27 June 2022

RE: Supplemental information.

Manal Ismail
Chair, Governmental Advisory Committee (GAC)

Dear Manal,

Congratulations on the successful conclusion of the Governmental Advisory Committee (GAC) meetings during ICANN74 in The Hague, Netherlands. The GAC's participation at the Internet Corporation for Assigned Names and Numbers (ICANN) is a critical element in strengthening the credibility of ICANN's global multistakeholder approach to policy development. Thank you for your leadership and the GAC's invaluable contributions to ICANN's mission.

The purpose of this letter is to address some apparent misunderstandings that arose during some of the GAC's Public Safety Working Group (PSWG) sessions in the Hague.

Concern: The design of the System for Standardized Access/Disclosure to Nonpublic Generic Top-Level Domain Registration Data (SSAD) creates a fragmented disclosure system, which results in thousands of registries and registrars individually applying their own versions of the balancing test when responding to third-party requests for access to personal registration data.

Response: The European General Data Protection Regulation (GDPR), not the SSAD, requires data controllers (in this case, registries and registrars), to decide whether or not to grant access to personal data. The GDPR also imposes liability on these data controllers who violate the privacy rights of data subjects by not protecting their data against unlawful disclosures. The SSAD is envisioned as a platform for facilitating the submission of requests to access registration data and the consideration of those requests by registries and registrars. It cannot take away the obligation of individual data controllers to apply the balancing test, nor can the SSAD relieve registries and registrars from liability for any unlawful disclosure of personal data. The SSAD also cannot eliminate requirements for requestors to demonstrate a legitimate interest in accessing nonpublic generic top-level domain (gTLD) registration data, where such requirements exist under applicable law. In brief, the GDPR imposes limits on the functionality of the SSAD that cannot be overcome by design changes made by the ICANN community.

Concern: ICANN Compliance can take enforcement actions against registrars that do not pay dues but not against those who violate Domain Name System (DNS) abuse obligations. ICANN Compliance believes that it lacks the tools to enforce DNS abuse obligations.

Response: ICANN Compliance has the tools it needs to vigorously enforce existing DNS abuse obligations as they apply to registries and registrars.

Registries and registrars are subject to obligations related to DNS security threats in their agreements with ICANN.

The following are examples of the abuse-related provisions enforced by ICANN Compliance:

- Under section 3.18 of the RAA, registrars are required to:
    - Take reasonable and prompt steps to investigate and respond appropriately to abuse reports
    - Maintain a dedicated point of contact (monitored 24/7) for reports of illegal activity filed by law enforcement, consumer protection, quasi-governmental or similar authorities within the registrar's jurisdiction, and review well-founded reports submitted by these authorities within 24 hours
    - Publicly display abuse contact information and abuse report handling procedures
    - Maintain records related to the receipt of and response to abuse reports and provide these records to ICANN upon reasonable notice

- Registry operators have an obligation to include a provision in their agreements with registrars, for registrars' agreements with registrants to prohibit registrants from engaging in certain activities, and requiring consequences for the registrants for such activities, including suspension of their domain. (Base Registry Agreement, specification 11 3(a)).
- Registry operators are required to periodically conduct a technical analysis to assess whether domains in their gTLD are being used to perpetrate security threats, such as pharming, phishing, malware and botnets. In addition, registry operators are required to maintain statistical reports on the number of security threats identified, including the actions taken as a result of these periodic security checks for the term of the Registry Agreement (RA), and to provide copies of these reports to ICANN upon request (Base Registry Agreement, specification 11 3(b)).
- Registry operators are required by Specification 6, Section 4.1 of the Base Registry Agreement to provide to ICANN and publish on their websites their accurate contact details. This includes a valid email and mailing address, as well as a primary contact for handling inquiries related to malicious conduct in the top-level domain (TLD). Registry operators are required to provide ICANN with prompt notice of any changes to such contact details.

ICANN Compliance enforces these obligations in response to external complaints, through proactive monitoring, and by conducting audit-related activities. Most investigations into compliance with abuse-related obligations are prompted by external complaints and resolved within the informal resolution stage of the compliance process.

From May 2021 through April 2022, Contractual Compliance:

- Initiated 575 cases with registrars pertaining to abuse report handling obligations
- Resolved and closed 575 abuse obligations-related investigations with registrars
    - Of these, approximately 40% resulted in the suspension of the domain name(s) or associated hosting services. In approximately 52% of the remaining cases, the registrar took other steps to investigate and respond, resulting for example in the removal of the allegedly abusive content from a website.

- Issued one formal notice of breach due to the registrar's failure to comply with abuse-related obligations with respect to reports involving two domain names engaged in the distribution of malware and the control of infected computers (bots), respectively
    - Upon receiving the breach notice, the registrar investigated the reports, decided to suspend both domains and presented a remediation plan to ensure timely compliance with abuse-related obligations moving forward.
- Issued another formal breach notice based on a failure of a registrar to comply with abuse obligations
    - An abuse report was issued in May 2022, which found a domain name allegedly engaged in phishing. This issue is ongoing.
- Completed audits focusing on abuse-related obligations
    - For example, the registry operator audit focused on DNS security threats conducted from November 2018 through June 2019, and the registrar abuse obligations audit conducted from 1 February 2021 through June 2021.
- Reviewed Registry-Registrar Agreements (RRAs) for completeness in terms of content mandated by the RA (as part of ICANN's review and approval of changes to a RRA contemplated in Article 2.9 of the RA), including abuse-related content in Section 3(a) of Specification 11 of the RA
- Published metrics and reports on complaints received, as well as resolutions to help inform ongoing community discussions related to DNS Abuse
    - The latest report on abuse-related complaints with data from May 2021 through April 2022 can be found here.

ICANN Compliance has the tools and resources it needs to enforce the DNS security threat obligations as they currently exist in the agreements with registries and registrars. Should these obligations change, either through community policy development processes or through contractual amendments, ICANN Compliance will ensure that it has the tools and resources needed to enforce the new obligations.

We hope this information is helpful and contributes to a constructive collaboration with the GAC on the important issues facing the community.

Sincerely,

Göran Marby
President and Chief Executive Officer
Internet Corporation for Assigned Names and Numbers (ICANN)