ICANN BUSINESS CONSTITUENCY

19 July 2021

Dear ICANN:

On behalf of ICANN's Business Constituency (BC), the following is submitted in reply to ICANN's Request for Information: Systems and Processes for Standardized System for Access and Disclosure (SSAD). While the BC does not intend to place a formal bid, our constituency is grateful to ICANN for the opportunity to lodge its constructive thoughts and recommendations.

Our input is provided in specific reply to Question 31 in RFI Sec. 6.5:

> *If you have any additional information, ideas, knowledge, assumptions, or comments related to this initiative that you think would be beneficial to share, please provide a file attachment of the same here (in the ICANN Sourcing tool).*

The BC welcomes the opportunity to contribute and invites ICANN to follow up with the BC for further discussion as warranted.

_____

The BC thanks the ICANN community volunteers and staff who have devoted hundreds of hours of work to Phases 1, 2, and 2a of the expedited policy development process (EPDP), which of course is meant, in part, to describe to the community a utilitarian SSAD. This has been a significant investment of time and resources, and the BC is grateful to volunteers and staff for their ongoing work.

Unfortunately, however, the SSAD, as currently proposed, falls short of the ongoing needs of the business, security, law enforcement, rights holders and other communities with legitimate interests in access to and disclosure of domain name registration data (know historically as Whois). The BC -- as well as the Governmental Advisory Committee, the Security and Stability Advisory Committee, the Intellectual Property Constituency, and the At Large Advisory Committee -- all have registered their concerns with the system as currently proposed, and have encouraged EPDP participants to reconsider their output with an eye toward making the system more robust and functional. The BC's contributions herein are designed to contribute to a more holistic solution to the problem.

Further, interceding factors have impacted, or should impact, community considerations. The most significant of these, of course, arises from the European Union (EU) via the European Commission's (EC) proposed directive on the security of network and information systems (the NIS2 proposal). This proposed directive clarifies European regulators' intentions about the availability and accessibility of Whois data which, naturally, should be strongly factored into EPDP deliberations regarding the SSAD. Regrettably, such regulatory developments mostly have been dismissed by the EPDP working group, which leads to the danger of creating a disclosure system that, from the outset, would be non-compliant with European regulation.

The need for a highly functioning SSAD is well documented inside and outside the ICANN community. The most recent data set is a [survey](#) conducted in 2021 by the Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG) and the Anti-Phishing Working Group (APWG) on the impact of Europe's General Data Protection Regulation (GDPR) on Whois. The survey's findings come as no surprise to those with a stake in domain name data registration policy: Lack of registrar responsiveness is up, as are delays in providing non-public data for legitimate purposes, both of which have led to, as documented in the survey report, "cyber-investigators…significantly impaired in their ability to investigate relationships between malicious domains and actors."

Data from the study clearly indicates the need for an SSAD that is:
- Much more responsive to the time-sensitive nature of online crime and abuse investigations;
- Capable of handling registration data requests in bulk, without the need to enter data item-by-item; and
- Not a cost burden to investigators, law enforcement, rights holders, and others entitled to non-public registration data for legitimate purposes.

It is the hope of the BC that these needs will be reflected in the eventual construct of the SSAD.

Here is specific input the BC requests ICANN to consider in its selection of vendors, and in the design of the SSAD:

The primary objective of any operational SSAD should be to provide qualified requesters with timely and consistent access to beneficial registrant data in a responsive manner.

Unfortunately, ICANN's bifurcation of its privacy/proxy implementation work and the EPDP policy work has resulted in a proposed SSAD which is not fit for purpose. Specifically, it has resulted in an accreditation and ticketing system that will most likely result in the referral of qualified requesters to privacy/proxy or similar data instead of timely access to the beneficial registrant information they seek.

The accuracy of and lack of access to relevant non-public registrant data has been a systemic problem, even pre-dating the creation of ICANN. However, instead of engaging in a *holistic* approach to finally solve the root problem, the ICANN community has engaged in a nearly two decades-long patchwork approach to address the resulting various harms. Instead of a comprehensive solution, the community, in reality, has had no solution at all. The arrival of the General Data Protection Regulation offers the ICANN community a generational opportunity to finally get it right. Regrettably, however, it is on the precipice of wasting that chance.

During ICANN's SSAD webinar on 13 July 2021, ICANN org stated that the purpose of the now underway Operational Design Phase (ODP) was to "provide the ICANN Board with relevant information to help decide if a recommendation is in the best interest of the ICANN community or ICANN." The BC submits that proceeding -- at an estimated cost of US$9 million -- with the design and implementation of an SSAD model that is static, does not enjoy a mechanism for evolution, and ultimately does not provide qualified requesters with timely access to the beneficial registrant information is not in the best interest of ICANN community or ICANN.

The RFI uniquely positions ICANN not only to complete its Operational Design Assessment but to address registrant verification and know-your-business-customer (KYBC) requirements.

While there was consensus within the EPDP on the requirement to properly identify potential requesters, emerging requirements (via the European Union's Digital Services act and NIS2 directive) impose similar requirements on domain name registration providers. Like the GDPR, these initiatives will require verification of registrant data to ensure accuracy, and have an extraterritorial scope that would have a direct and material impact on the broader domain name industry. The confluence of these facts gives ICANN org an opportunity to *proactively* address necessary changes rather than play catch-up as it did with the implementation of the GDPR. This should include addressing requirements for privacy/proxy services and providers.

Any operational SSAD solution must be built using standardized and open technologies to promote innovation and competition across a geographically diverse marketplace of providers.

It is the hope of the BC that ICANN does not repeat the mistakes of the Trademark Clearinghouse (TMCH) by designing and implementing a technologically cumbersome SSAD solution with limited value and vendor exclusivity. There already is a vibrant marketplace of companies providing identity verification and credential issuance services. This marketplace includes established companies such as Certificate Authorities (CAs) that have been doing identity proofing for decades, as well as newer providers using newer technologies.

ICANN should employ a solution that permits the interoperability of these different technologies, and in the interest of economic efficiency, permit some requesters to use existing forms of verified identity, provided that the identity provider issuing SSAD credentials meets the requirements established by ICANN.

Conclusion

While the BC has significant concerns regarding not only the outcomes of SSAD-related policy work but also regarding processes that no longer facilitate compromise, we remain committed to seeking improved outcomes within ICANN's multistakeholder model that take into account the legitimate needs of those within and outside the ICANN community.

ICANN Org now has the opportunity to build on newfound clarity about how GDPR applies to registration data -- clarity it has long sought from European authorities. Now, with better and more reliable information available to it, ICANN should take the responsible path and save time, frustration and resources by making a course correction today: Return to the GNSO Council the task of revising SSAD policy recommendations with an eye toward holistically addressing the matter (incorporating privacy/proxy services). ICANN org should actively promote innovative options that can be evaluated for viability before presenting another incomplete solution.

The BC stands ready to participate in such responsible policy development and looks forward to engaging further with ICANN community colleagues to achieve an equitable and usable SSAD.

--
This input is based on these previously-approved BC positions:

Comments and proposed amendments of the ICANN Business Constituency on provisions of the draft NIS2 Directive related to domain name registration data. May-2021, at https://cbu.memberclicks.net/assets/docs/positions-statements/2021/2021_05May_31%20BC%20position%20paper%20on%20EP%20NIS2%20amendments%20May%202021%5B19%5D.pdf

Comment for Board consideration of EPDP Phase 2 Policy Recommendations. Mar-2021, at https://cbu.memberclicks.net/assets/docs/positions-statements/2021/2021_03March_30%20BC%20comment%20for%20Board%20consideration%20of%20EPDP%20Phase%202%20Policy%20Recommendations.pdf

Minority Statement of the Business Constituency (BC) and Intellectual Property Constituency (IPC) on the EPDP Phase 2 Final Report. Jul-2020, at https://www.icannbc.org/assets/docs/positions-statements/2020/2020_07July_29%20Minority%20Statement%20of%20the%20BC%20and%20IPC%20on%20the%20EPDP%20Phase%202%20Final%20Report.pdf