

The PSWG is an internal working group of the GAC that focuses on those aspects of ICANN’s policies and procedures that implicate the safety of the public. This document outlines the strategic goals and associated work items of the PSWG for 2023-2024. As work items evolve, this document may require updating and further details will be provided by the PSWG per the GOPE Working Group guidelines.

STRATEGIC GOAL 1 – DEVELOP AND SUPPORT DNS ABUSE AND DNS RELATED UNLAWFUL ACTIVITY MITIGATION METHODS AND CAPABILITIES

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

	Work Item	Description
1.1	Seek and Support Improved Registries Prevention and Response to Security Threats	Seek and support contractual standards and standard practices relating to mitigation of DNS Abuse. Make recommendations to the GAC and encourage proactive steps Registries may take against Security Threats and consider supporting appropriate registration practices associated with mitigating DNS Abuse. Assess effectiveness of Specification 11(3)(b), its related Advisory and the Security Framework for Registries to Respond to Security Threats in implementing the GAC Beijing Communique Safeguards Advice. Support uptake where appropriate for the "Framework to Address Malware and Botnet Domains at Scale" and other voluntary frameworks where they address security threats. This work stream includes engagement with the Registries on these topics
1.2	Seek and Support Registrars Adoption of Proactive Anti-Abuse Measures	Seek and support elevation of contractual standards and standard practices. Recommend to the GAC possible incentives for registrar actions aimed at mitigating DNS abuse. Encourage and track adoption of voluntary frameworks aimed at addressing DNS Abuse. Support timely responses to law enforcement requests for domain name registration data. This work stream includes engagement with the Registrars on these topics.
1.3	Review and identify ccTLD Best Practices for adoption in the gTLD space	Review and assess ccTLD best practices in mitigating security threats such as abuse prediction and registrant validation and verification policies, with a view to identify possible practical and implementable approaches and consider how they may inform elevated contractual standards in the gTLD space.
1.4	Support Effective Enforcement of DNS Abuse and Unlawful Activity Related Provisions in ICANN Contracts	Track and consider contribution to implementation of relevant policies and review recommendations to ensure that related requirements in Registries and Registrars contracts are sufficiently clear to be enforced. Track compliance audit and complaint reporting and assess effectiveness of enforcement and remediation procedures, including in addressing patterns of recurrent non-compliance. Recommend options to the GAC for improved implementation of DNS abuse related provisions in ICANN contracts

	Work Item	Description
1.5	Consideration of CCT Review Recommendations for Subsequent Rounds of New gTLDs	Track with a view to contributing to the GAC’s and other stakeholders consideration and ICANN implementation of the recommendations issued by the Competition, Consumer Trust and Consumer Choice Review Team and how they may contribute to public safety and consumer protection within subsequent rounds for new gTLDs.
1.6	Consideration of SSR2 Recommendations	Track with a view to contribute to the GAC’s and other stakeholders consideration and ICANN implementation of the recommendations issued by the Second Security Stability and Resiliency Review Team and how they may contribute to public safety and consumer protection.
1.7	Improve DNS Abuse Data Collection, Quantification, Reporting and Use by Relevant Stakeholders	Track for GAC awareness, and provide summarized briefings to the GAC on, DNS Abuse reports – such as ICANN’s Domain Abuse Activity Reporting (DAAR), the DNS Abuse Institute’s monthly Intelligence reporting, ad hoc reporting by specific Working Groups, and similar reports. On an approximately annual basis, supplement such reporting with briefs to the GAC providing public safety/cybercrime trend reporting which addresses the same DNS Abuse issues from the public safety / victim perspectives.
1.8	Improve Domain Seizure And Forfeiture Process, in Coordination With Contracted Parties	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.
1.9	Follow-up on Previous GAC Advice Regarding the Mitigation of DNS Abuse	Track, where appropriate the implementation of previous GAC input and advice on DNS Abuse. Assess the contribution of the SSR and Contractual Compliance departments of ICANN org to the prevention and mitigation of domain name abuse. Recommend options for the GAC to consider for more effective implementation of prior advice.

STRATEGIC GOAL 2 - PROMOTE LAWFUL ACCESS TO AND ACCURACY OF DOMAIN NAME REGISTRATION DATA

Identify and recommend steps to promote and support the continued accessibility and improved accuracy of domain registration information that is consistent with applicable privacy regulatory frameworks

	Work Item	Description
2.1	Support the Implementation of New gTLD Registration Data Policy (EPDP Phase 1)	Track and contribute to work regarding the implementation of the EPDP Phase 1 policy recommendations.
2.2	Effective Interim Mechanisms for Reasonable Access to Non-Public gTLD Registration Data (EPDP Phase 1 Rec. 18)	Assess whether the interim requirements for Registries and Registrars to provide reasonable access to non-public domain name registration data is being 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, recommend improvements to meet the required needs.
2.3	Support the Implementation of a Standardized System for Access and Disclosure to Non-Public gTLD Registration Data (EPDP Phase 2)	Track and contribute to the GAC’s work towards policy development and subsequent implementation efforts towards the timely delivery of the future Standardized System for Access and Disclosure (SSAD) to non-public gTLD domain name registration data that is compliant with relevant data protection law. Support work on proof of concept to encourage implementation of community policy recommendations.
2.4	Accreditation of Public Authorities into Future Systems for Access to gTLD Domain Name Registration Data	Support implementation of the GAC-approved Accreditation Principles for Public Authorities to access any future Standardized System for Access and Disclosure of non-public domain name registration data.
2.5	Long Term Access to Non-Public Domain Name Registration Data for Law Enforcement and Cybersecurity Practitioners	Track the evolving needs of law enforcement and their cybersecurity partners relating to lawful access to non-public domain name registration data are being met. Consider all relevant policies, systems and mechanisms available or envisioned, where applicable recommend to the GAC evolutions and improvements. Update PSWG/GAC to ensure knowledge of current access policies and actual practices.
2.6	Improve gTLD Domain Name Registration Data Accuracy	Track efforts making recommendations to the GAC and engaging with relevant stakeholders with a view to improving the overall accuracy of domain name registration data based on regular assessments and reporting of inaccuracy, appropriate compliance enforcement, and identification and implementation of industry best practices while taking into account different legislative developments, globally.

	Work Item	Description
2.7	Public Access to Legal Persons Domain Name Registration Data (Legal vs. Natural)	Assess the feasibility of public availability of non-personal information of legal entities involved in gTLD domain registrations. Support appropriate follow-up on GAC Advice to revisit the interim redaction of such data, where it is not required under applicable data protection law.
2.8	Lookup Capabilities for Law Enforcement Investigations	Track the development and implementation of appropriate policies, processes and technologies, in the DNS ecosystem, with a view to enable law enforcement to identify all assets controlled by nefarious individuals and entities under investigation. Follow deliberations of EPDP Phase 2A on the GAC’s proposal to publish unique pseudonymized email addresses for each registrant across TLDs, Track development and implementation of RDAP capabilities for pivot search.
2.9	Support Resumed Implementation of the Privacy/Proxy Services Accreditation Policy	Support the resumption of the implementation of an accreditation framework for Privacy/Proxy service providers, with appropriate disclosure requirements that promote effective lawful access by law enforcement to shielded registrant information.
2.10	Collection and Publication of The Chain of Parties Responsible For gTLD Domain Name Registrations	Develop input and recommendations relating to the implementation of CCT Review recommendation 17, including the collection and publication of Registrars’ reseller information. Advise the GAC on this topic throughout relevant policy development processes and contractual negotiations between ICANN and contracted parties, as appropriate.
2.11	Assess the execution of ICANN’s Bylaw requirements in Relation to Domain Name Registration Data	Assess ICANN’s performance in relation to its key bylaw responsibilities regarding accuracy, access and protection of gTLD domain name registration data. Advise the GAC on the implementation of relevant recommendations of the bylaws-mandated WHOIS-RDS Reviews.

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
3.1	Maintain PSWG Work Plan	Follow execution and adjustment of the work plan, consistent with PSWG Terms of Reference, GAC priorities, and ICANN Bylaws, taking into account ongoing work throughout the ICANN Community processes.
3.2	Reporting and Coordination with the GAC	Ensure alignment of PSWG activities with GAC guidance and priorities. Maintain GAC/PSWG leadership coordination. Coordinate GAC endorsement of key PSWG work products.
3.3	Develop and Maintain Talking Points	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.
3.4	Maintain PSWG Documentation for Effective ICANN Meetings	Ensure continuous improvement of PSWG schedule and briefing documentation to facilitate PSWG Members' interactions with the GAC and other relevant ICANN stakeholders and processes during ICANN meetings.
3.5	Maintain PSWG Collaboration Resources	Support PSWG usage of the GAC Website and other relevant resources to ensure ease of access to relevant public and private documentation
3.6	Develop Participation and Leadership in PSWG Activities	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.