Second Security, Stability, and Resiliency (SSR2) Review Team Final Report

https://www.icann.org/public-comments/ssr2-final-report-2021-01-28-en

NCSG Comments

April 07, 2021

About NCSG

NCSG represents the interests of non-commercial domain name registrants and end-users in the formulation of Domain Name System policy within the Generic Names Supporting Organisation (GNSO). We are proud to have individual and organizational members in over 160 countries, and as a network of academics, Internet end-users, and civil society actors, we represent a broad cross-section of the global Internet community. Since our predecessor's inception in 1999 we have facilitated global academic and civil society engagement in support of ICANN's mission, stimulating an informed citizenry and building their understanding of relevant DNS policy issues.

About this Public Comment Proceeding

Thank you for the opportunity to provide a comment on the SSR2 final report.

It is imperative for us to emphasize the importance of keeping the ICANN mission technical and the definition of DNS abuse limited to technical issues at ICANN. The SSR2 report however falls short of that.

Emphasis on intellectual property rights is wrong
The security and stability of the DNS is a technical function. It has nothing to do with intellectual property holders and their rights. They can protect their rights through other avenues. The report consistently brings intellectual property attorneys and their issues to the fore, which is irrelevant and can result in mission creep.

Registration Data: The report discusses the Registration Directory Services and insists that it is important to provide access to domain name registrants personal and sensitive data. As the report mentions too, EPDP (a policy development group) has already provided a policy document to provide access to registrants personal and sensitive data and its work has not finished yet. But the review team is not satisfied with the work-in-progress of the policy group. It

is not clear for us if it is even within the scope of the review team to get involved with providing a rather one sided feedback for a bottom-up consensus policy that has not been even implemented.[1] It surely comes across as those unsatisfied with the outcome of the EPDP, attempting to provide their feedback through the SSR2 review.
Further, the report claims: “The minority statements consistently found that the report recommendations did not appropriately balance the rights of those providing data to registries and registrars with the public interest to prevent harms associated with malicious activities that leverage the DNS”.[2] Then in a related footnote NCSG’s minority has been mentioned. We would like to clarify that our minority statement only addressed a couple of issues (in fact, one was about the SSR definition and ICANN mission) that were not resolved which would not protect registrants’ data at an optimal level. We believe the EPDP consensus policy can effectively provide the necessary security for the DNS.[3] If there are shortcomings in the EPDP final report, they are related to not protecting registrants’ data enough.
We believe this entire section on RDS and the comments related to EPDP need to be removed.

Centralized Zone Data Service: Brand protection and intellectual property protection are not security and stability issues.[4] But in this section “brand protection” is again invoked. This is a risky path to take and can lead to extending the ICANN mission and the definition of DNS abuse.

The ICANN DNS Abuse Activity Reporting: The review team argues that DAAR is inadequate for research. Because it believes that: “***Identifying registries and registrars harboring disproportionate levels of abuse*** would facilitate informed policymaking and add a measure of transparency and accountability to the domain name registration system that does not exist today”[5] DAAR was never set up for the purpose of auditing registries and registrars. It is not a “punishment mechanism” but a research mechanism. It should never have a mission such as identification of registries and registrars that harbor a disproportionate level of abuse. DAAR was recommended by GAC in multiple communiques and it provides useful statistics that can be helpful for security research. So it should not be discontinued at the request of the review team but the community as a whole should decide which direction it should take.

Definition of DNS abuse
In the Annex, the team tries to provide a definition for DNS abuse: “Intentional misuse of the universal identifiers provided by the DNS for cybercrime infrastructure and directed users to websites that enable other forms of crime, such as child exploitation, intellectual property infringement, and fraud.”(p.60)

---

[1] The SSR2, page 37.
[2] Ibid. page 38.
[3] ICANN Generic Names Supporting Organization, “Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process,” 31 July 2020, https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf.
[4] Ibid, page 39.
[5] Ibid, page 40

This definition of DNS abuse is very objectionable. DNS abuse has a definition limited to technical threats and it should not under any circumstances address intellectual property or other similar non-technical issues. We recommend scraping this definition from this review.

Final remarks:
Security, Stability and Resiliency of the Domain Name System are very important. However, as the NCSG has repeatedly said, SSR's definition and scope has to be defined according to ICANN bylaws and respect the limited technical definition of SSR. We believe the report falls short of that and attempts to address issues that are not and should never be related to SSR.