SAC114
SSAC Comments on the GNSO New gTLD Subsequent Procedures Draft Final Report

A Comment from the ICANN Security and Stability Advisory Committee (SSAC)
11 February 2021

Preface

This is a comment to the ICANN Board in response to a call for comments on the Draft Final Report on the new gTLD Subsequent Procedures Policy Development Process from the ICANN Security and Stability Advisory Committee (SSAC). Due to time constraints, the SSAC chose not to submit its comment through the Working Group's Public Comment process. Instead, the SSAC analyzed the Draft Final Report holistically and prepared this comment to the ICANN Board for consideration. The SSAC is thankful to the Working Group for the opportunity to provide preliminary comments on the Final Report during the Working Group's 19 October 2020 teleconference.

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), technical administration matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). The 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

Executive Summary

The SSAC welcomes the opportunity to provide input to the ICANN Board related to the Final Report on the new gTLD Subsequent Procedures Policy Development Process.[1] The SSAC's comments are divided into two categories: high level comments on the assumptions and approaches of the Final Report and detailed comments on specific sections of the Final Report.

At a high level, the SSAC makes the following comments and recommendations. For the full and official recommendations see Section 4 of this publication.

- First, the SSAC believes that the introduction of more gTLDs to the root namespace is not consistent with ICANN's mission and commitment to keep the Internet secure, stable, and interoperable. The fundamental question from the SSAC's security and stability perspective is whether adding more generic top-level domains (gTLDs) to the root namespace should remain a primary response to furthering the overall objectives of ICANN, namely "keeping the Internet secure, stable and interoperable. [ICANN] promotes competition and develops policy on the Internet's unique identifiers."[2] This comment is not a criticism of the Final Report or the community effort, but the SSAC thinks now is a good time for the ICANN Board to address this question.

  The SSAC recommends that the ICANN Board initiate a fundamental review to determine whether continuing to increase the number of gTLDs is consistent with ICANN's strategic objective to "evolve the unique identifier systems in coordination and collaboration with relevant parties to continue to serve the needs of the global Internet user base."[3] This review should be considered an input towards updating ICANN's strategic goals in conjunction with implementing the CCT Review Team's recommendations (see Recommendation 1).

- Second, given a general intent to proceed with this program in any case, there is a clear need to add greater levels of not only process oversight, but also a systemic consideration of the program's impact, attendant risks and appropriate mitigations to the DNS itself. The systemic considerations would include addressing, monitoring and mitigating impacts on the entire DNS resolution chain (e.g., root servers, DNS recursive resolver performance) and services that provide and/or are dependent upon it.

  In addition, numerous items relating to risks, outcomes, and impacts of increasing the gTLD namespace need to be measured and analyzed to better understand some of the fundamental questions considered by the Working Group as well as areas it did not

[1] See Draft Final Report on the new gTLD Subsequent Procedures Policy Development Process, https://gnso.icann.org/en/drafts/draft-final-report-new-gtld-subsequent-21sep20-en.pdf

[2] See What Does ICANN Do? https://www.icann.org/resources/pages/what-2012-02-25-en

[3] See page 8, "Strategic Objectives," and page 22, "Strategic Goal: Support the continued evolution of the Internet's unique identifier systems with a new round of gTLDs that is responsibly funded, managed, risk-evaluated, and consistent with ICANN processes," in ICANN Strategic Plan for Fiscal Years 2021-2025, https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf

explore. The SSAC agrees with the measurements proposed by the Working Group Recommendations 7.1 - 7.5 and suggests additional goals and measurements.

The SSAC recommends that, as part of the process for creating new gTLDs, ICANN develop and adopt a protocol for measuring progress against stated goals of the program and thresholds, which if crossed, may require mitigation actions. Such measurements and actions should consider the entirety of the DNS ecosystem (see Recommendation 2).

- Third, on the issue of DNS abuse, while the SSAC agrees that a holistic approach to DNS abuse issues has merit, we note that security threats and attendant abuse of the DNS remain a constant and rapidly evolving challenge, and that ICANN recognizes "Domain name abuse continues to grow" as a Strategic Risk[4] to the achievement of its Strategic Objectives. Waiting until efforts to mitigate DNS abuse can be equally applied to all existing and new gTLDs effectively cedes the ground to malicious actors who can depend upon a long policy development process to hinder meaningful anti-abuse measures.

  The SSAC recommends that the ICANN Board, prior to launching the next round of new gTLDs, commission a study of the causes of, responses to, and best practices for the mitigation of the domain name abuse that proliferates in the new gTLDs from the 2012 round. This activity should be done in conjunction with implementing the CCT Review Team's relevant recommendations. The best practices should be incorporated into enforced requirements, as appropriate, for at least all future rounds (see Recommendation 3).

In addition to the high-level comments, the SSAC makes comments on specific sections of the Final Report. The SSAC recommends the ICANN Board take the comments in Section 3 of this document into consideration in its deliberations on accepting the recommendations of the Final Report and subsequent implementations of the approved recommendations (see Recommendation 4).

Finally, the SSAC makes the following specific recommendations to the ICANN Board for its consideration of the Final Report:

- The SSAC recommends that the ICANN organization (ICANN org) develop reference materials or a set of tutorials to teach the basics of registry service provision as a prerequisite for new registry service providers. The purpose of the reference materials is to educate potential registry service providers on the requirements and testing thresholds for pre-delegation testing (see Recommendation 5).

- The SSAC recommends that the words "intended use" be removed as a defining characteristic to determine whether or not applications should be placed in the same contention set (see Recommendation 6).

[4] See page 12, "Strategic Goal: Identify and mitigate security threats to the DNS through greater engagement with relevant hardware, software, and service vendors," in ICANN Strategic Plan for Fiscal Years 2021-2025, https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf

- The SSAC recommends that the ICANN Board, prior to authorizing the addition of new gTLDs to the root zone, receive and consider the results of the Name Collision Analysis Project, pursuant to Board Resolution 2017.11.02.30 (see Recommendation 7).

1 Introduction

The SSAC welcomes this opportunity to provide input to the ICANN Board related to the Final Report on the new gTLD Subsequent Procedures Policy Development Process, as prepared by the GNSO New gTLD Subsequent Procedures Working Group. Hereinafter referred to in this publication as the Final Report and the Working Group, respectively. The SSAC previously provided input to this PDP Working Group in October 2018 on the Initial Report[5] and in December 2017 on the subject of root scaling.[6] The SSAC also met with the Working Group on October 19, 2020 to provide feedback and discuss most of the comments the SSAC has articulated in this document on specific areas of the Final Report.

While this document was originally developed to provide input to the Working Group, this report is being published after their work has completed. The SSAC took an in-depth look at broader issues related to this topic space and used this opportunity to provide to the ICANN Board substantive comments and recommendations on the future of deploying new generic top-level domains (gTLDs).

These comments are organized by subject matter and include regular references to the specific recommendations given in the Final Report. Each section usually begins with a listing of relevant recommendations from the Final Report then follows with the SSAC's comment.

2 High-Level Comments

2.1 Strategic Reflection on Overall Objectives of gTLD Expansion

The Final Report contains a set of proposals that adjusts the approach to the next round of expansion of the top-level domain (TLD) space in terms of addressing identified weaknesses and shortcomings in the previous round of further gTLDs. The Final Report is necessarily limited in its perspective of the management of the TLD expansion program.

First, the SSAC believes that the introduction of more gTLDs to the root namespace is not consistent with ICANN's mission and commitment to keep the Internet secure, stable, and interoperable.[7] ICANN's Strategic Plan, which discusses ICANN's strategy for achieving its mission, calls out a strategic objective to "[e]volve the unique identifier systems in coordination and collaboration with relevant parties to continue to serve the needs of the global Internet user base,"[8] and that one strategic goal under this objective is to "[s]upport the continued evolution of the Internet's unique identifier systems with a new round of gTLDs that is responsibly funded,

[5] See SAC103: SSAC Response to the new gTLD Subsequent Procedures Policy Development Process Working Group Initial Report, https://www.icann.org/en/system/files/files/sac-103-en.pdf

[6] See SAC100: SSAC Response to the New gTLD Subsequent Procedures Policy Development Process Working Group Request Regarding Root Scaling, https://www.icann.org/en/system/files/files/sac-100-en.pdf

[7] See ICANN Bylaws, Section 1.1.a and Section 1.2.a.i, https://www.icann.org/resources/pages/governance/bylaws-en/#article1

[8] See page 18, ICANN Strategic Plan: Fiscal Years 2021-2025, https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf

managed, risk-evaluated, and consistent with ICANN processes."[9] However, it's not clear how simply having more names delegated in the root zone is necessary, or sufficient, or even beneficial to an intention to "[e]volve the unique identifier systems…." More of something isn't necessarily an evolutionary step; it might just be more of exactly what you already had. The SSAC is concerned that this strategic goal has been crafted without adequate learning from the prior expansion round to understand the trade-offs between benefits garnered and costs incurred in relation to the program's overall strategic objectives, and that "adequate learning" was outside of the Final Report's scope. The SSAC's concern aligns with concerns raised in the Competition, Consumer Trust, and Consumer Choice (CCT) Final Report[10] and its challenges with being able to adequately assess "the extent to which the expansion of gTLDs promoted consumer trust and the effectiveness of safeguards adopted by new TLD operators in mitigating certain risks involved in such expansion." [11]

The fundamental question from the SSAC's perspective is whether adding more gTLDs to the root namespace should remain a primary response to furthering the overall objectives of ICANN, namely "keeping the Internet secure, stable and interoperable. [ICANN] promotes competition and develops policy on the Internet's unique identifiers."[12] The SSAC's comment is not a criticism of the Final Report or the community effort, but the SSAC thinks now is the best time for the ICANN Board to address this question. An update to the Board's rationale document from 2011 seems appropriate.[13]

Recommendation 1: The SSAC recommends that the ICANN Board initiate a fundamental review to determine whether continuing to increase the number of gTLDs is consistent with ICANN's strategic objective to "evolve the unique identifier systems in coordination and collaboration with relevant parties to continue to serve the needs of the global Internet user base."[14] This review should be considered an input towards updating ICANN's strategic goals in conjunction with implementing the CCT Review Team's recommendations. Such a fundamental review should include at least the following areas of study based on prior rounds of the New gTLD program:

- **Impacts on root server operations**
- **Impacts on SSR issues**
- **Impacts on overall DNS operations**
- **Analysis of how all metrics for success were met**

---

[9] See page 22, ICANN Strategic Plan: Fiscal Years 2021-2025, https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf

[10] See Competition, Consumer Trust, and Consumer Choice Final Report, https://www.icann.org/en/system/files/files/cct-final-08sep18-en.pdf

[11] See Chapter 5, Data-Driven Analysis: Recommendations for Additional Data Collection and Analysis, Competition, Consumer Trust, and Consumer Choice Review (CCT) Final Report, https://www.icann.org/en/system/files/files/cct-final-08sep18-en.pdf

[12] See What Does ICANN Do? https://www.icann.org/resources/pages/what-2012-02-25-en

[13] See ICANN Board Rationales for the Approval of the Launch of the New gTLD Program, https://www.icann.org/en/system/files/bm/rationale-board-approval-new-gtld-program-launch-final-20jun11-en.pdf

[14] See page 8, "Strategic Objectives," and page 22, "Strategic Goal: Support the continued evolution of the Internet's unique identifier systems with a new round of gTLDs that is responsibly funded, managed, risk-evaluated, and consistent with ICANN processes," in ICANN Strategic Plan for Fiscal Years 2021-2025, https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf

- **Risk analysis**

2.2 Comments on Overall Approach

The Working Group's approach is to define the entire process of this round of gTLD expansion, operate this process to completion, and then evaluate the outcomes.

The challenge for reviewers of the Working Group's proposal is to consider carefully how the process will operate, anticipate what issues may arise both in terms of risk and unintended consequences, and review the proposal in such a light. The proposal is substantive both in length and detail, and any thorough competent review that explores these issues of risk and identification of potential consequences would likely consume an amount of time and effort comparable to that taken to draft the proposed process in the first place. It is reasonable to conclude that issues will arise, both in specific instances and in more general terms, that may expose shortcomings in the process itself that have eluded both the drafting team and the various reviewers in advance of the operation of this process.

The SSAC observes that the general approach being proposed in the report is to react to any adverse impacts from this program after they have already occurred. The premise of this approach is that any such adverse impacts will be reversible, and any harms that result within the large DNS environment can be mitigated. Without a reasonably complete understanding of the larger environment and its dynamic properties, such an approach could be viewed as reckless given that adding further labels to the root zone entails a number of irreversible steps.[15] In order to follow the conservatism principle,[16] this environmental understanding would include identifying and understanding the risks involved with implementing the program as well as the ability to measure its impacts throughout the DNS ecosystem through tools like the previously proposed early warning system.[17]

Given a general intent to proceed with this program in any case, there is a clear need to add greater levels of not only process oversight, but also a systemic consideration of the program's impact to the DNS itself. The systemic considerations would include addressing, monitoring and mitigating impacts on the entire DNS resolution chain and services that provide and/or are dependent upon it. Examples include DNS root server performance, DNS recursive resolver performance, response times for completing full DNS queries across the Internet as a whole, and other areas where an expanding system of names to query and cache may impact systems' performance and reliability.

---

[15] See SAC100: SSAC Response to the New gTLD Subsequent Procedures Policy Development Process Working Group Request Regarding Root Scaling, https://www.icann.org/en/system/files/files/sac-100-en.pdf

[16] See See RSSAC052: Statement on Recommendations for an Early Warning System for Root Zone Scaling, https://www.icann.org/en/system/files/files/rssac-052-25nov20-en.pdf and SAC084: SSAC Comments on Guidelines for the Extended Process Similarity Review Panel for the IDN ccTLD Fast Track Process, https://www.icann.org/en/system/files/files/sac-084-en.pdf

[17] See SAC100: SSAC Response to the New gTLD Subsequent Procedures Policy Development Process Working Group Request Regarding Root Scaling, https://www.icann.org/en/system/files/files/sac-100-en.pdf and RSSAC031: Response to the GNSO Policy Development Process (PDP) Working Group on the new Generic Top Level Domains (gTLDs) Subsequent Procedures, https://www.icann.org/en/system/files/files/rssac-031-02feb18-en.pdf

2.3 Review Prior Rounds and Set Goals for Future Rounds

Numerous items relating to risks, outcomes, and impacts of increasing the number of gTLDs could be measured and analyzed to better understand some of the fundamental questions considered by the Working Group as well as areas it did not explore. The SSAC and many others[18] have expressed concerns about several of these issues (e.g., DNS abuse, name collisions, and impacts on root scaling) yet recommendations are being put forward on how to proceed with further expansion without having identified and learned key lessons from the prior expansion. The CCT Review Team called out several of these and other issues that one would expect to have been completed prior to further expansion. In general, it is irresponsible to proceed without completing key work to understand the successes and failures of the prior round. In order to accomplish that, objective criteria on how to judge the prior round, as well as criteria for moving forward, should be created and agreed across the community.

As stated in Topic 7, in Recommendations 7.1 through 7.5 of the Final Report, criteria should be developed for measuring how well goals are being met both during and after completion of any future gTLD expansion rounds. Those goals should include not only the stated aspirations of undertaking a program (e.g., increased competition, consumer trust & choice, innovation, access) as recommended, but also the performance, stability, security, and other areas that may be affected either adversely or positively during the process. Metrics for continuously measuring results against these criteria should be developed, collected, analyzed, published, and acted upon during implementation. Beyond these recommendations, and following the examples of sound engineering processes, various thresholds and limits should be maintained to allow for course corrections, pausing, or reversing decisions made during the ongoing delegation processes.

Recommendation 2: The SSAC recommends that, as part of the process for creating new gTLDs, ICANN develop and adopt a protocol for measuring progress against stated goals of the program and thresholds, which if crossed, may require mitigation actions. Such measurements and actions should consider the entirety of the DNS ecosystem.

2.4 Comments on DNS Abuse

The Final Report touches on the topic of domain name abuse only in Topic 9: Registry Voluntary Commitments / Public Interest Commitments. In one of the sub-recommendations (9.15) in this section, the Working Group explains its position that DNS abuse should not be dealt with by this effort, but should be dealt with separately and "holistically" to apply to all gTLDs rather than new ones.

> *Recommendation 9.15: The Working Group acknowledges ongoing important work in the community on the topic of DNS abuse and believes that a holistic solution is needed to account for DNS abuse in all gTLDs as opposed to dealing with these recommendations with respect to only the introduction of subsequent new gTLDs. In addition, recommending new requirements that would only apply to the new gTLDs added to the root in subsequent rounds could result in singling out those new gTLDs for disparate*

[18] See ALAC Advice on DNS Abuse, https://atlarge.icann.org/advice_statements/13747

> *treatment in contravention of the ICANN Bylaws. Therefore, this PDP Working Group is not making any recommendations with respect to mitigating domain name abuse other than stating that any such future effort must apply to both existing and new gTLDs (and potentially ccTLDs).*

A logical implication of this recommendation is that the issues surrounding DNS abuse should be addressed by a separate GNSO Policy Development Process (PDP) and that this work should happen before any process to add additional gTLDs is started. While the SSAC agrees that a holistic approach to DNS abuse issues has merit and supports any community effort to proceed with such a holistic approach, we note that security threats and attendant abuse of the DNS remain a constant and rapidly evolving challenge. If the ICANN Board chooses to proceed with a new gTLD round prior to a holistic, community-wide effort to address DNS abuse as recommended by the CCT Review Team, the SSAC suggests it should at least take actions to address DNS abuse in all subsequent rounds.

Waiting until efforts to mitigate DNS abuse can be equally applied to all existing and new gTLDs effectively cedes the ground to malicious actors who can depend upon a long PDP to hinder meaningful anti-abuse measures. Just as in the prior round ICANN mandated the use of DNSSEC and IPv6 as requirements for new gTLDs, in this and subsequent rounds best practices in DNS abuse mitigation measures must be considered as requirements for new gTLDs, while awaiting policy development mechanisms to retroactively apply such measures to existing gTLDs. In addition, the ICANN community has been highly engaged in discussions of DNS abuse issues from 2019 through 2020, and the GNSO has indicated that they have prioritized work in this space for 2021. The SSAC has concurrent work in this area as well, so there is some chance that any new round of new gTLDs will occur with new knowledge and policy in place. However, as this has been an issue under consideration for over a decade without resolution, it would be an irresponsible failure if strong anti-abuse policies were not enacted and enforced prior to any round of expansion of the gTLD space.

Given the serious problems that some new gTLDs had with DNS abuse,[19,20] it is clear that these issues need to be understood and mitigated prior to the launch of any new gTLDs under a new policy regime. For example, a focused effort to understand these issues by the ICANN organization (ICANN org) could inform the crafting of new guidance to potential TLD operators and enable the adoption of best practices learned in dealing with large-scale problems in the previous round. The SSAC is concerned that failure to address these issues before new TLDs are introduced will lead to wholesale blocking of *all* new TLDs introduced going forward by many network operators. This blocking of new TLDs in their entirety as a mitigation response was commonly proposed after the prior round,[21,22] and the technology for enabling such blocking has

[19] See Phishing Landscape 2020: A Study of the Scope and Distribution of Phishing, http://www.interisle.net/PhishingLandscape2020.html

[20] See Cybercrime After the Sunrise: A Statistical Analysis of DNS Abuse in New gTLDs, https://www.sidnlabs.nl/downloads/gogl-IZCQkidFmzVvw72ug/48cedd55a528b8f8039a5d7a0286fb3c/asiaccs2018-submitted.pdf

[21] See Block that Top Level Domain! https://bluecatnetworks.com/blog/block-that-top-level-domain/

[22] See Generic top-level domains (gTLDs) have become a magnet for cybercriminals https://www.titanhq.com/generic-top-level-domains-gtlds-have-become-a-magnet-for-cybercriminals/

only grown more prevalent since then. This presents a serious threat to the successful adoption of new TLDs, and the success of ICANN's Universal Acceptance program,[23] should history repeat itself.

The Working Group cites the CCT Review Team's recommendations that touched on DNS abuse (14, 15, 16), but notes that only a portion of recommendation 16 was referred to the Working Group for consideration. The Working Group does not cite SAC103 at all with respect to DNS abuse, which seems to be an oversight. We draw attention to the following observation about the Preliminary Report made in SAC103: "The SSAC is concerned there are no questions or preliminary recommendations in the Initial Report on the subject of domain name abuse (e.g., phishing, malware)." While SAC103 went on to state that the SSAC would likely study the topic, there was an expectation that the Working Group would investigate this issue further as part of its remit. While pointing out this should be treated holistically is a fair conclusion, one of the purposes for this PDP was to take lessons learned in the 2012 round to make better policy for future gTLD expansion, and this seems to have been a missed opportunity.

The CCT Review Team provided very specific recommendations (recommendations 14-21) relevant to better dealing with DNS abuse, and many of those recommendations have been adopted by the ICANN Board and are in the process of being implemented while two are still pending.[24] Many of these recommendations ask for further data collection and studies to understand the drivers of DNS abuse, including DNS abuse observed during the latest expansion round, and request that mitigation actions be developed for such issues.

Recommendation 3: The SSAC recommends that the ICANN Board, prior to launching the next round of new gTLDs, commission a study of the causes of, responses to, and best practices for mitigation of the domain name abuse that proliferates in the new gTLDs from the 2012 round. This activity should be done in conjunction with implementing the CCT Review Team's relevant recommendations. The best practices should be incorporated into enforced requirements, as appropriate, for at least all future rounds.

3 Comments on Specific Sections of the Final Report

The comments in this section are structured in the same sub-groupings as the table in Section 2.1 of the Final Report. These comments are rooted in security, stability, and resiliency fundamentals, but also focus on areas where process gaps or omissions could reasonably cause issues upon implementation. The SSAC believes that where new mechanisms or processes are contemplated or created, they must be subject to a "burn-in" period so we may understand and mitigate issues from corner cases that will almost certainly arise. In addition, the SSAC suggests that ICANN consider monitoring and reviewing key competencies of operators as the default model, rather than monitoring and reviewing only at specific instances (such as an application for a new TLD).

[23] See Universal Acceptance, https://www.icann.org/ua

[24] See Competition, Consumer Trust and Consumer Choice Review (CCT) as of 21 January 2021, https://www.icann.org/resources/reviews/specific-reviews/cct

Recommendation 4: The SSAC recommends the ICANN Board take the comments in SAC114 Sections 3.1-3.3 into consideration in the Board's deliberations on the following items:

1) **accepting the recommendations of the Final Report on the new gTLD Subsequent Procedures Policy Development Process;**
2) **subsequent implementations of the approved recommendations developing the policy; and**
3) **the implementation of the policy.**

3.1 Comments on Section 2.2 - Overarching Issues

3.1.1 Comments on Affirmation 1.3

Affirmation 1.3 states:

> *The Working Group affirms that the primary purposes of new gTLDs are to foster diversity, encourage competition, and enhance the utility of the DNS.*

Experience has shown that expanding the gTLD space challenges the security, stability, and resiliency of the domain name system. This creates a tension between ICANN's objective to "foster diversity, encourage competition, and enhance the utility of the DNS" and its objective to "maintain the security, stability, and resiliency of the domain name system." The Final Report does not pay adequate attention to documenting and navigating this fundamental tension with safeguards or other protective measures.

3.1.2 Comments on Recommendation 2.1

Recommendation 2.1 states:

> *Additionally, the Working Group recommends the formation of a Standing Predictability Implementation Review Team ("SPIRT")(Pronounced "spirit") to serve as the body responsible for reviewing potential issues related to the Program, to conduct analysis utilizing the framework, and to recommend the process/mechanism that should be followed to address the issue.*

The scope of SPIRT vis-à-vis existing policy mechanisms is yet to be established. It is not clear whether SPIRT will have either the appropriate technical expertise or the resources to appoint appropriate technical experts in cases that involve security or stability. Specifically, security issues that take the form of "may occur" or "could occur" require nuanced approaches and subject matter expertise to arrive at informed conclusions.

In addition, how SPIRT will be filled and led is nearly as important as any other decision for the next round. A politicized mechanism to fill its membership roster may result in lowered credibility and utility of its reviews.

What mechanisms are to be used during the operation of the process to evaluate the effectiveness of the process and allow for revision as such issues occur and are

identified? The SPIRT proposal in Recommendation 2.1 talks about the review of potential issues and the recommendation of process alteration or mechanism that should be followed to address the issue, but the intent of this implementation review team is unclear in the use of the term "potential", nor in terms of the escalation process to be used to evaluate such recommended mechanisms. For example, would the SPIRT be able to invoke a "hard stop" in the event of a widespread failure of process or implementation that imperils the stability and security of the DNS? Or would some other escalation process be invoked? Furthermore, is SPIRT intended to review specific incidents that occur during the process (as distinct from "potential" issues)? Is SPIRT empowered to take steps to address such specific issues? Or are other remediation steps contemplated that are not specifically described in this proposal?

The SSAC observes that no systematic study has been undertaken to understand why registries that withdrew their TLDs from the 2012 round have done so. The SSAC does not assert any unifying rationale for such withdrawals, but it is important to eliminate security or stability issues as a root cause of withdrawals. SPIRT should be set up to monitor and handle issues related to security and stability, and in order to be successful, should be informed by an understanding of any prior incidents.

Furthermore, SPIRT does not appear to be set up to review overarching problems or systemic issues that may require either a halt or a slowdown in the rollout of TLDs; it seems to be set up to review individual applications or contention sets rather than to look at systemic issues. SPIRT is a non-PDP mechanism, and under the ICANN Bylaws and GSNO remit a non-PDP mechanism cannot be used to solve policy problems.

Two specific issues of concern to SSAC are:

1. SPIRT's ability to recognize a large, overarching issue that may be politically unpopular but technically important, and
2. SPIRT's ability to enact real outcomes on such an issue.

Finally, it is unclear whether a recommendation by SPIRT can be overturned by the GNSO Council, regardless of the merit of the SPIRT recommendation.

3.1.3 Comments on Recommendation 3.6

Recommendation 3.6 states:

> *Absent extraordinary circumstances, future reviews and/or policy development processes, including the next Competition, Consumer Choice & Consumer Trust (CCT) Review, should take place concurrently with subsequent application rounds. In other words, future reviews and/or policy development processes must not stop or delay subsequent new gTLD rounds.*

First, the SSAC suggests that the word "must" be replaced by the word "should."

Second, it is possible that the delegation of some TLDs or other factors may create a security environment that merits caution in the processing of gTLD rounds. Such an

event may be considered "extraordinary," but the SSAC suggests either more tightly defining "extraordinary" or allowing for ordinary but troubling security or stability issues to be a reasonable cause for delay, investigation, or stoppage.

Finally, the SSAC would like to ask how the Board's decision to change Article 4.6 of the ICANN Bylaws to eliminate the Specific Reviews (including CCT) affects the Final Report.

3.1.4 Comments on Recommendation 6.5

Recommendation 6.5 states:

> *Pre-evaluation occurs prior to each application round and only applies to that specific round. Reassessment must occur prior to each subsequent application round.*

Should it become apparent during an application round followed by delegation and operation that a Registry Service Provider's (RSP's) operations and mechanisms are insufficient or cause continued degradation of service for the TLDs the RSP operates, a method to investigate and require a resolution of such problems must be available. In other words, no one wants an RSP who is "perfect" on examination day and underperforms thereafter.

The ability to scale up is a consideration that may be difficult to examine during pre-evaluation. Operational volume limits often manifest when operations are under stress. This will become apparent over time as an RSP adds TLDs if there is a limit to the number of TLDs that can be managed as well as transaction limits that may not become apparent until one or more TLDs are operational at a given RSP.

Additionally, the SSAC believes evaluation of a provider for one set of criteria does not qualify it to run TLDs under a different set of criteria. Although there is a set of essential services that apply to all TLDs, many TLDs will have unique business rules or requirements based on the needs of the community they serve. These differences may bring to light issues that challenge an RSP's essential services. It is important to test these different features prior to delegation.

Based on prior experience from the 2011 round, it is important that RSP skills be reviewed on a regular basis, rather than through a "past the finish line" approach. For example, tasks such as DNSSEC key rolls, synchronized failover exercises, handling of variants, and bundling of variants are complex tasks for which the appropriate skills and technology have to be kept fresh all the time, rather than just at the time of taking a test.

Further, we note that there is insufficient detail and importance provided to the depth and the quality of pre-delegation testing. The fundamental requirement for ICANN org is to ensure that registry operators and RSPs are able to operate in a secure and stable manner. This means not only demonstrating the ability to conform to service-level agreements (SLAs) or other performance requirements, but also demonstrating competence in the

day-to-day ability to execute the basic operations of a registry. We note several anecdotal instances[25] in the 2012 round where ICANN org staff had to "hand-hold" registry providers so as to avert a DNS or registry outage.

In all of these areas, our concern is to ensure that RSPs are appropriately resourced and skilled to fulfill the day-to-day operations of a registry, rather than hiring "surge programmers" to pass ICANN's qualifications tests, and then default to standards that might result in poor security practices and lead to unstable operation.

Recommendation 5: The SSAC recommends that ICANN org develop reference materials or a set of tutorials to teach the basics of registry service provision as a prerequisite for new registry service providers. The purpose of the reference materials is to educate potential registry service providers on the requirements and testing thresholds for pre-delegation testing.

3.1.5 Comments on Root Scaling (Recommendations 7.1-7.5, 26.2)

The SSAC originally included comments on root zone scaling to the new gTLD Subsequent Procedures Policy Development Process Working Group in SAC103 and to the ICANN org in SSAC2019-07.[26,27]

The SSAC noted in SAC103 that the initial proposed recommendations would lower the barriers to making applications with an anticipation of lower application costs and streamlined evaluation and approval processes. The SSAC asked whether the organization's operational capability could scale to meet the demands. This question appears to be addressed in Recommendation 7.1, guidance 7.2, and Recommendations 7.3, 7.4, and 7.5. We note that the recommendations do not propose any followup actions for the organization in the event of failure in performance.

SAC103 called for ICANN org to further develop root zone monitoring functionality and early warning systems, which was included in the preliminary recommendations and also in *Implementation Guidance 26.8: ICANN should continue developing the monitoring and early warning capability with respect to root zone scaling.*

SAC103 also called for recommendations to include an acceptable rate of change to the root zone instead of a yearly delegation limit, and that the obligations of new gTLD registries be structured so that their addition to the root zone could be delayed in case of DNS service instabilities. This is addressed in

> *Implementation Guidance 26.4: The number of TLDs delegated in the root zone should not increase by more than approximately 5 percent per month, with the understanding that there may be minor variations from time-to-time.* ; in

[25] Based on private correspondence between SSAC members and OCTO staff

[26] See SAC103: SSAC Response to the new gTLD Subsequent Procedures Policy Development Process Working Group Initial Report, https://www.icann.org/en/system/files/files/sac-103-en.pdf

[27] See SSAC2019-07: ICANN org's preparation toward implementation of a new round of gTLDs, https://www.icann.org/en/system/files/files/ssac2019-07-30aug19-en.pdf

> *Implementation Guidance 26.5: ICANN should structure its obligations to new gTLD registries so that it can delay their addition to the root zone in case of DNS service instabilities. Objective criteria should be developed to determine what could be classified as a "service instability."* ; and in
>
> *Implementation Guidance 26.6: ICANN should investigate and catalog the long term obligations for root zone operators of maintaining a larger root zone.*

There appear to be no outstanding issues in this area, as the matters noted in SAC103 have been adequately addressed in the Final Report. The SSAC thanks the Working Group for its consideration and incorporation of SAC103.

Recommendation 26.2 deserves to be called out due to its vagueness:

> *Recommendation 26.2: ICANN must honor and review the principle of conservatism when adding new gTLDs to the root zone.*

It is not easy to understand what particular actions this recommendation is calling for, and the Final Report contains no further guidance or commentary. From the SSAC's perspective, the principle of conservatism is articulated in SAC084[28] and RFC6912:[29]

> Conservatism Principle: Because the root zone of the global DNS is a shared resource, the decision to add a label to the root should be governed by a conservative bias in favor of minimizing the risk to users (regardless of the language or script they are using and whether the label will be a gTLD or a ccTLD) and minimizing the potential for the need to make decisions that later must be changed or overridden in painful or incompatible ways. In order to minimize risk, doubts should always be resolved in favor of rejecting a label for inclusion rather than in favor of including it.

If this is the Working Group's intent, then we suggest the Working Group incorporate SAC084 and RFC6912 by reference.

3.1.6 Comments on Rationale for Recommendations 7.4 and 7.5

The rationale for Recommendations 7.4 and 7.5 states:

> *In a public comment to the Working Group's Initial Report, the SSAC noted that, "In general, it is preferable to discover major failures before delegation instead of after the TLD is in operation. Past performance is not a guarantee of future performance." However, the Working Group believes that expanded operational testing in conjunction with more robust ongoing monitoring will better ensure*

[28] See SAC084: SSAC Comments on Guidelines for the Extended Process Similarity Review Panel for the IDN ccTLD Fast Track Process, https://www.icann.org/en/system/files/files/sac-084-en.pdf

[29] See RFC 6912: Principles for Unicode Code Point Inclusion in Labels in the DNS, https://tools.ietf.org/html/rfc6912

> *that registries are able to meet SLAs. To support the development of recommendations on this topic and related topics, the Working Group requested that ICANN org provide the Working Group with statistics resulting from SLA monitoring and data on EBERO thresholds reached.*

The SSAC notes that the Working Group did not accept the advice in SAC103 and accepts the Working Group's explanation and response in the rationale.

3.1.7 Different TLD Types

From a protocol or DNS operation perspective, no meaningful differences exist among valid DNS strings that would support the definition of a "type" of TLD. In the case of IDNs and IDN variants, various software applications may treat those strings differently for a variety of services and display purposes as defined by various RFCs, so there is technical merit in describing IDNs and IDN variants as a special "type" of string for some purposes. Any other differentiation is purely based on policy, e.g., TLD applicants who may qualify to apply, intended TLD use, limitations on registrants, etc. String "types" that differentiate along such policy lines lie largely outside the SSAC's purview.

Recommendation 4.1 states:

> *The Working Group recommends differential treatment for certain applications based on either the application type, the string type, or the applicant type. Such differential treatment may apply in one or more of the following elements of the new gTLD Program: Applicant eligibility; Application evaluation process/requirements; Order of processing; String contention; Objections; Contractual provisions.*

The SSAC is concerned about the inclusion of the concept of "TLD type" as a way of differentiating strings for string contention purposes. We note that the subsequent list of iterated circumstances in the Final Report where various TLD types may be considered does not include string contention. The concept of grouping strings together into various string contention sets appears in Topic 24: String Similarity Evaluations (discussed below). The SSAC does *not* support the use of "TLD Types" in order to create separate string contention sets, and further discussion of string contention can be found below (3.3.4).

The SSAC notes that there may be security issues and unintended consequences to be considered if "TLD Type" is used for the ongoing evaluation and categorization of names. Security issues may arise when TLDs that are initially categorized and deployed under some sort of "restrictive" type (e.g. .Brand, Community, or PIC encumbered TLDs), which may require some security-related behaviors, are subsequently reclassified to a looser policy regime. This is further discussed in relation to "intended use" for determining contention sets below (3.3.4).

3.2 Comments on Section 2.3 - Foundational Issues

3.2.1 Comments on Recommendation 9.15

Recommendation 9.15 states:

> *The Working Group acknowledges ongoing important work in the community on the topic of DNS abuse and believes that a holistic solution is needed to account for DNS abuse in all gTLDs as opposed to dealing with these recommendations with respect to only the introduction of subsequent new gTLDs. In addition, recommending new requirements that would only apply to the new gTLDs added to the root in subsequent rounds could result in singling out those new gTLDs for disparate treatment in contravention of the ICANN Bylaws. Therefore, this PDP Working Group is not making any recommendations with respect to mitigating domain name abuse other than stating that any such future effort must apply to both existing and new gTLDs (and potentially ccTLDs).*

The SSAC notes that while this is an overarching issue not limited to new TLDs, the successful adoption of new TLDs by the greater community may very well depend upon dealing with these issues in the near term. Either such PDP work must commence immediately to address them in their entirety prior to the introduction of any new TLDs or new TLD guidance must adopt best practices learned from the prior round to alleviate issues in new TLDs. This subject is covered more thoroughly in Section 2.2.

3.2.2 Comments on Recommendation 11.3

Recommendation 11.3 states:

> *Applicants should be made aware of Universal Acceptance challenges in ASCII and IDN TLDs. Applicants must be given access to all applicable information about Universal Acceptance currently maintained on ICANN's Universal Acceptance Initiative page, through the Universal Acceptance Steering Group, as well as future efforts.*

The SSAC suggests that applicants be required to submit a plan to become ready for Universal Acceptance within a defined time period (for example, less than 3 years from the time of application) in order to ensure that their TLD operations conform to the principles of UA-Readiness (e.g., accept IDN-based email addresses in contact data, accept new gTLD based nameservers) as found in the documents at uasg.tech.[30]

3.3 Comments on Section 2.7 - Application Evaluation/Criteria

3.3.1 Comments on Topic 21: Reserved Names

The Final Report states:

> *The Initial Report requested community input on the possibility of removing the reservation of two-character letter-number combinations at the top level. The Working Group noted that in the 2012 round, digits were disallowed entirely, so*

[30] See Become Universal Acceptance Ready, https://uasg.tech/become-universal-acceptance-ready/

> *any recommendation on this issue would be contingent on the removal of that additional restriction. The Working Group reviewed public comments on this issue, which included a substantial number of responses raising concern about potential confusion with country code top-level domains. The Working Group considered that one possible means of addressing potential confusion would be to conduct an analysis as part of the string similarity review.*

The SSAC strongly recommends continuing to disallow single character TLDs, digit-only TLDs, and two-character letter-number combinations. Our rationale is as follows:

1) RFC952, which is the original host name specification, specifies that the first character of a name must be an alphabet character (A-Z), followed by one or more characters or digits. It should never start with a digit and be followed by one or more letters, digits, or hyphens. It should also never end with a hyphen or a period.[31] A similar definition is used in RFC 1934.

2) RFC 1123 relaxes the restriction that a label must start with an alphabet character by allowing a label to start with either a letter or a digit. However, the RFC also clearly states that the "highest-level component label will be alphabetic."[32] This means that a TLD label cannot contain numbers or hyphens.

3) RFC1123 further requires "...The host SHOULD check the string syntactically for a dotted-decimal number before looking it up in the Domain Name System." Some implementations would parse #.#.#.#. as an IP address and would not look it up in the DNS. The same is true for single character TLDs, where some implementations would parse letters a to f as hexadecimals.

4) Currently, some websites and/or clickbait in phishing have a full numeric label as in http://www.12345678.yourbank.com/ where the number then gets parsed as an IP number, leading to the phisher's attack server. This situation could be exacerbated should hostnames of dotted-decimal form become more prevalent.

Based on the general principle of robustness ("be conservative in what you do; be liberal in what you accept from others"), the SSAC recommends:

- Single (ASCII) character TLDs SHOULD NOT be allowed;
- All-digit TLDs SHOULD NOT be allowed.
- Two-character letter-number combinations SHOULD NOT be allowed at the top level.

[31] See Assumption, RFC 952: DOD Internet Host Table Specification, https://tools.ietf.org/html/rfc952

[32] See Section 2.1 Host Names and Numbers, RFC 1123: Requirements for Internet Hosts -- Application and Support, https://tools.ietf.org/html/rfc1123

3.3.2 Comments on Affirmation 22.1

Affirmation 22.1 states:

> *The Working Group affirms existing registrant protections used in the 2012 round, including the Emergency Back-end Registry Operator (EBERO) and associated triggers for an EBERO event and critical registry functions. In addition, as described under Topic 27: Applicant Reviews: Technical/Operational, Financial and Registry Services, the substantive technical and operational evaluation is being maintained and therefore, protections against registry failure, including registry continuity, registry transition, and failover testing continue to be important registrant protections. The Working Group also supports the registrant protections contained in Specification 6 of the Registry Agreement.*

Rationale for Recommendation 22.7 states:

> *The Working Group agreed that all registrant protections from the 2012 round are appropriate and important in the case of open TLDs. However, the Working Group believes that EBERO requirements should not apply in business models where there are no registrants in need of such protections in the event of a TLD failure. In particular, the Working Group believes that gTLDs that are exempt from Specification 9 (including .Brand TLDs qualified for Specification 13) should also be exempt from Continued Operations Instrument requirements.*

The SSAC advised in SAC103 that "the implications of exempting any TLD from Emergency Back-end Registry Operator (EBERO) requirements should be considered carefully." While the Working Group appears to have accepted that recommendation in Affirmation 22.1, the SSAC is unclear about the somewhat contradictory statement contained in the Rationale for Recommendation 22.7. The SSAC recommends that the ICANN Board and GNSO Council refrain from exempting .Brand TLDs from Continued Operations Instrument requirements.

3.3.3 SSAC Concerns about organization's qualifications

Recommendation 22.4 states:

> *The Working Group supports Recommendation 2.2.b. in the Program Implementation Review Report, which states: "Consider whether the background screening procedures and criteria could be adjusted to account for a meaningful review in a variety of cases (e.g., newly formed entities, publicly traded companies, companies in jurisdictions that do not provide readily available information)."*

Implementation Guidance 27.18 states:

> *Implementation Guidance 27.18: If any of the following conditions are met, an applicant should be allowed to self-certify that it is able to meet the goals as described in Implementation Guidance 27.17. This self-certification will serve as evidence that the applicant has the financial wherewithal to support its application for the TLD.*
>
> *i. If the applicant is a publicly traded corporation, or an affiliate as defined in the current Registry Agreement, listed and in good standing on any of the world's largest 25 stock exchanges (as listed by the World Federation of Exchanges);*
>
> *ii. If the applicant and/or its officers are bound by law in its jurisdiction to represent financials accurately and the applicant is is good standing in that jurisdiction; or,*
>
> *iii. If the applicant is a current registry operator or an affiliate (as defined in the current Registry Agreement) of a current registry operator that is not in default on any of its financial obligations under its applicable Registry Agreements, and has not previously triggered the utilization of its Continued Operations Instrument.*
>
> *If the applicant is unable to meet the requirements for self-certification, the applicant must provide credible third-party certification of its ability to meet the goals as described in Implementation Guidance 27.17.*

The SSAC is disappointed that the Final Report rejects the recommendations contained in SAC103 that "[p]ublicly traded companies must not be exempted from the financial evaluation" and "[n]o applicant should be allowed to self-certify…" While there are some reasonable safeguards called out in the Final Report (e.g., use of only major stock exchanges for public companies) it is very difficult to find standards that are consistent worldwide to address the questions that can relatively easily be answered by direct evaluation. Recently, the US Securities and Exchange Commission (SEC) has been reported to be working on a rule that restricts activities by listed foreign companies that do not allow their books to be audited by established non-local firms[33] due to concerns about varying standards of quality. Certainly providers do not need to repeat the process for topics that do not differ between applications, so one certification can serve for all gTLDs with the exception of those areas with different operational or technical requirements. The SSAC believes that the Final Report's rejection of the SSAC's suggestions in this regard is short-sighted and may inadvertently create loopholes that may compromise the security and stability of the domain name space. The SSAC maintains its positions as stated in SAC103:

Text from SAC103, Section 6.3, Financial and Technical Evaluation

> Publicly traded companies must not be exempted from the financial evaluation. The barrier to be publicly traded is very low in some jurisdictions (such as "penny stocks" in the United States), and such companies do not "undergo extensive ... screenings." For example,in the USA, not all public companies are subject to the

[33] See How China Stars Like Alibaba May Be Forced From U.S., https://www.bloomberg.com/news/articles/2020-05-22/delisting-chinese-firms-gains-traction-in-washington-quicktake

> Securities and Exchange Commission’s reporting requirements. Exemptions should not be extended to, "officers, directors, material shareholders, etc. of these companies," all of whom should be subject to background screening. No applicant should be allowed to self-certify that it has the financial means to support its proposed business model. None of the proposed reasons to allow self-certification provide surety. There is great variance in requirements from jurisdiction to jurisdiction and they provide no reasonable baseline that can replace due diligence during ICANN's evaluation process,

Text from SAC103, Section 6.1, Provider Approval

> Existing providers should not be deemed "pre-approved," and must receive fresh evaluation in the new round. This is not onerous and represents good diligence. For example, the next gTLD contract may contain provisions that differ from the current ones, and existing operation is not synonymous with the ability to handle upcoming requirements.
>
> Back-end providers may provide templated answers, but those answers will sometimes be customized per application depending upon the technical and business plans provided in individual applications. It is therefore not enough to check off a technical provider's generic capabilities. The problem is identifying when an application departs from a provider's template, and which application questions need specific evaluation. This problem can arise in several circumstances, such as when an application proposes a new registry service, when there is a Public Interest Commitment (PIC) obligation, or when a variant technical implementation will be used in the TLD.

3.3.4 Comments on Recommendation 24.3

Recommendation 24.3 states:

> *The Working Group recommends updating the standards of both (a) confusing similarity to an existing top-level domain or a Reserved Name, and (b) similarity for purposes of determining string contention, to address singular and plural versions of the same word, noting that this was an area where there was insufficient clarity in the 2012 round. Specifically, the Working Group recommends prohibiting plurals and singulars of the same word within the same language/script in order to reduce the risk of consumer confusion...*

Is there evidence to support the assertion that singular and plural versions of the same word have caused confusion? There are several examples from the 2012 round where this combination was allowed. What is the data from those examples?

The SSAC stated in SAC103, and reaffirms here, that trying to determine confusability based on the meaning of words rather than the visual similarity of strings is fundamentally misguided. Domain names are not semantically words in any language, notwithstanding the obvious expectation that they will be recognized as such and that it

drives applicants' interest in specific new gTLD strings. In that context the SSAC notes that although some languages (such as English) have distinct singular and plural noun forms that may or may not be visually similar, others (such as Mandarin Chinese and most of the Austronesian languages) do not.

Recommendation 24.3 also states:

> *...Applications will not automatically be placed in the same contention set because they appear visually to be a single and plural of one another but have different intended uses…*

There is grave danger in adopting "intended use" as a defining characteristic for whether applications should be placed in the same contention set or not. There are at least three issues the SSAC sees with this approach:

1) As pointed out in SAC103, which quoted RFC5894,[34] a string has no context on its own prior to delegation and, while an applicant may have a particular context in mind, there is no guarantee that context will prevail indefinitely in practice. It is also questionable whether a majority of registrants or internet users will apply that same context, which may cause confusion and usability issues. In some cases there may be security concerns where a string may imply some provenance of having a secure, vetted, or otherwise controlled registration and/or operational criteria to some set of internet users when, in fact, none exists. This can arise in both "generic" contexts and where specific strings are similar to famous brands and expectations do not match reality.

2) There are many cases where the application's intended use changes significantly over time – in fact, many of the gTLDs currently in use had specific "intended uses" that were changed either by the operator, or simply by how the TLD strings were used by its 2LD registrants. For example, the .pro TLD's original intended use was for the "professional" community, validated by the vetting of professional licenses. Over time, the validation criteria were relaxed and the TLD today is operated similarly to any unrestricted gTLD.

3) The situations identified in points 1 and 2 above would open the door for gaming. Gaming could occur when an applicant applies with an intended use in mind that differs from the stated purpose, in order to obtain preferential treatment based on the criteria. The applicant could relax or change the restrictions on the TLD once delegated citing a panoply of reasons.

Recommendation 6: The SSAC recommends that the words "intended use" be removed as a defining characteristic to determine whether or not applications should be placed in the same contention set.

[34] See SAC103: SSAC Response to the new gTLD Subsequent Procedures Policy Development Process Working Group Initial Report https://www.icann.org/en/system/files/files/sac-103-en.pdf and RFC5894, https://tools.ietf.org/html/rfc5894

3.3.5 Comments on Recommendation 24.6

Recommendation 24.6 states:

> *Eliminate the use of the SWORD tool in subsequent procedures.*

Replacing one defective tool with another may not be a good solution for the community. If a new tool were to be used, it would have to be subjected to community based evaluation, including possibly source code examination, to ensure that biases and other problems that beset the 2012 tool did not recur in a replacement.

3.3.6 Comments on Topic 26: Security and Stability

Topic 26 deals with core SSR issues that were considered by the Working Group.

The SSAC notes and appreciates that the Final Report adopted several prior SSAC and RSSAC recommendations in this topic area, including:

- Recommendation 26.1: Strings must not cause any technical instability
- Recommendation 26.2: ICANN must honor and review the principle of conservatism when adding new gTLDs to the root zone
- Recommendation 26.3: ICANN must focus on the rate of change for the root zone over smaller periods of time (e.g., monthly) rather than the total number of delegated strings for a given calendar year
- Recommendation 26.9: Emoji in domain names, at any level, must not be allowed

These overall recommendations are important guidelines for any plan to expand the number of TLDs in the DNS Root Zone. The SSAC notes three areas that remain of some concern for the stability of the DNS Root Zone based on the implementation guidance contained in Final Report(26.5, 26.6 and 26.8).

> *Implementation Guidance 26.5: ICANN should structure its obligations to new gTLD registries so that it can delay their addition to the root zone in case of DNS service instabilities. Objective criteria should be developed to determine what could be classified as a "service instability."*

The proposed mitigation of DNS service instabilities detected during roll-out of new TLDs is to merely delay addition of new zones. This appears to assume such instabilities are transient and solvable in a short period of time and do not cover cases where larger instabilities and potential systemic issues are uncovered that may require halting or even scaling back TLD delegations. Such circumstances would likely require contractual or well-constructed consensus policies to provide the necessary controls to allow ICANN to deal with a major issue. While the guidance correctly calls for objective criteria to be developed to determine when a service instability occurs, it does not provide guidance on who would be expected to make a call and implement corrective actions. This gap should be addressed.

> *Implementation Guidance 26.6:ICANN should investigate and catalog the long term obligations for root zone operators of maintaining a larger root zone.*

This guidance along with the associated rationale leaves the term "obligations" very vague. Further, the SSAC notes that the term "root zone operators" does not completely encompass the universe of entities that serve the root zone or are affected by its size, such as recursive operators with large client bases and those who engage in security tactics like negative caching.

> *Implementation Guidance 26.8: ICANN should continue developing the monitoring and early warning capability with respect to root zone scaling.*

The SSAC notes the recent publication of OCTO-015,[35] "Recommendations for Early Warning for Root Zone Scaling," which discusses this concept and concludes that such a system is not likely to be feasible. The SSAC will comment separately on that document but is concerned that the important guidance for recommendation 26.8, which mirrors similar recommendations from SAC046[36] and SAC100,[37] may not be implemented. On the issue of early warning systems, the RSSAC is also investigating what a failure of the RSS might look like and investigating ways to detect such a failure. If the exploration is successful, RSSAC could issue advice which would help establish an early warning framework.[38]

3.3.7 Comments on Recommendation 29.1

Recommendation 29.1 states:

> *ICANN must have ready prior to the opening of the Application Submission Period a mechanism to evaluate the risk of name collisions in the New gTLD evaluation process as well as during the transition to delegation phase.*

Affirmation 29.2 states:

> *The Working Group affirms continued use of the New gTLD Collision Occurrence Management framework unless and until the ICANN Board adopts a new mitigation framework. This includes not changing the controlled interruption duration and the required readiness for human-life threatening conditions for currently delegated gTLDs and future new gTLDs.*

---

[35] See OCTO-015: Recommendations for Early Warning for Root Zone Scaling, https://www.icann.org/en/system/files/files/octo-015-01oct20-en.pdf

[36] See SAC046: Report of the Security and Stability Advisory Committee on Root Scaling, https://www.icann.org/en/system/files/files/sac-046-en.pdf

[37] See SAC100: SSAC Response to the New gTLD Subsequent Procedures Policy Development Process Working Group Request Regarding Root Scaling, https://www.icann.org/en/system/files/files/sac-100-en.pdf

[38] See RSSAC052: Statement on Recommendations for an Early Warning System for Root Zone Scaling, https://www.icann.org/en/system/files/files/rssac-052-25nov20-en.pdf

The SSAC disagrees with Affirmation 29.2, as it suggests we already know everything we need to know and therefore a new gTLD round could proceed according to the currently documented Name Collision Occurrence Management Framework.[39]

The SSAC has reported multiple times[40,41,42] that there are issues to be considered and we should take this opportunity to study the past round and ensure that a Collision Occurrence Management framework that is thorough, complete, and balanced is developed and deployed *before* a new gTLD round results in adding new TLDs to the root zone. The ICANN Board has taken note of these observations and launched the Name Collision Analysis Project[43] to address these concerns and to provide guidance to the Board as to how to proceed.

3.3.8 Comments on Implementation Guidance 29.5

Implementation Guidance 29.5 states:

> *The ICANN community should develop name collision risk criteria and a test to provide information to an applicant for any given string after the application window closes so that the applicant can determine if they should move forward with evaluation.*

The SSAC notes that this is one of the few cases where there is a specific assignment of responsibility to the "ICANN Community."The SSAC does not agree with this specific assignment. This work is already properly included in the Name Collision Analysis Project and believes the assignment here should be more generally to ICANN, similar to most advice, so the proper assignment of this work can be made when it is deployed.

Recommendation 7: The SSAC recommends that the ICANN Board, prior to authorizing the addition of new gTLDs to the root zone, receive and consider the results of the Name Collision Analysis Project, pursuant to Board Resolution 2017.11.02.30.[44]

[39] See Name Collision Occurrence Management Framework, https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf

[40] See SAC062: SSAC Advisory Concerning the Mitigation of Name Collision Risk, https://www.icann.org/en/groups/ssac/documents/sac-062-en.pdf

[41] See SAC066: SSAC Comment Concerning JAS Phase One Report on Mitigating the Risk of DNS Namespace Collisions, https://www.icann.org/en/system/files/files/sac-066-en.pdf

[42] See SAC090: SSAC Advisory on the Stability of the Domain Namespace, https://www.icann.org/en/system/files/files/sac-090-en.pdf

[43] See Approved Board Resolutions, Consideration of .CORP, .HOME, and .MAIL and other Collision Strings, https://www.icann.org/resources/board-material/resolutions-2017-11-02-en#2.a

[44] See Approved Board Resolutions, Consideration of .CORP, .HOME, and .MAIL and other Collision Strings, https://www.icann.org/resources/board-material/resolutions-2017-11-02-en#2.a

4 Recommendations

While the comments in Section 3 of this document were developed to provide input to the GNSO New gTLD Subsequent Procedures Policy Development Process Working Group, this Comment is being published after their work has completed. The SSAC took an in-depth look at broader issues related to this topic space and used this opportunity to provide substantive comments and recommendations on the future of deploying new TLDs. Thus, this recommendation section is directed to the ICANN Board with the intention of considering comments specific to the final report from the GNSO New gTLD Subsequent Procedures Policy Development Process Working Group as part of their deliberations of that report.

Recommendation 1: The SSAC recommends that the ICANN Board initiate a fundamental review to determine whether continuing to increase the number of gTLDs is consistent with ICANN's strategic objective to "evolve the unique identifier systems in coordination and collaboration with relevant parties to continue to serve the needs of the global Internet user base." This review should be considered an input towards updating ICANN's strategic goals in conjunction with implementing the CCT Review Team's recommendations. Such a fundamental review should include at least the following areas of study based on prior rounds of the New gTLD program:

- Impacts on root server operations
- Impacts on SSR issues
- Impacts on overall DNS operations
- Analysis of how all metrics for success were met
- Risk analysis

Recommendation 2: The SSAC recommends that, as part of the process for creating new gTLDs, ICANN develop and adopt a protocol for measuring progress against stated goals of the program and thresholds, which if crossed, may require mitigation actions. Such measurements and actions should consider the entirety of the DNS ecosystem.

Recommendation 3: The SSAC recommends that the ICANN Board, prior to launching the next round of new gTLDs, commission a study of the causes of, responses to, and best practices for mitigation of the domain name abuse that proliferates in the new gTLDs from the 2012 round. This activity should be done in conjunction with implementing the CCT Review Team's relevant recommendations. The best practices should be incorporated into enforced requirements, as appropriate, for at least all future rounds.

Recommendation 4: The SSAC recommends the ICANN Board take the comments in SAC114, Sections 3.1-3.3 into consideration in the Board's deliberations on the following items:

1) accepting the recommendations of the Final Report on the new gTLD Subsequent Procedures Policy Development Process;
2) subsequent implementations of the approved recommendations developing the policy; and
3) the implementation of the policy.

Recommendation 5: The SSAC recommends that ICANN org develop reference materials or a set of tutorials to teach the basics of registry service provision as a prerequisite for new registry service providers. The purpose of the reference materials is to educate potential registry service providers on the requirements and testing thresholds for pre-delegation testing.

Recommendation 6: The SSAC recommends that the words "intended use" be removed as a defining characteristic to determine for whether applications should be placed in the same contention set or not.

Recommendation 7: The SSAC recommends that the ICANN Board, prior to authorizing the addition of new gTLDs to the root zone, receive and consider the results of the Name Collision Analysis Project, pursuant to Board Resolution 2017.11.02.30.

5 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 Comment. The Dissents and Withdrawals 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. This section also identifies individual members who have withdrawn and recused themselves from discussion of the subject matter of this Comment. Except for members listed in the Dissents and Withdrawals section, this document has the consensus approval of all members of the SSAC.

5.1 Acknowledgments

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

SSAC members
Jaap Akkerhuis
Lyman Chapin
KC Claffy
James Galvin
Julie Hammer
Geoff Huston
Merike Kaeo
Warren Kumari
Barry Leiba
Ram Mohan
Rod Rasmussen
Suzanne Woolf

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

5.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: https://www.icann.org/resources/pages/ssac-biographies-2021-01-07-en

5.3 Dissents and Withdrawals

There were no dissents or withdrawals.