SAC110
SSAC Comments on the Second Security, Stability, and Resiliency (SSR2) Review Team Draft Report

A Comment from the ICANN Security and Stability Advisory Committee (SSAC)
19 March 2020

Preface

This is a public comment to ICANN's Second Security, Stability, and Resiliency Review Team (SSR2 RT), in response to a call for comments on the SSR2 draft report from the ICANN Security and Stability Advisory Committee (SSAC).

The SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), administrative matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to other parties, and the advice offered here should be evaluated on its merits.

Table of Contents

1 Introduction

The ICANN Security and Stability Advisory Committee (SSAC) appreciates the circulation of an early draft of the findings and recommendations from the Second Security, Stability, and Resiliency (SSR2) Review Team (RT) Draft Report,[1] and we thank the RT for the opportunity to comment on this interim report. In this comment the SSAC presents general comments about the SSR2 review and specific comments on individual recommendations in the report.

The SSAC has endeavored to meet the SSR2 timeline, and due to these time constraints this response may not be as comprehensive as the SSAC would have preferred. The SSAC would be happy to discuss these comments with the SSR2 RT at their convenience to explain any items that are unclear and require further elaboration.

There are some strongly-held mixed opinions within the SSAC on parts of the SSR2 report. Where there is SSAC consensus the document will state a view on behalf of the SSAC. Where there is a diverse set of opinions within SSAC, the SSAC comment will indicate this.

The SSAC would like to acknowledge the significant time and effort devoted by the members of the SSR2 Review Team and thank them for their contribution on this important topic.

2 General Comments

The ICANN Bylaws state a requirement for a, "*periodic review of ICANN's execution of its commitment to enhance the operational stability, reliability, resiliency, security, and global interoperability of the systems and processes, both internal and external, that directly affect and/or are affected by the Internet's system of unique identifiers that ICANN coordinates*".[2] The provisions relating to this review then enumerate five areas where the review is tasked to "*assess*" various specific aspects of this overall topic.

The SSAC's comments on this draft SSR2 report are based on an interpretation of what constitutes such an assessment and then applying this interpretation to the substance of the draft report.

2.1. Some SSAC reviewers expect, based on industry standards, that any review of ICANN's security and resiliency commitments would contain the following elements, as this would be helpful in evaluating the RT's recommendations:

- An assessment of the current environment which highlights changes in the environment since the last review;

[1] See Second Security, Stability, and Resiliency (SSR2) Review Team Draft Report, https://www.icann.org/public-comments/ssr2-rt-draft-report-2020-01-24-en

[2] See ICANN Bylaws, section 4.6 (c), https://www.icann.org/resources/pages/governance/bylaws-en

- An inventory of the ICANN organisation (ICANN org) and ICANN community's resources and capabilities; and

- A strengths and weaknesses assessment which highlights 1) where the ICANN org and ICANN community are effective, operating efficiently and meeting expectations, and 2) where there are potential issues and where performance on security, stability and resilience matters could be improved.

Such an environmental assessment would allow the report to determine where there is an effective security and stability framework in place, and where there are areas requiring further attention. From this foundation, the recommendations made in this review could be seen as proposed responses to be carried out by the organisation and the community that would, in the RT's opinion, mitigate or completely address these issues. The SSR2 RT should consider adding such an environmental assessment, inventory, and a strengths and weaknesses assessment to the final report, as this would be helpful to many readers, and make the report more actionable and easier to prioritize.

Further prioritization and consolidation of issues should be considered to make the report stronger. The report contains 27 high-priority recommendations and 4 medium-priority recommendations. The SSR2 recommendations are further elaborated in the report into 108 component recommendations, of which there are 96 high-priority recommendations. This large collection of actions is proposed to the ICANN Board for implementation without a substantive situational analysis, with little recognition of existing capability and strengths within the ICANN org and the ICANN community, and without a contextual analysis of weaknesses and potential areas of failure. As a consequence, it is challenging to assess the relative criticality of the report's recommendations and difficult to agree or disagree with the nomination of 27 of these high-level recommendations, or 96 component recommendations, as meriting a high priority for the ICANN Board's immediate attention. Without such further context the proposed prioritisation of these SSR2 recommendations it is very difficult for the SSAC to assess.

Other SSAC reviewers are of the view that the provisions of the Bylaws were taken as strict constraints in the SSR2 study, and topics not explicitly noted in the Bylaws were not evaluated and should not be included in this report.

2.2. Some SSAC reviewers believe that it would be helpful for the community and helpful in terms of overall accountability for SSR2 to have included an assessment of the extent to which the ICANN community, ICANN Board, and ICANN org are operating effectively from a security and stability perspective. Such an assessment could include consideration of the following questions:

- Is the community sufficiently mindful of security and resilience perspectives, and are such perspectives actively sought?

- Are security and stability needs being adequately addressed in the policy-making processes?

- What are the appropriate benchmarks and measurable metrics that would assess "adequacy" in this space?

- Are staff of ICANN org appropriately trained, adequately resourced, and adequately empowered to respond to concerns related to the security and resilience of the organisation?

Such an assessment would place more context on the recommendations in this report and determine if these recommendations are imperatives that address shortcomings in ICANN's current capabilities and procedures, or if they are refinements that are intended to bring the organisation's capabilities to a level that is commensurate with the current threat landscape.

2.3. It would be helpful if the SSR2 RT provided context and reasoning to substantiate each of the recommendations within the body of the report. It would also be helpful if they described the intention of the recommendations in terms of the resulting benefit and cost to the ICANN org, and ICANN community, if these particular recommendations were to be implemented.

3 Comments on Recommendations

The Summary of SSR2 recommendations notes that, "the SSR2 RT removed any recommendations from this report that did not clearly align with the strategic plan." No rationale is given as to why this filtering of recommendations was chosen, nor a description of what considerations were removed as a result of this alignment. The Bylaws do not place any such constraint on the Security, Stability, and Resiliency (SSR) review. The SSAC is concerned about the possibility of relevant and useful considerations that impact security and stability have been removed from this report. Even if they are not recommendations, such material should be noted in this report.

The SSAC also notes that this section of the report asserts, "All SSR2 RT recommendations align with ICANN org's strategic plan, and so are considered high priority." Yet 4 of the 31 recommendations are marked as medium priority. The SSAC believes it would be helpful for the report to indicate how these priorities were calculated.

The comments in this section are structured in the same manner as the SSR2 report, in four workstreams. It is noted that some recommendations in this report speak to specific items found in the International Organization for Standardization (ISO) standard ISO 27001/2 or the National Institute of Standards and Technology (NIST) Cyber Security Framework compliance mandates. What the review would have benefitted from was an overarching structured matrix as found in those compliance frameworks. This would have created a consistent template of what should be

reviewed, along with some measure of progress metrics that would act as a template for future reviews. The workstreams provide an overall template of the review, but it is not clear how comprehensive this adopted framework has proven, and the NIST Cybersecurity Framework may have provided some helpful structure to the review and this report. SSAC is aware that ICANN org has adopted the NIST Cybersecurity framework. Thus, had SSR2 RT adopted it as well, this shared framework could have provided alignment between ICANN org's framework and the review framework. With that in mind, the SSR2 RT might consider rearranging their final report along this structure, time permitting.

3.1 Comments on Workstream 1: Review of SSR1 Implementation and Impact

3.1.1. The SSAC notes that the SSR2 RT concluded that none of the First Security Stability and Resiliency Review (SSR1) recommendations have been fully implemented. Having reached this conclusion, the SSR2 report includes extensive discussion of why this has happened and how to improve the situation, including specific suggestions for each SSR1 recommendation in Appendix D.

In most cases this guidance appears to be helpful, but this conclusion raises an essential question on the feasibility of completing these 27 SSR1 recommendations. The report's consideration of the SSR1 recommendations notes that the underlying common issues with these recommendations do not appear to be a perceived lack of clarity in the original recommendation.

This would infer that other factors have contributed to this situation, including a lack of resources to implement the recommended measures, inappropriate scoping assumptions, and organisational decisions about priorities. However, the report is unclear in stating the reasons why SSR2 believes that these recommendations have not been fully implemented. It could also be the case that this further guidance from the SSR2 draft report restates the scope and purpose of the original SSR1 recommendations so that they are substantively new recommendations, but SSAC has not had the time to perform this comparative analysis in drafting this response. It would be helpful for the SSR2 final report to provide a more thorough clarification of the reasons why these SSR1 recommendations are, in SSR2 RT's opinion, not fully implemented.

3.1.2. In addition to the 27 outstanding SSR1 recommendations, the SSR2 draft report adds 26 new recommendations, making a total of 53. If all the specific items described in each of these 26 SSR2 recommendations are considered, then the count of SSR2 recommendations rises to 108, in addition to the 27 SSR1 recommendations.

The SSAC has some concerns about the viability of implementation of such a significant list of actions. Specifically, the SSAC is concerned about the extent, cost, sequence, and timeframe of the necessary actions required to implement all of these recommendations. Are there other measures that the SSR2 RT may wish to propose that would give the 135

proposed recommendations a significant prospect of avoiding the same incomplete fate as the 27 outstanding SSR1 recommendations by the time of the next SSR review?

3.1.3. Recommendation 2 states:

> *SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications*

Given that Recommendation 1 of the SSR2 report recommends the completion of the SSR1 recommendations, and Appendix D of the SSR2 report contains further details relating to findings and conclusions, including SSR1 Recommendation 9, SSR2 Recommendation 2 seems duplicative.

The SSAC believes that with so many recommendations from both reports where there appears to be overlap or adjacency between recommendations in SSR1 and SSR2 that they should group them accordingly, ensure that they are in fact distinct recommendations and not duplicates, and that the proposed actions and deliverables are unique. A table and categories for each class of recommendations in the reports would likely serve both the RT and the audience well.

3.1.4. Recommendation 3 states:

> *SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures*

Given that Recommendation 1 of the SSR2 report recommends the completion of the SSR1 recommendations, and Appendix D of the SSR2 report contains further details relating to findings and conclusions, including SSR1 Recommendations 12, 15, and 16, SSR2 Recommendation 3 seems duplicative. Please see the SSAC's feedback in 3.1.3 regarding the overlap or adjacency between recommendations in SSR1 and SSR2.

Notwithstanding this suggestion, the SSAC has some further comment on recommendations 3.1, 3.2, 3.3 and 3.4, as follows.

3.1.5. Recommendation 3.1. states:

> *ICANN org should address security issues clearly, publicly (with consideration for operational security, e.g., after an established moratorium and anonymization of the information, if required), and promote security best practices across all contracted parties.*

This recommendation prompted several questions from the SSAC: How does this differ from current ICANN org procedures? What factors led the SSR2 RT to reach this conclusion? Is there an inference that ICANN org has not addressed security issues?

The second part of the recommendation relating to promoting security best practices appears to be a distinct issue and merits further clarification. Is ICANN org deficient in this area, and does the SSR2 RT propose actions that would implement their recommendation? Specifically, where are the gaps in capabilities and actions by ICANN org or community in this area? What specific best practices does the SSR2 RT believe should be developed or implemented to address such gaps, and what do they envision as a useful framework to catalog, share, and enhance operational best practices related to a given topic that is relevant to the ICANN community?

3.1.6. Recommendation 3.2 states:

> *ICANN org should also capture SSR-related best practices in a consensus document, establish clear, measurable, and trackable objectives, and then implement the practices in contracts, agreements, and MOUs [Memorandums of Understanding].*

The SSAC believes that this recommendation is not practical and cannot be implemented in a reasonable time frame.

The assumption behind this recommendation is that such best practices are if not immutable then at least they are stable and largely consistent. There are many SSR best practices and some conflict with each other. Many best practices are bound to their context and in an evolving risk environment this means that such practices change at a similar rate. The documentation of best practices is an objective task calling on subject matter expertise, which does not lend itself to a consensus process with its implied compromises. A consensus-based task on security best practices could inherently pose a risk to the quality of its implementation.

Getting any “best practices” memorialized in contracts may require using the Generic Names Supporting Organization (GNSO) Policy Development Process (PDP), which would start the process over and would be subject to conflicting interests. In any case, the process itself would take years and the likelihood that the outcome would reflect the same needs and the same risk environment that existed when the effort commenced is low. Non-binding best practices are, by definition, optional (in so far as they are not standards specifications), and relevant parties might not implement them, leaving the effort ineffective. There is a definite need to consider new security-related policies that could become binding for ICANN’s contracted parties, but the proposed process using a consensus approach drawn from a very broad community of diverse interests does not appear to be an optimal solution.

3.1.7. Recommendation 3.3 states:

> *ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues should be communicated promptly to trusted, relevant parties (e.g., those affected or required to fix the given issue), such as in cases of breaches at any contracted party and in cases of key vulnerabilities discovered and reported to ICANN org.*

The actions in this recommendation are unclear. SSAC understands that ICANN org has, appropriately, already implemented responsible disclosure on a need-to-know basis. What is ICANN org not doing at present that it should do? How does one measure whether the reporting is done appropriately or not when such disclosures cannot necessarily be open disclosures?

3.1.8. Recommendation 3.4 states

> *ICANN org should establish a clear communication plan for reports to the community and produce regular (at least annual) and timely reports containing anonymous metrics of the vulnerability disclosure process. These communiques should contain responsible disclosure as defined by the community-agreed process and include anonymized metrics.*

SSAC understands that ICANN org has established a vulnerability disclosure process. What aspects of this recommendation differ from ICANN org's current practices?

3.1.9. Recommendation 4 states:

> *SSR1 Recommendations 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs [generic top-level domains]*

Given that Recommendation 1 of the SSR2 report recommends the completion of the SSR1 recommendations, and Appendix D of the SSR2 report contains further details relating to findings and conclusions, including SSR1 Recommendations 20 and 22, SSR2 Recommendation 4 appears duplicative. Please see the SSAC's feedback in 3.1.3 regarding the overlap or adjacency between recommendations in SSR1 and SSR2.

3.1.10. Recommendation 5 states:

> *SSR1 Recommendation 27 - Risk Management*

Given that Recommendation 1 of the SSR2 report recommends the completion of the SSR1 recommendations, and Appendix D of the SSR2 report contains further details

relating to findings and conclusions, including SSR1 Recommendation 27, SSR2 Recommendation 5 appears duplicative.

The SSAC is aware that ICANN org maintains a centralized risk matrix. To what extent do the measures proposed in SSR2 Recommendation 5 differ from current practice within ICANN org? What is the failing in the organisation's policies and procedures that motivate this recommendation? Please see the SSAC's feedback in 3.1.3 regarding the overlap or adjacency between recommendations in SSR1 and SSR2.

3.1.11. Appendix D enumerates each SSR1 Recommendation and assesses the level of implementation. This section of the report starts by summarizing the SSR2 RT's understanding of the reasons for the incomplete implementation of the SSR1 Recommendations:

> *"1. There is a lack of indicators, measurement, and goalposts that would allow the community and ICANN org to track and understand the security space and their own activities.*
>
> *2. There is a lack of publicly available evidence, definitions, and procedures, inhibiting observation of SSR activities, which leads to a lack of clarity regarding what is being done, when it is done, by whom, and how.*
>
> *3. There is also a lack of community review and accountability, denying the ICANN community opportunities to provide input on SSR matters.*
>
> *4. ICANN org does not currently have an overarching strategy, identifiable goals, or a clear and comprehensive SSR policy. Without a functional SSR strategy and integrated security and risk management (e.g., policy, procedures, standards, baselines,guidelines), SSR related responsibilities are not assigned, measured, and tracked, leading to a lack of transparency and accountability."*

The SSAC believes that these observations merit further consideration. The SSAC suggests that one way for the report to prompt such consideration is to rephrase these observations as proposals for implementation in the form of Recommendations in the main body of the document.

3.2 Comments on Workstream 2: Key Stability Issues within ICANN

3.2.1. Recommendation 6 states:

> *Create a Position Responsible for Both Strategic and Tactical Security and Risk Management*

The SSAC notes that ICANN org's current organisational structure is consistent with that used by many enterprises and this is conveyed in ICANN's SSR1 implementation report discussion of this matter. This SSR2 recommendation proposes a single individual on the ICANN org Executive Team that is responsible for this entire activity space, rather than harmonization and close coordination across the entire team. The SSAC notes that ICANN org Strategic Plan has adopted the organisational model of a shared responsibility in this area.

The SSAC believes that it would be helpful to understand the context of this recommendation in the light of the existing organisational structure and capabilities of ICANN org.

3.2.2. Recommendation 7 states:

Further Develop a Security Risk Management Framework

This is a restatement of Recommendation 5 and it is unclear what objective is achieved through this repetition. The SSAC comments in relation to Recommendation 5 apply here, including the tensions relating to the levels of open disclosure of risk profiles.

An appropriate attitude to risk is that an organisation's activities should be informed by risk, but not necessarily fully dictated by considerations of risk. This is the opposite of the direction espoused by recommendation 7.3.2.

The SSAC suggests that the report should clarify what is being requested here and clearly identify how this recommended action and the associated deliverables differ from related recommendations in this report.

3.2.3. Recommendations 8 and 9, respectively, state:

Establish a Business Continuity Plan Based on ISO 22301

Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented

The draft report at this point contains no commentary on any Business Continuity (BC) or Disaster Recovery (DR) plans that may exist within ICANN org. An uninformed reader may conclude from these recommendations that no such plans exist for ICANN org at the current time. Is this really the case?

An alternative interpretation of this section of the report, and of Recommendations 8 and 9, is that the SSR2 RT has assessed the current state of ICANN org's BC and DR plans and found that they could be improved by taking measures as set forth in the recommendations. A complete lack of BC and DR plans within the organisation would be a significant failing and the recommendations would be correctly judged to be high

priority imperatives. If these are recommendations to review these existing plans and make adjustments, it would be helpful to understand in what parts the current plans have been judged to be inadequate and why these specific recommendations to adjust these plans have been made by the SSR2 draft report.

The SSAC believes that the SMART[3] methodology that the SSR2 RT adopted should be used for these recommendations. Specific and clear proposals should be phrased as to how existing BC and DR plans should be revised to meet the criteria described in relevant ISO and ISO/International Electrotechnical Commission (IEC) standards.

3.3 Comments on Workstream 3: Review of Security, Stability, and Resilience of the DNS System

3.3.1. The Abuse and Compliance section of the report makes the claim that, "*ICANN org's record regarding their support of impactful SSR measures appears insufficient [in helping to ensure the security, stability, and resiliency of the Internet's unique identifier systems] when considered against the criticality of the systems in question.*"[4] It is unclear from the report to what extent this observed insufficiency is due to the significant and increasing extent of behaviours that undermine the security and stability of this system, or the extent to which ICANN org's SSR measures to date are insufficient. As Appendix F notes, it is clear that the domain name system (DNS) is under continual pressure from various forms of abusive and fraudulent behaviours, and the position is not improving. ICANN by itself does not have the ability to put an end to abusive behaviours in the DNS, and a realistic objective of any effective effort will involve a coalition of actors working to a common overall objective to mitigate this problem. The question is whether ICANN as a whole is performing adequately in taking up its share of responsibilities in this space or not.

The report makes the case that ICANN org's performance is inadequate in this area. The report notes that, "SSR2 RT found that the publications, statements, and related actions by ICANN org have consistently understated or omitted the impact of systemic abuse of the DNS and its use as a platform for launching systematic attacks on individual and organisational systems worldwide." On the other hand, the report also notes that, "ICANN org historically has stated in compliance and SSR2-related matters that it does not have the contractual tools necessary to enforce against registries and registrars." While the report identifies this tension, it is not clear how the proposed actions would resolve this in measurable ways.

It is clear that the nature of abuse in the DNS is so pervasive that elimination is not a realistic objective in the foreseeable future. It would be helpful for the report to note the larger picture of abuse and the necessarily scoped range of actions and consequences that

[3] Specific, Measurable, Achievable, Relevant, and Time-bound (SMART)
[4] See SSR2 Draft Report, page 31

lie within ICANN org's area of responsibility so that expectations as to the outcomes of the proposed measures are set to achievable levels.

3.3.2. Recommendation 10 states:

> *Improve the Framework to Define and Measure Registrar & Registry Compliance.*

Unless the underlying contractual commitments exist to compel contracted parties to act within clearly defined parameters and responsibilities, then the compliance measures proposed here seem ineffectual. Does the SSR2 RT believe that these contracts are sufficiently prescriptive with respect to behaviours and the residual issue is simply one of enforcement of compliance? As the report notes, "Compliance has few options to enforce the agreements"[5] and the measurements proposed in this recommendation appear to measure ineffectuality of enforcement. Are there measures that could have a beneficial outcome on improving this space?

This is acknowledged to be a complex space, and the SSAC agrees with the intended direction of Recommendations 10.1 and 10.2, while having some concerns over measurement of effectiveness of these proposed actions in their current form.

3.3.3. Recommendation 10.3 states:

> *Amend the SLA [service-level agreement] renewal clause from 'automatically renewed' to a cyclical four-year renewal that includes a review clause included (this review period would consider the level of compliance to the performance metrics by the Registrar and Registry and recommend the inclusion of requirements to strengthen the security and resilience where non-compliance was evident)*

Given that the report has noted some challenges relating to enforcement of agreements with contracted parties, it is unclear what the review and the subsequent "*recommend the inclusion of requirements"* precisely entails.

Which party is to perform these reviews? Is it the team envisaged in recommendation 10.2? If not then who would be performing such a review? If so, would these compliance officers possess the skills to be able to, "*recommend the inclusion of requirements to strengthen the security and resilience where non-compliance was evident"*? Who is to receive the review's recommendations? What criteria would be used by this party to assess these recommendations for additional requirements?

If requirements are being proposed, where is the contractual foundation to enforce these requirements? Does recommendation 10.3 implicitly refer to recommendation 15, where

[5] See SSR2 Draft Report, page 36

changes to the contractual conditions are proposed? Some further clarity on these recommendations would be helpful to understand both the detail of the proposed actions and the overall intent of these recommended measures.

3.3.4. Recommendation 11.2 states:

> *ICANN org and Board should implement the SSR-relevant commitments (along with CCT [Competition, Consumer Trust and Consumer Choice Review] and RDS [Registration Directory Service]/WHOIS2 Review recommendations) based on current, community vetted abuse definitions, without delay.*

If the underlying issue is that SSR2 has found evidence that the ICANN Board and ICANN org are not properly processing and acting on the outcomes of other reviews then it should say so explicitly. This recommendation that refers to recommendations from other reviews tends to suggest such a conclusion without actually saying so.

3.3.5. Recommendation 11.3 states:

> *ICANN Board, in parallel, should encourage community attention to evolving the DNS abuse definition (and application), and adopt the additional term and evolving external definition of "security threat"—a term used by the ICANN Domain Abuse Activity Reporting (DAAR) project, and the GAC [Governmental Advisory Committee] (in its Beijing Communique and for Specification 11), and addressed in international conventions such as the Convention on Cybercrime and its related "Explanatory Notes" —to use in conjunction with ICANN org's DNS Abuse definition.*

What specific actions did the SSR2 RT have in mind? It is challenging to understand the intended objectives of this particular recommendation given the imprecision of the term "encourage community attention".

3.3.6. Recommendation 11.4 states:

> *The ICANN Board should entrust SSAC and PSWG [Public Safety Working Group] to work with e-crime and abuse experts to evolve the definition of DNS Abuse, taking into account the processes and definitions outlined in the Convention on Cybercrime.*

It appears that the part of this recommendation that refers to SSAC actions is already underway with the formation of a DNS Abuse Work Party within SSAC. SSAC would be happy to brief the SSR2 RT on the objectives of this DNS Abuse Work Party. The SSR2 RT should consider whether to retain Recommendation 11.4 or simply note in the report that this activity is underway within SSAC.

3.3.7. Recommendation 12.1 states:

> *The ICANN Board should create a legal and appropriate access mechanisms [sic] to WHOIS data by vetted parties such as law enforcement.*

The SSAC largely agrees with the intent of this recommendation, while noting that this measure admits the risk of unintended consequences when considering the generality of the Internet and the diversity of bodies that enforce national regulations. How could ICANN minimize such risks in the context of the implementation of this recommendation?

The SSAC notes the volume of existing activities including the GNSO Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Policy Recommendations, General Data Protection Regulation (GDPR) compliance, PSWG, Registration Data Access Protocol (RDAP), RDS, "trusted notification" and have asked if the SSR2 RT have identified gaps in the current work that they believe should be highlighted through specific recommendations. This general recommendation appears not to take into account the existing activities in this area.

3.3.8. Recommendation 13 states:

> *Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program*

It is unclear if "completeness" here refers to the limited realm of second level domain names in gTLDs. If the intent is a far broader scope of "completeness" including all top-level domains (TLDs) and all labels to an arbitrary depth of delegation, then it would be helpful if the report indicated how such an extension of this activity could take place.

Also, the draft report should clearly indicate what is actionable with the specific recommendations, and more precisely, how effectiveness can be measured. Who should get the Domain Abuse Activity Reporting (DAAR) reports, and what should be made public, needs further attention in this recommendation.

The SSAC suggests that further consultation within the ICANN community on DAAR methodologies would be helpful.

3.3.9. Recommendation 14 states:

> *Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse.*

Given that ICANN has deliberately distanced itself from any role as a regulator of pricing in this space and holds a position where market forces determine pricing, then what is the context of this analysis and how could such a rigorous quantitative analysis inform the

mechanisms of market-based pricing? Further elaboration of the envisaged use of such an analysis would be useful to understand the intended effect of this recommendation.

If this recommendation is an oblique reference to heavily discounted prices being applied to bulk name registration practices, then is the underlying abuse issue pricing or bulk registration?

3.3.10. Recommendation 15 states:

> *Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse*

This appears to be a more detailed and clearer restatement of Recommendation 10.3, and in this light Recommendation 10.3 appears to be somewhat unnecessary.

The SSAC believes that preventing and impeding DNS abuse will be contributing factors in improved security for all, and assists in positive messaging regarding security measures in the gTLD space, the contracted parties, and ICANN itself. Accordingly, the SSAC is largely in agreement with the measures proposed in Recommendation 15. However, it would be difficult to understand the precise extent to which these measures would mitigate abuse, so caution should be exercised in phrasing metrics relating to the implementation of this measure in terms of levels of abuse.

3.3.11. Recommendation 16 states:

> *Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats*

The SSAC notes that this recommendation may be premature, as it presupposes the results from the activity proposed in Recommendation 14.

The SSAC has some concerns regarding the propriety and practicality of this recommendation. This proposal may transfer abuse behaviour into those parts of the domain name space that are not directly subject to the same incentives and constraints. Such a program may be extremely difficult to manage and its effectiveness difficult to measure.

This recommendation also proposes a shift of ICANN’s role, as ICANN has moved away from a price regulatory role and towards an environment where pricing is a function of market dynamics.

More generally, the SSAC believes it is an inherent responsibility of service vendors on the Internet to keep their businesses free of crime and abuse. It should not require monetary rewards, and such reward schemes do not exist in other industries.

3.3.12. Recommendation 17.1 states:

> *ICANN org should establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties.*

Some SSAC reviewers have noted that there are various views of the efficacy of introducing an intermediary in the process of abuse reporting, including the view that ICANN should not play an exclusive role as an intermediary in the abuse complaint process.

The SSAC sees value in tracking and measuring instances of abuse as a supplement to the DAAR activity and in related efforts responding to DNS abuse.

The SSAC suggests that this recommendation be given a clearer rationale and also should note that any implementation of such a measure should carefully mitigate the inherent risks of undertaking this role of intermediary in abuse reporting.

3.3.13. Recommendation 18 states:

> *Ensure that the ICANN Compliance Activities are Neutral and Effective*

The SSAC is unsure of how this recommendation materially differs from Recommendations 10 and 15.

It would be helpful in this report if all the recommendations concerning specific activities or responsibilities, for example contract management, be consolidated in the report.

3.3.14. Recommendation 19 states:

> *Update Handling of Abusive Naming*

The rationale that reducing the potential for name similarity contributes to improved security of the DNS can be countered by the desire to express names meaningful to humans in the DNS in the languages, scripts and glyphs that humans use. There is a tension here between utility and security that the report does not cover in sufficient depth. SSAC notes that Recommendations 19's consideration to 'update handling of abusive naming' may be an inappropriate designation of responsibility.

In the public DNS Abuse community session in ICANN 66 there were many statements made by various communities (including Law Enforcement, the Computer Emergency Response Team (CERT) community, contracted parties and ICANN) that were intended to delineate individual responsibilities and cooperate within their realm of authority. These recommendations would benefit from an assessment of what falls under ICANN org's remit to enforce, and what efforts ICANN org may be able to facilitate to support a broader community of interest.

3.3.15. Recommendation 20.1 states:

> *ICANN org should complete the development of a suite for DNS regression testing*

The DNS name resolution infrastructure is a large and highly diverse environment, and ICANN bears no responsibility for its operation. This environment includes the use of a small number of open source implementations of name resolution and name server software, but it also includes a diversity of various DNS operational libraries. These DNS libraries are integrated into other applications, are used by Original Equipment Manufacturers (OEMs) who customize implementations of DNS service functions, and used in private codes in various contexts.

It is useful to understand how various available implementations of DNS name services operate, but it must be remembered that almost any collection of DNS software would by no means include the entirety of the DNS service environment. There are no well understood means of measuring how many end users and services use any particular software bundle, directly or indirectly.

3.3.16. Recommendation 20.2 states:

> *ICANN org should ensure that the capability to perform functional testing of different configurations and software versions is implemented and maintained*

It is unclear to the SSAC what objective is achieved from this recommendation.

The SSAC observes that the Root Server System Advisory Committee (RSSAC) Caucus developed such a program,[6] and notes the report from the RSSAC Caucus Work Party states "there was limited use of the testbed after it was completed."[7] The SSAC believes that the work is useful and important to the larger community. It is suggested that the recommendation be revised to recognise the existing activity and to include some proposed measurable outcomes.

3.3.17. In the section dealing with the management of the Key Signing Key (KSK) rollover the report finds that: "The review team found no evidence that the propagation delay between publication to each of the letters, and then to each of a letter's instances, is well understood. Propagation delay is (for example) a relevant aspect of ensuring that validating resolvers are able to retrieve the same DNSKEY RRset, and rollover timing can be predictable."[8] The interactions of DNS resolvers with respect to multiple instances of authoritative data, and the interactions with cached data held in various recursive

[6] See Resolver Testbed, https://github.com/icann/resolver-testbed

[7] See Report on the Conclusion of the RSSAC Modern Resolvers Work Party, https://community.icann.org/download/attachments/96208150/Report%20on%20the%20Conclusion%20of%20the%20RSSAC%20Modern%20Resolvers%20Work%20Party.pdf?version=1&modificationDate=1580815571000&api=v2

[8] See SSR2 Draft Report, page 44

resolvers are appreciated in the design of the KSK role. The report's assertion relating to propagation delay is technically fallacious in this context.

3.3.18. The paragraph in the draft report beginning with, "Software and systems process analysis is a research branch of computer science's software engineering …"[9] appears to stem from an incomplete picture of the particular environment of the DNS. Various groups, including the KSK Design Workgroup, the Internet Engineering Task Force (IETF) DNS Operations Working Group and a number of DNS research groups all studied the KSK roll and the collective conclusion was that the DNS is sufficiently opaque that the trust state of validating resolvers in advance of a KSK roll is unknowable. [10] The hypothetical question of "what is the impact of a KSK roll" is quantitatively unanswerable and this paragraph in the report heads off in a direction which is misleading and inaccurate with respect to this particular issue.

Some SSAC reviewers suggest that this paragraph, and the preceding paragraph beginning with, "For example, the global DNS Root .." should be deleted from the draft SSR2 report.

3.3.19. Recommendation 21.1 states:

> *ICANN org should implement the recommendations from SAC063 and SAC073 in order to ensure the SSR of the KSK rollover process.*

If the underlying issue is that the SSR2 review has found evidence that the ICANN Board and Org are not properly processing and acting on the outcomes of other reviews and sources of advice, then it should say so explicitly in this report. This recommendation suggests such a conclusion, namely that the ICANN Board and Org are not paying due attention to SSAC advice, without actually saying so.

SAC063 contains five recommendations that were phrased in an environment of evolving understanding of the behaviours of Domain Name System Security Extensions (DNSSEC) in the DNS. The SSAC notes that recommendations 3 and 4 have been considered complete since the beginning of the Action Request Register (ARR) tracking of SSAC advice to the ICANN Board.[11] At the time of this comment,[12] recommendations 1, 2, and 5 are in Phase 5 | Close Request of the ARR, which indicates the "item has been implemented and is pending confirmation by the ICANN Board."[13] Were the same issue to be reviewed in the light of experiences following the first KSK roll it appears to be the

[9] See SSR2 Draft Report, page 44
[10] See Measuring the Root Zone KSK Keyroll, page 2, https://www.potaroo.net/ispcol/2015-09/ksktest.pdf
[11] See Recommendations to the Board: Advice Status Reports, https://www.icann.org/board-advice-status-current.pdf
[12] See ICANN Board Status Advice Report as of 29 February 2020, https://www.icann.org/en/system/files/files/board-advice-status-report-pdf-29feb20-en.pdf
[13] See Security and Stability Advisory Committee (SSAC) Advice Status: Board Advice Register Phases and Descriptions, https://features.icann.org/board-advice/ssac

case that recommendations 2, 3 and 4 of SAC063 would not be relevant to the DNS as it exists today. SAC073 contains no new information, and simply reproduces SAC063 in its entirety. Furthermore, more recent advice from the SSAC may have superseded past SSAC advice on KSK rolls.[14]

The SSAC suggests removing this recommendation in its entirety.

3.3.20. Recommendation 21.2 states:

> *ICANN org should establish a formal procedure, supported by a formal process modeling tool and language to specify the details of future key rollovers, including decision points, exception legs, the full control-flow, etc. Verification of the key rollover process should include posting the programmatic procedure (e.g., program, FSM) for public comment, and community feedback should be incorporated. The process should have empirically verifiable acceptance criteria at each stage, which should be fulfilled for the process to continue. This process should be reassessed at least as often as the rollover itself (i.e., the same periodicity) so that lessons learned can be used to adjust the process.*

Some SSAC reviewers believe that this recommendation is simply not implementable in the context of the DNS and the KSK roll. In many other system contexts, such a generic recommendation might have some relevance, but not in the DNS. There are no clear and authoritative means of measuring DNS name resolution and validation and no way of defining either acceptance criteria nor failure thresholds.

Some SSAC reviewers have suggested that the SSR2 RT should clarify what work currently underway by ICANN org is not meeting their expectations and identify what work needs to be expanded upon or retooled.

3.3.21. Recommendation 21.3 states:

> *ICANN org should create a group of stakeholders involving relevant personnel (from ICANN org or the community) to periodically run table-top exercises that follow the Root KSK rollover process.*

The issue with the KSK roll was not the ability of known software to respond to clear signals in the DNS root zone and alter their locally cached trust point accordingly. The problem was the unknown number of DNSSEC-validating DNS implementations that behaved in unpredictable ways. Table-top exercises would not necessarily ameliorate this and run the risk of instilling a false sense of confidence that such changes in the trust points of a secured DNS name resolution environment would have no impact whatsoever. Further investigation and study of the dynamics of trust change in the DNS and the

[14]See SAC108: SSAC Comments on the IANA Proposal for Future Root Zone KSK Rollovers, https://www.icann.org/en/system/files/files/sac-108-en.pdf

behaviour of resolvers may well be a useful outcome of this area of study. While this recommendation may be useful, it should not be considered a high priority.

3.3.22. Recommendation 22 states:

Establish Baseline Security Practices for Root Server Operators and Operations

The relationship between the Root Server operators and ICANN appears to one that safeguards the autonomy of the root server operators. These operators are not contracted agents of ICANN, as described in RSSAC037 and RSSAC038.

ICANN, as an important stakeholder in the DNS root server framework is certainly capable of advocating a particular stance and this report may well recommend such a position of advocacy, but that position falls short of any enforcement capability. The principles espoused in recommendations 22.1 and 22.1 are sound, but their manner of implementation by ICANN should reflect the realities of the at-a-distance relationship between the root server operators and ICANN.

3.3.23. Recommendation 22.3 states:

ICANN org should document hardening strategies of the ICANN Managed Root Server (IMRS), commonly known as L- Root, and should encourage other RSOs to do the same

This recommendation refers to a "hardening strategy" that is not explained in the draft report.

3.3.24. Recommendation 23 states:

Accelerate the Implementation of the New Generation RZMS

There are many reasons why secure systems take time to develop and test. Identifying vulnerabilities in any system takes time and careful analysis. The task of assuring the end client of a secure system that the system is indeed adequately robust and secure requires a comprehensive phase of analysis. It is unclear why this report is recommending that the process be "accelerated". What issue or issues are being addressed by hastening this particular development? The report does not clearly explain why this acceleration is necessary

3.3.25. The section relating to root zone Data and Internet Assigned Numbers Authority (IANA) Registries[15] seems to contain a mix of considerations relating to the content of the root zone of the DNS, the work of maintaining a collection of protocol parameter registries as a service to the IETF, and the Centralized Zone Data Service (CZDS), which

[15] See SSR2 Draft Report, page 47

appears to be a service that is a component of the ICANN gTLD DNS function. It may be helpful for the report to independently consider these areas.

3.3.26. Recommendation 24.1 states:

> *ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of each type of unique identifier information, such as root-zone related service, IANA registries, and any gTLD service that ICANN org has authoritative purview over.*

The term "of each type of unique identifier information" is used and specific mention is made of "IANA Registries." The scope of this recommendation apparently includes the IETF Protocol Parameter Registry function. Should the agency for whom the function is being performed, namely the IETF, perform a review of ICANN's performance of execution of the roles described by the Memorandum of Understanding (MoU) between ICANN and the IETF?

3.3.27. Recommendation 25.2 states:

> *ICANN org should implement the four recommendations in SSAC 97 [quotes four recommendations from SAC097]*

This again raises the same issue of quoting recommendations from other ICANN supporting organisations and advisory committees. If the reason to reproduce these recommendations in the SSR2 report is because the SSR2 RT has concluded that the ICANN board is not paying due attention to its advisory bodies then it should say so directly. If this is not the case, then what purpose is served by reproducing these recommendations here?

3.3.28. Recommendation 26.3 states:

> *ICANN org should publicly conduct EBERO [Emergency Back-end Registry Operator] smoke-testing at predetermined intervals using a test plan coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised and publish the results*

This recommendation refers to "smoke-testing". The term is not explained in the draft report.

3.4 Comments on Workstream 4: Future Challenges

3.4.1. The discussion on cryptography notes that: "Recent guidance from the US National Security Agency recommends using 3072 bits for RSA. ECDSA [Elliptic Curve Digital Signature Algorithm] seems to offer a better alternative than very large RSA keys". The

reference listed has specific nuances in an National Security System (NSS) context but would necessarily not apply to DNSSEC. While recommendation 27.1 is general and sufficient as a recommendation, the rationale is too prescriptive.

3.4.2. Recommendation 27.1 states:

> *PTI [Public Technical Identifiers] operations should update the DPS [DNSSEC Practice Statement] to facilitate the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to ECDSA or to future post-quantum algorithms, which will create a more resilient DNS while providing the same or greater security.*

The SSAC agrees with the recommendation that the DPS should provide explicit mention of the possibility of a transition from one digital signature to another.

The SSAC believes that the explicit references to ECDSA and post-quantum algorithms are unnecessary in this recommendation. The expectation that any such algorithm changes will not degrade security is a prudent expectation, but this recommended action to revise the DPS should remain more generic in nature.

3.4.3. Recommendation 27.2 states:

> *As root DNSKEY algorithm rollover is a very complex and sensitive process, PTI operations should work with other root zone partners and the global community to develop a consensus plan for future root DNSKEY algorithm rollovers, taking into consideration the lessons learned from the first root KSK rollover in 2018.*

The DPS[16] notes that there are two distinct roles in the Root Zone, namely the Root Zone Key Signing Key (RZ KSK) Operator, a function currently performed by PTI and the Root Zone Zone Signing Key (RZ ZSK) Operator, a function currently performed by Verisign. Prudent operational practice would require close collaboration between these two functions, as well as some level of community consultation as part of any process to update the DPS, as proposed in Recommendation 27.2. Accordingly, the SSAC agrees with this recommendation.

3.4.4. It is unclear why the topic of "Name Collision" in Workstream 4 falls into this Future Challenges category when the topic seems more like an aspect of the current environment that has been studied for over a decade already and continues to be studied, including as part of the SSAC's Name Collision Analysis Project (NCAP). A more logical place for this section of the report would appear to be within Workstream 3's Review of the Security, Stability and Resilience of the DNS System.

[16] See DNSSEC Practice Statement for the Root Zone KSK, https://www.iana.org/dnssec/icann-dps.txt

3.4.5. Recommendation 28 states:

> *Develop a Report on the Frequency of Name Collisions and Propose a Solution*

It is unclear what is being proposed here. The recommendation title in the summary at the front of the report and the recommendation title in the body of the report differ, although the text of the sub-recommendations match. It is also unclear what is meant by "Propose a Solution". This section could benefit from more clarity and context on whether ICANN org should be proposing a solution, to whom the proposal should be presented and how that proposed solution relates to the current NCAP study.

3.4.6. Recommendation 28.1 states:

> *ICANN org should produce findings that characterize the nature and frequency of name collisions and resulting concerns. The ICANN community should implement a solution before the next round of gTLDs.*

In what way does this recommendation materially differ from the existing NCAP study being undertaken under the auspices of SSAC?

3.4.7. Recommendation 28.2 states:

> *ICANN org should facilitate this process by initiating an independent study of name collisions through to its eventual completion and adopt or account for the implementation or non-adoption of any resulting recommendations. By "independent," SSR2 RT means that ICANN org should ensure that the SSAC Name Collision Analysis Project (NCAP) work party research and report evaluation team's results need to be vetted by parties that are free of any financial interest in TLD expansion.*

It is unclear what is being proposed here. Does this recommendation propose the establishment of a new study of name collisions that is to operate in parallel to, but fully independent of, the SSAC NCAP activity? Or is the recommendation proposing a "vetting" of the SSAC NCAP outcomes by some third party or parties that have no financial interest in TLD expansion?

3.4.8. Recommendation 28.3 states:

> *ICANN org should enable community reporting on instances of name collision*

What is the intended objective of this recommendation? How would the reported data be used? To what end? The report fails to adequately motivate this recommendation, lack a clear definition of what is intended by "community reporting," nor give a clear indication of measurable outcomes. In terms of SMART criteria, this recommendation appears to be lacking in terms of specificity, measurability, and relevance.

3.4.9. Recommendation 29 states:

> *Focus on Privacy and SSR Measurements and Improving Policies Based on Those Measurements*

(Please note that the numbering of the component recommendations in the Summary section of the SSR2 draft report (29.1 to 29.4) does not match the numbering in the main body of the report (29.5 to 29.8). The former numbering is used to reference recommendations below.)

Why is the topic of "Privacy" in Workstream 4 a Future Challenge? This would conventionally be classified as a current topic.

Does the SSR2 RT have evidence that ICANN org is not adequately focusing on Privacy and SSR Measurements already? The recommendation implies that the review has taken the position that the level of focus and attention is inadequate, but has not provided any material in the report that substantiates such a conclusion.

3.4.10. The report notes in the section relating to Rationale and Findings on Privacy, that "ICANN org, in having a privacy policy that covers registration information and having Bylaws that requires it enforce its own policies, is in conflict with their statement that ICANN org is not responsible for data protection and privacy."[17] This is an unusual interpretation of the ICANN statement, in that the disclaimer is about the general state of privacy on the Internet while the org does have a privacy policy relating to data gathered by the org.

3.4.11. Recommendation 29.1 states:

> *ICANN org should monitor and regularly report on the privacy impact of technologies like DoT (DNS over TLS) and DoH (DNS over HTTPS)*

In terms of using the SMART criteria for the report's recommendations it is not clear how this particular recommendation is directly relevant to ICANN. The manner of DNS name resolution between stub and recursive name resolvers on the Internet, and the protocols used to perform such resolution appears to fall outside the scope of ICANN's activities and authority. Because of this question of direct relevance to ICANN's scope and mission, this action may be more appropriately included as part of the report's set of "suggestions," and listed on the basis of the broader topic of potential actions by ICANN org that would provide value to the community through the provision of assessments of aspects of the larger environment of the domain name space and its evolving use.

[17] See SSR2 Draft Report, page 55

The SSAC is aware of current activity within both ICANN org and the ICANN community in this space already, including a recently published SSAC study on the implications of DNS over HTTPS and DNS over TLS,[18] and there is some lack of clarity as to how this recommendation differs from current practice.

3.4.12. Recommendation 29.2 states:

> *ICANN org's consensus policies and agreements with registry operators and registrars should, therefore, have clauses to reflect compliance with these while ensuring that the DNS is not fragmented because of the need to maintain/implement minimum requirements governing the collection, retention, escrow, transfer, and display of registration data, which includes contact information of the registrant, administrative, and technical contacts as well as technical information associated with a domain name.*

The introduction of the concept of DNS "fragmentation" makes no clear sense in this context. The recommendation should phrase the concern in a different way that avoids the particular term "fragmentation", or explain the concept of "fragmentation" in detail.

3.4.13. Recommendation 29.3.2 states:

> *Monitor relevant and evolving privacy legislation (e.g., CCPA and legislation protecting personally identifiable information (PII)) and ensure that ICANN org's policies and procedures are aligned and in compliance with privacy requirements and the protection of personally identifiable information as required by relevant legislation and regulation.*

This recommendation appears to present certain logistical challenges for ICANN org to ensure that ICANN policies and procedures are aligned and in compliance with privacy requirements across all legislative regimes, as the recommendation proposes. Within the review's adopted approach of phrasing SMART recommendations it is unclear how these logistical challenges are to be measured and tracked. The reference to "relevant legislation and regulation" might benefit from a more specific formulation that takes into account the considerable spectrum of variance of national regulations in this space.

3.4.14. Recommendation 29.3.3 states:

> *Develop and keep up to date a policy for the protection of personally identifiable information. The policy should be communicated to all persons involved in the processing of personally identifiable information. Technical and organisational measures to appropriately protect PII should be implemented.*

[18] See SAC109: The Implications of DNS over HTTPS and DNS over TLS, https://www.icann.org/en/system/files/files/sac-109-en.pdf

The SSAC agrees with the principle behind this recommendation. However, the recommendation appears to imply that ICANN does not have such a policy already, as the recommendation calls for the development of such a policy. To what extent does the ICANN Privacy Policy[19] fall short of the objectives of this recommendation?

3.4.15. Recommendation 29.3.4 states:

> *Conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they, at a minimum, have procedures in place to address privacy breaches.*

This recommendation lacks clarity and appears to lack measurable outcomes.

The term "audit" is conventionally used in the context of checking the adherence of an organisation to its documented procedures. In this case the recommendation appears to call for ICANN to determine, for all accredited registrars, whether or not they have a privacy policy, to what extent they are committed to adhere to their privacy policies and to what extent these privacy policies contain measures in relation to privacy breaches.

The intent of these recommendations appears to be to ensure that registrars have privacy procedures in place. The recommendation further requires that such procedures "address privacy breaches". It is unclear what specifically is intended by the term "address". Is this public disclosure? Notification to affected parties? Other measures?

To what extent are such measures already encompassed in ICANN's contractual arrangements? If there is no contractual obligation on the part of registrars then what is the intended purpose of such an exercise? The report noted an interchange with ICANN Contractual Compliance on this topic but did not explicitly address whether these contracts adequately covered this topic, implying that the matter was one of enforcement of compliance, or whether the contracts themselves were inadequate in this area.

3.4.16. Recommendation 30 states:

> *Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates*

This recommendation appears to take a one-sided view of leveraging academic and research activity without proposing giving anything back to this community. It would be more balanced for this recommendation to also propose that ICANN org take an active stance in sponsoring such academic and research gatherings where appropriate, and possibly supporting fellowships for researchers to participate in these conferences.

[19] See ICANN org Privacy Policy, https://www.icann.org/privacy/policy

It would also be helpful to have phrased this recommendation in the context of the existing program of support for academic and research gatherings undertaken by ICANN org, including, for example, ICANN's support for participating in IETF activities, the ICANN DNS Symposium and support for DNS Operations, Analysis, and Research Center (DNS-OARC) gatherings.

The SSAC agrees with the importance of the ICANN community remaining closely engaged with academic research activities, and is highly supportive of efforts to further improve this engagement. In that light, the three specific recommendations in this section for ICANN org actions (30.1, 30.1.1, 30.1.2) fall short of proposing measures that would facilitate a more engaged interaction between the ICANN community and academic research. The SSR2 RT may wish to consider recommending measures that take a broader approach to this engagement and look at the longer term objectives of such an engagement, instead of the approach taken in this draft report that specifies the content of individual reports (as described in Recommendations 30.1.1 and 30.1.2). In this case the recommendations appear to be specific to the point of being too prescriptive, and it would be better to propose a more general set of measures that would facilitate positive outcomes for both the ICANN community and the general academic research effort in this area of study.

3.4.17. Recommendation 31 states:

Clarify the SSR Implications of DNS-over-HTTPS

This recommendation appears to be a restatement of recommendation 29.1.

The report needs to explain why DNS over HTTPS (DoH) has direct relevance to ICANN and its remit. The report's rationale and findings related to DNS-over-HTTPS misrepresents opinions and conjecture as established facts, and supports a supposition that network operators have a right to inspect and control DNS transactions. The arguments relating to bypassing DNSSEC validation are also not clearly expressed.

The SSAC recently published a report on DoH and DoT.[20] The SSR2 RT could consult with the SSAC concerning this SSAC report prior to committing this particular action into the final report's set of recommended actions.

There is merit in a more general rephrasing of this recommended action. The domain namespace is not fixed and immutable, and evolution in aspects of the use of this namespace will inevitably impact ICANN and its stakeholder community in various ways. The SSAC agrees with the general principle that ICANN and the broader community should keep themselves informed of evolutionary pressures on the domain

[20] See SAC109: The Implications of DNS over HTTPS and DNS over TLS, https://www.icann.org/en/system/files/files/sac-109-en.pdf

namespace and its use. Perhaps the recommendation should be phrased in these more general terms and not specifically refer to DoH.

3.5 Appendix B: Further Suggestions

3.5.1. The report contains an appendix titled "Further Suggestions" with 5 suggestions listed in this section.[21] This section has some of the characteristics of a record of responses to some of the challenges of the SSR2 RT in undertaking this review, but without any motivating text it is challenging to understand the purpose of this section of the report. It would be helpful if the report could clarify the RT's intentions in listing these suggestions. What is the status of these suggestions? Are they formal recommendations? If not, then what is the intended status of the work items that are listed here?

4 Acknowledgments, Statements of Interests, and Dissents and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of the SSAC process. The Acknowledgments section lists the SSAC members, outside experts, and ICANN staff who contributed directly to this particular document. The Statements of Interest section points to the biographies of all SSAC members, which disclose any interests that might represent a conflict—-real, apparent, or potential—-with a member's participation in the preparation of this Report. The Dissents section provides a place for individual members to describe any disagreement that they may have with the content of this document or the process for preparing it. The Withdrawals section identifies individual members who have recused themselves from discussion of the topic with which this Report is concerned. Except for members listed in the Dissents and Withdrawals section, this document has the consensus approval of all of the members of SSAC.

4.1 Acknowledgments

The committee wishes to thank the following SSAC members for their time, contributions, and review in producing this report.

SSAC members
Greg Aaron
Jeff Bedser
Lyman Chapin
kc claffy
James Galvin
Julie Hammer
Geoff Huston (work party chair)
Merike Kaeo

[21] See SSR2 Draft Report, Appendix B

Danny McPherson
Ram Mohan
Rod Rasmussen
Suzanne Woolf

ICANN staff
Danielle Rutherford (editor)
Andrew McConachie
Kathy Schnitt
Steve Sheng

4.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: https://www.icann.org/resources/pages/ssac-biographies-2019-11-20-en

4.3 Dissents and Withdrawals

There were no dissents or withdrawals.