD space.	Tjabbe Bos (European Commission)
<b>2.5</b>	<b>Ensure Enforceability and Effective Enforcement of Safeguards Provisions in ICANN Contracts</b>	Monitor and contribute to implementation of relevant policies and review recommendations to ensure that related requirements in Registries and Registrars contracts are enforceable. Monitor compliance audit and complaint reporting and assess effectiveness of enforcement and remediation procedures, including in addressing patterns of recurrent non-compliance.	Laureen Kapin (US FTC)

	Work Item	Description	Topic Lead
2.6	<b>Improve DNS Abuse Data Collection, Quantification, Reporting and Use by Relevant Stakeholders</b>	Seek the evolution of ICANN’s Domain Abuse Activity Reporting (DAAR) to ensure effective registration and abuse data collection, accurate quantification of Security Threats, and enable appropriate use of granular data and reporting by all relevant stakeholders, including law enforcement, registries and registrars.	Gabriel Andrews (US FBI)
2.7	<b>Improve Domain Seizure And Forfeiture Process, in Coordination With Contracted Parties</b>	Work with Contracted Parties and ICANN org to establish standard procedures for the management of domain names seized as part of law enforcement investigations, and for which Contracted Parties may continue to bear a financial responsibility.	Gabriel Andrews (US FBI)
2.8	<b>Follow-up on Previous GAC Advice Regarding the Mitigation of DNS Abuse</b>	Follow-up as appropriate on the Hyderabad and Copenhagen Communiqués aimed at assessing the effectiveness of previous GAC Advice in relation to the 2013 Registrar Accreditation Agreement and the New gTLD Registry Agreement. The GAC also sought to assess the contribution of the SSR and Contractual Compliance departments of ICANN org to the prevention and mitigation of domain name abuse.	Gabriel Andrews (US FBI)
2.9	<b>Assess Impact and Risks of DNS Encryption (DNS over HTTPS/TLS) on DNS Abuse Mitigation</b>	Engage in ICANN Community efforts to evaluate the impact of the adoption of DNS encryption technologies such as HTTPS (DoH) and DNS over TLS (DoT), in particular as it relates to current capabilities to mitigate DNS Abuse.	Katie Noyes (US FBI)

**STRATEGIC GOAL 3 - EFFECTIVE PSWG OPERATIONS AND STAKEHOLDER RELATIONS**

Ensure PSWG operations remain effective and consistent in meeting the needs of the GAC and public safety agencies.

	Work Item	Description	Topic Lead
3.1	<b>Maintain PSWG Work Plan</b>	Follow execution and adjustment of the work plan, consistent with PSWG Terms of Reference, GAC priorities, and ICANN Bylaws, taking into account current challenges and opportunities in ICANN Community processes.	Fabien Betremieux (GAC Support Team)
3.2	<b>Reporting and Coordination with the GAC</b>	Ensure alignment of PSWG activities with GAC guidance and priorities. Maintain GAC/PSWG leadership coordination. Coordinate GAC endorsement of key PSWG work products.	Laureen Kapin (US FTC) Cathrin Bauer-Bulst (European Commission)
3.2	<b>Develop and Maintain Talking Points</b>	Identify current and future policy issues and opportunities in support of the operational needs of public safety agencies. Seek expert input to inform contributions to the GAC and the ICANN Community.	Gregory Mounier (Europol)
3.3	<b>Develop PSWG Documentation for Effective ICANN Meetings</b>	Ensure continuous improvement of PSWG schedule and briefing documentation to facilitate PSWG Members' interactions with relevant ICANN stakeholders and processes during ICANN meetings.	Fabien Betremieux (GAC Support Team)
3.4	<b>Develop PSWG Collaboration Resources</b>	Develop PSWG usage of the GAC Website and other relevant resources to ensure ease of access to relevant public and private documentation	Fabien Betremieux (GAC Support Team)
3.5	<b>Contribute PSWG Experience into Guidelines for GAC Working Groups</b>	Follow and contribute to the work of the GAC Operational Principle Evolution Working Group, in particular regarding the development of Guidelines for GAC Working Group	Laureen Kapin (US FTC)
3.6	<b>Develop Participation and Leadership in PSWG Activities</b>	Provide regular and predictable structure of meetings to address the needs of interested GAC and PSWG stakeholders. Provide opportunities for participation at varying levels of expertise into PSWG work and initiatives.	Laureen Kapin (US FTC)