ICANN | GAC

Governmental Advisory Committee

Status	Final
Distribution	Public
Date	8 April 2021

Governmental Advisory Committee Comments on the Final Report of the Second Security, Stability, and Resiliency (SSR2) Review Team Final Report

Contents

Introduction

The GAC welcomes the work done by the SSR2 Review team since March 2017, and the submission of its Final Report for public comments on 28 January 2021.

The GAC attributes great importance to the stability, reliability, resiliency, security, and global interoperability of the DNS in particular and welcomes the opportunity to provide input for the final report.

As was indicated[1] in the prior GAC Comment (3 April 2020) on the SSR2 Review Team Draft Report (24 January 2020), the GAC welcomed many of the Draft Report's recommendations - particularly those pertaining to the improvement of DNS Abuse-related reporting activities and the strengthening of compliance mechanisms.

The GAC focuses on the following important topics:

1. General considerations regarding the review exercise;
2. Mitigating DNS Abuse (Recommendations 8-15)[2];
3. Overall views on the rest of the Final Report (Recommendations 1-7 and 16-24).

The GAC may also, of course, provide further views on the Report.

1) General views on the review exercise

The GAC reiterates its strong commitment to specific reviews, including to this review of how effectively ICANN is meeting its commitment to enhance the operational stability, reliability, resiliency, security and global interoperability of the systems/processes (internal/external) that affect the Internet's unique identifiers. The GAC stresses that issues at stake are substantive for ensuring security and safety of the Internet, and hence for public interest, and that urgently addressing these issues is even more critical in a COVID and post-COVID world where much of economic and societal activities are dependent on the Internet.

The GAC further respects the efforts made by the SSR2 Review authors to provide metrics-based recommendations with clear thresholds set for when such recommendations might be considered fully implemented or effective. These metrics are especially important, given the SSR2's assessment that none of the 28 SSR1 recommendations are deemed to have been fully implemented, which the GAC considers undesirable and not advisable for repetition, and that the lack of metrics to measure such implementation are a major contributing factor to that assessment. The theme of establishing clear definitions, metrics, and shared understanding of facts is thus both constructive and appreciated.

[1] In considering the recommendations made within the SSR2 Review Team Final Report, the GAC notes that its input provided for the review of the Draft Report stands; efforts made within this document to avoid repeating prior views should not be interpreted as abandonment of those positions.

[2] For clarity, please note this document will refer to the SSR2 recommendations by their group number. E.g., "recommendation 10" is intended to refer to all of the recommendations grouped within heading 10, to include 10.1, 10.2, and 10.3.

The GAC welcomes the recommendations that in its view would help reinforcing and improving the security, stability, and resiliency of the DNS. The Recommendations also provide a good basis for policy adaptations and new measures to mitigate DNS Abuse. The GAC highlights the report's finding that issues under consideration have not been addressed for many years. From that perspective, the below comments aim to support and reinforce the recommendations where necessary, with a view to their swift adoption and implementation.

2) Mitigating DNS Abuse (Recommendations 8-15)

SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties

The GAC agrees with the spirit of Recommendation 8, which seeks to incorporate the needs of the public safety and consumer interests into the contract negotiations. Clearly, these contracts have significance in terms of what might be done to counter DNS Abuse. We recognise though that contract negotiations between ICANN and the Contracted Parties do not currently include third parties and therefore would encourage ICANN to consult with independent security experts (i.e. non-contracted entities) for the purposes of developing and agreeing upon security-related provisions that can be incorporated into the contracts.

SSR2 Recommendation 9: Monitor and Enforce Compliance

The GAC shares the concerns with SSR2 Review authors that faith in the ICANN multistakeholder model can suffer harm when community guidance on topics as important as the stability, reliability, resiliency, security, and global interoperability of the DNS is not clearly incorporated within enforceable provisions of the contracts between ICANN and Registries and Registrars.

It is particularly concerning that ICANN Contractual Compliance would assert to the SSR2 Review Team in April 2018 - that "*current contracts with registries and registrars do not authorize ICANN org to require registries to suspend or delete potentially abusive domain names and are thus ineffective in allowing them to pursue those engaged in systemic DNS Abuse.*" This gap in the current contracts, identified by both ICANN Contract Compliance and the ICANN Board[3] demonstrates the need for improved and enforceable provisions to address DNS Abuse.

The GAC strongly supports for implementation the recommendations put forward in Recommendation 9 for the Board to:

[3] Botterman (ICANN Board Chair) Letter to Selli (Business Constituency Chair) https://www.icann.org/en/system/files/correspondence/botterman-to-selli-12feb20-en.pdf

- (9.1) direct the compliance team to "strictly enforce" SSR and abuse-related obligations as they may exist within contracts;
- (9.2) focus enforcement efforts on Contracted Parties who exist as outliers in the volume of abuse reporting they are responsible for (while noting that the rationale for setting the number of filed complaints or reports at 50 merits further analysis). Concerning this recommendation, the GAC stresses the need for the Final Report to specify in relation to contractual obligations the need for rigorous compliance mechanisms to ensure access to registration data for parties with legitimate purposes in line with *Draft Recommendation 15.3.* Moreover, given that the validation of domain registration data plays an important role in deterring criminals seeking anonymous domain registrations, the GAC welcomes this SSR2 recommendation to monitor and enforce Registry and Registrar contractual obligations to improve registration data accuracy as instrumental measure to mitigate DNS Abuse.
- (9.3) build ICANN community confidence in ICANN Org's compliance activities via external audits whose reports are publicly published, and to encourage compliance; and
- (9.4) be vocal advocates for enumeration and acquisition of tools they need to accomplish their SSR mission.

SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms

Recent ICANN sessions discussed and debated the meanings of terms such as "DNS Abuse". Some stakeholders view these disagreements as an obstacle to taking meaningful action to combat threats to the security, stability, reliability, and resiliency of the DNS. Consequently, the GAC welcomes and supports Recommendation 10's request that ICANN Org establish and maintain a web page containing working definition of DNS Abuse and related terminology, to include clear categorization of which security threats ICANN org sees as within - or outside - its remit, and to make consistent and referenced use of the terms contained therein.

The GAC Public Safety Working Group would be happy to participate in the proposed Cross-Community Working Group to be tasked with annually updating the abuse-related terminology, to ensure that existing and future cybersecurity threats, abuse, and criminal activity can be adjudicated by ICANN org as within - or outside - its remit.

Many in the GAC take the view that too much time has already been spent in arguing about the definition of DNS Abuse, rather than in tackling it. All manifestations of DNS Abuse – be it cybersecurity threats to the internet infrastructure or the distribution of harmful or illegal material on the internet - have adverse effects on the security of and trust in the internet. From that perspective, a problem-based approach, mapping the issues affecting the security of the DNS, could serve as a starting point for operational solutions to address those.

The GAC also welcomes that the report identifies Recommendations 9 and 10 as high priority.

SSR2 Recommendation 11: Resolve CZDS Data Access Problems

Without commenting on the specifics of this recommendation, the GAC acknowledges the importance and utility of cybersecurity researchers' and academics' work, noting that Public Safety officials regularly benefit from such work. To the extent that access to such data as the Centralized Zone Data Service (CZDS) has been promised - but not realized - the GAC would welcome improvements to such processes.

SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review

The GAC welcomes the recommendations put forward in Recommendation 12 which seek to improve usability, transparency, and reproducibility of existing DNS Abuse Reporting, while noting that such ideals should not allow the perfect to become the enemy of the good.

In particular, while the recommendation (12.1) to create a DNS Abuse advisory team without financial conflict of interest - who would set as priorities "*actionable data, validation, transparency, and independent reproducibility*"- is worthy of consideration, there exist potential improvements to the usability/actionability of DNS Abuse reporting mechanisms which may nonetheless require concessions in terms of independent reproducibility. The GAC would urge the Board to consider the use case of Bulk Registrant Data Access ("BRDA"), access to which could enable ICANN researchers to improve their DNS Abuse reporting granularity to the level of Registrar/Registry operator (as sought by 12.3), by mirroring all future contracts to the language recently adopted in Verisign's .com RA provision.[4] This language specifically allows for ICANN to use BRDA data to "analyze the operational stability of the DNS". Granting ICANN research staff broad access to BRDA data would enable them to overcome existing rate-limits to WHOIS lookups, which have thus far made registrar/registry specific reporting (12.3) infeasible. While external researchers who would seek to confirm the validity of ICANN reporting would still potentially be constrained by such rate-limits, the "actionability" of registrar/registry specific abuse reporting could reasonably be seen to be of such importance as to supersede the concerns of "independent reproducibility" in this specific use case.

Further, the GAC recognizes that seeking to provide greater transparency and non-commercial sharing of the source data behind ICANN's DNS Abuse reporting (12.2) may require nuance and compromise when obtaining the rights to share such data non-commercially. Specifically, the source data is understood to be commercially valuable only for a limited time, but valuable for ICANN DNS Abuse analysis and reporting indefinitely. If the data providers were to agree to contracts enabling non-commercial sharing of their data feeds, but only after a set delay, this would be viewed by GAC as an acceptable compromise (e.g. if the data

[4] .COM Registry Agreement Appendix 5A Registration Data Publication Services Specification, section 2.1 https://itp.cdn.icann.org/en/files/registry-agreements/com/com-appx-05a-pdf-27mar20-en.pdf

providers and ICANN agreed to non-commercial sharing after a delay of 30 days from the date the data was obtained by ICANN).

The GAC agrees that Contracted Parties should be recognized for their efforts to fight DNS Abuse (12.4), and that published reports of the actions taken (such as metrics on time-to-response to abuse reporting) are valuable, and would provide such Contracted Parties with a platform to highlight their contributions and successes.

Finally, the GAC considers that Recommendation 12 could further specify actions foreseen under *Draft Recommendation 13.1.4*, i.e. assistance activities to the Board and all constituencies in interpreting Domain Abuse Activity Reporting (DAAR).

SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting

The GAC strongly supports the creation of a centralized DNS Abuse complaint portal capable of automatically routing all abuse reporting to the relevant parties. While the GAC would be supportive of ICANN org taking responsibility for such a system, and thereby collecting directly the non-personally identifying metadata and complaint category data associated with such reporting, the GAC is aware that other organizations seeking to contribute toward the fight against DNS Abuse have shown interest in the creation of similar tools. Therefore as long as the tools are easy to locate, use, and are adopted readily by all gTLD contracted parties, and generate independently verifiable reporting based on complaints received, the GAC is agnostic as to the party operating such a complaint portal.

SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements & SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements

While the GAC has not yet taken a view on whether or not a Temporary Specification is necessary to accomplish the goals set forth in Recommendation 14, it nonetheless wishes to flag constructive specific recommendations contained therein.

The GAC in particular stresses the importance of urgent action on those security improvements-related recommendations, calling for concrete de-accreditation steps based on observable conduct and for creating incentives for DNS Abuse prevention and mitigation, in line with the ICANN org task as non-profit public benefit corporation to ensure oversight of DNS security, stability, and policymaking in the public interest.

The GAC also notes that CCT Review Recommendation 12 also saw value in the financial incentivisation (SSR2 Recommendation 14.5) of contracted parties encouraging them to reach certain DNS Abuse milestones. Such financial incentives, of course, are only possible when there first exists a shared understanding of which domains within a contracted party’s portfolio are perceived to be abusive (SSR2 Recommendation 14.2).

The GAC supports Recommendation 15 to develop an EPDP on anti-abuse policy and in particular Recommendation 15.2 calling for appropriate countermeasures and remediation actions for different types of abuse, time-frames for contracted party actions like abuse report/response report timelines, and ICANN Contractual Compliance enforcement actions in case of policy violations. In line with this Recommendation, the GAC stresses the importance for ICANN org to insist on the power to terminate contracts in the case of a pattern and practice of harboring or ignoring abuse by any Contracted Party.

The GAC stresses "not to proceed with a new round of gTLDs until after the complete implementation of the recommendations in the Competition, Consumer Trust and Consumer Choice Review that were identified as "prerequisites" or as "high priority"".

3) Overall views on Recommendations 1-7 and 16-24

The Final Report found that the SSR1 recommendations were not sufficiently measurable, which created obstacles to assessing the progress of their implementation. As expressed in the GAC comments on the SSR2 Review Draft Report, the lack of clear standards to assess implementation raises important questions about the challenges for the implementation of ICANN's accountability measures and the challenges for the ICANN Board to act in the context of Specific Reviews mandated by the ICANN Bylaws.

The GAC notes the SSR2 Review Team's findings concerning the 28 SSR1 Review recommendations, out of which none was implemented fully, and all remained relevant. In this regard the GAC supports the development of measurable performance indicators that would enable, on the one hand, the identification of the underlying obstacles to full implementation and, on the other hand, would provide valuable measurement methods for the implementation of future recommendations. The GAC thus agrees with the Final Report's **Recommendation 1** that ICANN org should perform a further comprehensive review of the implementation of the SSR1 recommendations, taking into account the findings offered by the SSR2 Review Team.

The GAC welcomes **Recommendations 2-7** on standard security practices and stresses the urgency for ICANN to implement them, in line also with the below considerations. The GAC encourages ICANN to seriously consider, pursuant to Community and expert views implementing Recommendations 2-7**,** which aim at creating a 'C-Suite' (Chief Security Officer or Chief Information Security Officer) level position responsible for all security-related matters and budgeting. While such a centralised role may have various benefits such as making ICANN's work more efficient, providing a single point of contact for reporting on all SSR-related matters or offering a single voice for the public interest (*in this regard see also Recommendation 8.1 above*), the GAC would not wish to presume expertise in ICANN's internal administration of executive functions. Notably, the centralization of powers within a single role should not be allowed to create a scenario in which resources put toward protection of ICANN org are incentivized over resources put toward protection of the DNS.

The GAC considers that **Recommendation 16** should specify clearly the need for balancing GDPR-type privacy considerations with the need to ensure access to non-personal data in line with the efforts under EPDP phase 2.A to ensure appropriate access to WHOIS registration data. Furthermore, the GAC considers that Draft Recommendation 16.2 (institutionalizing training and certifications for all parties in measuring, tracking, detecting, and identifying DNS Abuse) is an important awareness- building channel that could contribute to a common understanding of issues related to DNS Abuse; as such, it would have merited a place in the final report.

Finally, the GAC appreciates the SSR2 Review's highlighting of DNS Name Collisions as a significant security concern, and supports **recommendation 17**'s request for a clear policy for avoiding gTLD-related name collisions to be implemented prior to further gTLD expansion.