SAC103
SSAC Response to the new gTLD Subsequent Procedures Policy Development Process Working Group Initial Report

An Advisory from the ICANN Security and Stability Advisory Committee (SSAC)
3 October 2018

Preface

This is an advisory to the ICANN Board, the ICANN Organization staff, the ICANN community, and, more broadly, the Internet community from the ICANN Security and Stability Advisory Committee (SSAC) about the new gTLD Subsequent Procedures Policy Development Process Working Group Initial Report.

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 SSAC welcomes this opportunity to provide input on the Initial Report of the new gTLD Subsequent Procedures Policy Development Process (PDP) Working Group (WG).[1] The SSAC previously provided input to this PDP WG in December 2017 on the subject of root scaling.[2]

Foremost, the SSAC is concerned that the new gTLD Subsequent Procedures PDP WG is moving too quickly. Specifically, they are not awaiting the completion of requisite dependent activities meant to serve as input to their work before consuming considerable resources from the community with these reviews. In particular, the Competition, Consumer Trust, and Consumer Choice Review (CCT) Final Report includes substantial recommendations related to improving security, stability, and resiliency related safeguards.[3] These recommendations need to be taken into account before requesting input on a subsequent round of TLDs, based on the review team's conclusion that the current safeguards have not been sufficiently effective.

Moreover, the current (2012) round has still not finished and there remain unresolved issues whose solutions must inform contractual, policy, and technical aspects of subsequent rounds. Attempting to get ahead of those efforts unnecessarily consumes considerable resources and creates a needless risk of making decisions without critical information. The ICANN Board Organizational Effectiveness Committee or other appropriate ICANN organization function should ensure that interdependence and optimal ordering is managed effectively here.

This report is organized by subject matter and includes regular references to the specific questions and preliminary recommendations given in the new gTLD Subsequent Procedures PDP WG Initial Report.[4] Each section begins with a listing of relevant questions and/or preliminary recommendations from the Initial Report then follows with the SSAC's comment. In this report the SSAC limits its advice to its scope and role.

[1] See Initial Report on the new gTLD Subsequent Procedures Policy Development Process (Overarching Issues & Work Tracks 1-4), https://gnso.icann.org/en/issues/new-gtlds/subsequent-procedures-initial-overarching-issues-work-tracks-1-4-03jul18-en.pdf

[2] See SAC100

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

[4] See Public Comment on the Initial Report on the New gTLD Subsequent Procedures Policy Development Process (Overarching Issues & Work Tracks 1-4), https://www.icann.org/public-comments/gtld-subsequent-procedures-initial-2018-07-03-en

2 Reserved Names and String Similarity

Preliminary Recommendations from the PDP Initial Report

Preliminary Recommendation	2.7.1.c.1: Reservation at the top level: Keep all existing reservations, but add:
Preliminary Recommendation	2.7.1.c.1.2: Special-Use Domain Names through the procedure described in IETF RFC 6761.
Preliminary Recommendation	2.7.4.c.1: Work Track 3 recommends adding detailed guidance on the standard of confusing similarity as it applies to 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 Work Track recommends:
Preliminary Recommendation	2.7.4.c.1.1: Prohibiting plurals and singulars of the same word within the same language/script in order to reduce the risk of consumer confusion. For example, the TLDs .CAR and .CARS could not both be delegated because they would be considered confusingly similar.
Preliminary Recommendation	2.7.4.c.1.2: Expanding the scope of the String Similarity Review to encompass singulars/plurals of TLDs on a per-language basis. If there is an application for the singular version of a word and an application for a plural version of the same word in the same language during the same application window, these applications would be placed in a contention set, because they are confusingly similar. An application for a single/plural variation of an existing TLD would not be permitted. Applications should not be automatically disqualified because of a single letter difference with an existing TLD. For example, .NEW and .NEWS should both be allowed, because they are not singular and plural versions of the same word.

2.1 Special-Use Domain Names

The following is excerpted from SAC090.[5]

> In the Applicant Guidebook for the most recent round of new generic Top Level Domain (gTLD) applications, ICANN cited or created several lists comprising strings that were prohibited as new gTLD names, such as the “reserved names” listed in Section 2.2.1.2.1, the “ineligible strings” listed in Section 2.2.1.2.3, the two-character ISO 3166 codes proscribed by reference in Section 2.2.1.3.2 Part III, and the geographic names proscribed by reference in Section 2.2.1.4. More recently, the IETF has placed a small number of

[5] See SAC090

potential gTLD strings into a Special-Use Domain Names Registry.[6] As described in RFC 6761, a string that is placed into this registry is expected to be processed in a defined "special" way that may be different from the normal process of DNS resolution.

Should ICANN formalize in policy the status of the names on these lists? If so:

I. How should ICANN respond to changes that other parties may make to lists that are recognized by ICANN but are outside the scope of ICANN's direct influence?

II. How should ICANN respond to a change in a recognized list that occurs during a round of new gTLD applications?

2) The IETF is an example of a group outside of ICANN that maintains a list of "special use" names. What should ICANN's response be to groups outside of ICANN that assert standing for their list of special names?

2.2 Singularity and Plurality in new gTLDs

The SSAC believes that a clear and consistent set of rules for 'confusing similarity' should be developed, in accordance with the Conservatism Principle,[7] and the resulting rules should be applied in subsequent rounds of new gTLDs.

This may not be as simple or straightforward as the above referenced preliminary recommendations state. For example, singular and plural noun forms are represented differently by different languages, and not all languages have two distinct modes of grammatical number; some have four, and others have none at all. Depending on the language and the noun, singular and plural forms may or may not be visually confusable. In English, for example, "language" and "languages" are visually similar; "mouse" and "mice" are not. In Arabic, sound plurals (which are created simply by adding a suffix to the singular form) are visually similar; broken plurals (which change the internal structure of the singular) are not.

Beyond visual similarity, trying to determine confusability based on the meaning of words is fundamentally misguided, as domain names are not semantically *words* in any language. From RFC 5894, "Internationalized Domain Names for Applications (IDNA): Background, Explanation, and Rationale":[8]

[6] See IANA Special-Use Domain Names, https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xhtml

[7] See SAC089

[8] See RFC5894, https://tools.ietf.org/html/rfc5894

> “DNS labels and fully-qualified domain names provide mnemonics that assist in identifying and referring to resources on the Internet. … **But domain "names" are not, in general, words in any language.** The recommendations of the IETF policy on character sets and languages (BCP 18 [RFC2277]) are applicable to situations in which language identification is used to provide language-specific contexts. The DNS is, by contrast, global and international and ultimately has nothing to do with languages. Adding languages (or similar context) to IDNs generally, or to DNS matching in particular, would imply context-dependent matching in DNS, which would be a very significant change to the DNS protocol itself. It would also imply that users would need to identify the language associated with a particular label in order to look that label up. That knowledge is generally not available because many labels are not words in any language and some may be words in more than one.”

3 Internationalized Domain Names

Questions and Preliminary Recommendations from the PDP Initial Report

Preliminary Recommendation	2.7.5.c.1: General agreement in Work Track 4 that IDNs should continue to be an integral part of the program going forward (as indicated in Principle B of the original Final Report on New gTLDs).
Preliminary Recommendation	2.7.5.c.2: General agreement that compliance with Root Zone Label Generation Rules (RZ-LGR, RZ-LGR-2, and any future RZ-LGR rules sets) should be required for the generation of IDN TLDs and valid variants labels.
Preliminary Recommendation	2.7.5.c.3: General agreement that 1-Unicode character gTLDs may be allowed for script/language combinations where a character is an ideograph (or ideogram) and do not introduce confusion risks that rise above commonplace similarities, consistent with SSAC and Joint ccNSO-GNSO IDN Workgroup (JIG) reports. Please see relevant question in section (f) below.
Preliminary Recommendation	2.7.5.c.4: Implementation Guidance: General agreement that to the extent possible, compliance with IDNA2008 (RFCs 5890-5895) or its successor(s) and applicable Root Zone Label Generation Rules (RZ-LGR, RZ-LGR-2, and any future RZ-LGR rules sets) be automated for future applicants.
Preliminary Recommendation	2.7.5.c.5: Implementation Guidance: General agreement that if an applicant is compliant with IDNA2008 (RFCs 5890-5895) or its successor(s) and applicable LGRs for the scripts it intends to support, Pre-Delegation Testing should be unnecessary for the relevant scripts.
Preliminary Recommendation	2.7.5.c.6: IDN gTLDs deemed to be variants of already existing or applied for TLDs will be allowed provided: (1) they have the same registry operator implementing, by force of written agreement, a policy of cross-variant TLD bundling and (2) The applicable RZ-LGR is already available at the time of application submission.
Option	2.7.5.d.1: Question 2.7.5.e.2 below regarding “bundling” asks whether the unification of implementation policies with respect to how variants are handled in gTLDs are matters for this PDP to consider or whether those matters should be handled through an Implementation Review Team or by each individual registry operator.
Question	2.7.5.e.1: For the recommendation regarding 1-Unicode character gTLDs above, can the more general “ideograph (or ideogram)” be made more precise and predictable by identifying the specific scripts where the recommendation would apply? Please see script names in ISO 15924.

Question	2.7.5.e.2: Should the policy of bundling second-level domains across variant TLDs be unified for all future new gTLDs or could it be TLD-specific? If unified, should it be prescribed in the Working Group final report or chosen at implementation? If TLD-specific, could it be any policy that adequately protects registrants, or would it need to be chosen from a menu of possible bundling implementations? Currently known bundling strategies include PIR's .ong/.ngo, Chinese Domain Name Consortium guidance and Latin-script supporting ccTLDs such as .br and .ca.
Question	2.7.5.e.3: Are there any known specific scripts that would require manual validation or invalidation of a proposed IDN TLD?
Question	2.7.5.e.4: For IDN variant TLDs, how should the Work Track take into account the Board requested and yet to be developed IDN Variant Management Framework?

The SSAC agrees with the preliminary recommendations that subsequent rounds of new gTLDs should be compatible with IDNA 2008[9,10] or its successor, and that Label Generation Rulesets (LGRs)[11] should be required for the generation of Internationalized Domain Name (IDN) TLDs and valid variant labels for the root zone. Sections below contain additional SSAC comments on several of the recommendations listed above.

3.1 TLD Bundling

The problem of "synchronization" of TLDs has been studied previously and it is clear that there are no generally applicable technical approaches that work consistently in the DNS. Informally, the goal of TLD bundling is for domain names that are identical below the level of the bundled TLDs to behave "the same" in all of the contexts in which users might encounter them. As documented by the Registry Services Technical Evaluation Panel (RSTEP) study of the Public Interest Registry (PIR) proposal to bundle .NGO and .ONG,[12] it is not possible to achieve this goal through purely technical means within the DNS. The RSTEP review concluded that PIR did not intend to market the .NGO/.ONG bundle to registrants as if it achieved this goal, and approved the proposal on that basis with the following warning:

[9] See RFCs 5890-5895, https://tools.ietf.org/html/rfc5890, https://tools.ietf.org/html/rfc5891, https://tools.ietf.org/html/rfc5892, https://tools.ietf.org/html/rfc5893, https://tools.ietf.org/html/rfc5894, https://tools.ietf.org/html/rfc5895

[10] See SAC095

[11] See RFC 7940, https://tools.ietf.org/html/rfc7940

[12] See Public Comment on the Registry Services Technical Evaluation Panel (RSTEP) Report on Public Interest Registry's Request to Implement Technical Bundling in .NGO and .ONG, https://www.icann.org/public-comments/rstep-technical-bundling-2014-07-29-en

> "There is no indication that PIR will market the service as causing a pair of names from a bundle to "be the same," to "act the same," or other phrases that would cause more significant security and stability issues. However it would be prudent to expect that registrars will perceive both names in the bundle to be "the same" because most EPP transactions on one name will automatically apply to the other. That is likely to pervade their thinking, both in terms of provisioning and engineering. This in turn is likely to trickle down into customer communications, perhaps in an even more garbled form, that reach registrants and the general public. It will require great care by all parties to make sure that wrong or misleading expectations are not set over "sameness" or at least kept to a minimum."

The SSAC advises the new gTLD Subsequent Procedures PDP WG to observe the findings of this RSTEP review in any resolution of Question 2.7.5.e.2.

3.2 Single Character Unicode gTLDs

In 2.7.5.c.3, the GNSO found general agreement to allow 1-unicode character TLDs for ideographs.

The SSAC expresses the following concern: For ideographic scripts such as Han, not only can a single character represent a complete "word" or idea, but in some cases different single characters can represent the same "word" or idea. Were ICANN to delegate each such different single character as a TLD label (whether to the same or to a different registrant), users would likely be subject to confusion based on varying deployments of the single character, defined by registry policy. The problem of "synchronization" of TLDs has been studied previously and it is clear that there are no unified technical approaches that work consistently in the DNS. To the extent that two or more different single characters that have the same meaning (variants) may be delegated, a context-free single-character TLD could represent a higher degree of confusability than an equivalent multi-character TLD with at least one non-confusable character.

3.3 IDN Variant Management Framework

In responding to 2.7.5.e.4, the SSAC believes the Work Track should take into account the IDN Variant Management Framework that has been requested by the Board and is currently under development.[13]

[13] See Recommendations for Managing IDN Variant Top-Level Domains, https://www.icann.org/public-comments/managing-idn-variant-tlds-2018-07-25-en

4 Security and Stability

Questions and Preliminary Recommendations from the PDP Initial Report

Question	2.5.1.e.6: Are we acknowledging and accepting of ICANN being a so-called "registry of registries" (i.e., does the community envision ICANN approving a few thousand / hundreds of thousands / millions of gTLDs to be added to the root? Should there be a cap?)
Preliminary Recommendation	2.7.6.c.1: In the 2012-round, some applicants ended up applying for reserved or otherwise ineligible strings, causing them to later withdraw or be rejected. Towards preventing that and streamlining application processing, the Work Track suggests the following as Implementation Guidance: The application submission system should do all feasible algorithmic checking of TLDs, including against RZ-LGRs and ASCII string requirements, to better ensure that only valid ASCII and IDN TLDs can be submitted. A proposed TLD might be algorithmically found to be valid, algorithmically found to be invalid, or verifying its validity may not be possible using algorithmic checking. Only in the latter case, when a proposed TLD doesn't fit all the conditions for automatic checking, a manual review should occur to validate or invalidate the TLD.
Preliminary Recommendation	2.7.6.c.2: For root zone scaling, the Work Track generally supports raising the delegation limit, but also agrees that ICANN should further develop root zone monitoring functionality and early warning systems as recommended by the SSAC, the RSSAC and the technical community.
Question	2.7.6.e.1: To what extent will discussions about the Continuous Data-Driven Analysis of Root Stability (CDAR) Report, and the analysis on delegation rates, impact Working Group discussions on this topic? How about the input sought and received from the SSAC, RSSAC, and the ICANN organization discussed below in section (f), under the heading Root Zone Scaling?
Question	2.7.6.e.2: The SSAC strongly discourages allowing emoji in domain names at any level and the Work Track is supportive of this position. Do you have any views on this issue?

4.1 Root Zone Scaling

The WG's recommendations will lower the barriers to making applications. For example, they seem to envision lower application costs in general (by emphasizing the revenue-neutral application principle), and create a streamlined process to evaluate and approve back-end providers, which will lower application costs for applicants (and will lower evaluation costs for the ICANN Organization). There are also questions such as, "Is there a way in which the application fee can be structured such that it can encourage competition and innovation?", which implies lower fees for at least some applications.

In such an environment, item 2.5.1.e.6 becomes important. How many more TLDs will be introduced? And can ICANN scale its operations to handle that many TLDs? This poses several security and stability issues. One issue is not so much whether the root zone can accommodate additional entries (see 2.7.6.c.2), but whether the ICANN organization's operations can scale.

The following is excerpted from SAC100.[14]

> **Recommendation (4): ICANN should investigate and catalog the long term obligations of maintaining a larger root zone.**
>
> A larger root zone may increase the complexity and cost of activities that operate on the entirety of the root zone. ICANN should investigate how increasing the size of the root zone will impact activities such as the DNSSEC Key Signing Key (KSK) rollover, IANA root zone change requests, TLD transfers, contract negotiations, the operations of the root zone maintainer, and any other administrative overhead. The ongoing management of these activities should be investigated prior to increasing the number of delegations in the root zone.

The SSAC is pleased to see a preliminary recommendation from the working group calling for the ICANN organization to further develop root zone monitoring functionality and early warning systems, as it previously recommended.[15] The SSAC also previously stated that the working group recommendations should include an acceptable rate of change to the root zone instead of a yearly delegation limit, and that obligations to new gTLD registries should be structured so that their addition to the root zone can be delayed in case of DNS service instabilities.[16]

4.2 Emoji in Domain Names

The SSAC continues to believe that emoji introduce security risks when present in any label of a domain name, and that emoji must not be permitted in TLDs.[17]

4.3 Domain Name Abuse

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). Further research is

[14] See SAC100, recommendation 4

[15] See SAC100, recommendation 1 & SAC042

[16] See SAC100, recommendations 2 and 3

[17] See SAC095

needed to better understand the scale of domain name abuse that is attributable to the introduction of new gTLDs in 2012, and the SSAC is highly likely to study this issue further in the near future.

5 Name Collisions

Questions and Preliminary Recommendations from the PDP Initial Report

Preliminary Recommendation	2.7.8.c.1: Include a mechanism to evaluate the risk of name collisions in the TLD evaluation process as well during the transition to delegation phase.
Preliminary Recommendation	2.7.8.c.2: Use data-driven methodologies using trusted research-accessible data sources like Day in the Life of the Internet (DITL) and Operational Research Data from Internet Namespace Logs (ORDINAL) .
Preliminary Recommendation	2.7.8.c.3: Efforts should be undertaken to create a "Do Not Apply" list of TLD strings that pose a substantial name collision risk whereby application for such strings would not be allowed to be submitted.
Preliminary Recommendation	2.7.8.c.4: In addition, a second list of TLDs should be created (if possible) of strings that may not pose as high of a name collision risk as the "Do Not Apply" list, but for which there would be a strong presumption that a specific mitigation framework would be required.
Preliminary Recommendation	2.7.8.c.5: Allow every application, other than those on the "do not apply" list, to file a name collision mitigation framework with their application.
Preliminary Recommendation	2.7.8.c.6: During the evaluation period, a test should be developed to evaluate the name collision risk for every applied-for string, putting them into 3 baskets: high risk, aggravated risk, and low risk. Provide clear guidance to applicants in advance for what constitutes high risk, aggravated risk, and low risk.
Preliminary Recommendation	2.7.8.c.7: High risk strings would not be allowed to proceed and would be eligible for some form of a refund.
Preliminary Recommendation	2.7.8.c.8: Aggravated risk strings would require a non-standard mitigation framework to move forward in the process; the proposed framework would be evaluated by an RSTEP panel.
Preliminary Recommendation	2.7.8.c.9: Low risk strings would start controlled interruption as soon as such finding is reached, recommended to be done by ICANN org for a minimum period of 90 days (but likely more considering the typical timeline for evaluation, contracting and delegation).
Preliminary Recommendation	2.7.8.c.10: If controlled interruption (CI) for a specific label is found to cause disruption, ICANN org could decide to disable CI for that label while the disruption is fixed, provided that the minimum CI period still applied to that string.
Question	2.7.8.e.1: Is there a dependency between the findings from this Working Group and the Name Collisions Analysis Project (NCAP)? If there is, how should the PDP Working Group and NCAP Work Party collaborate in order to move forward? Or, should the PDP Working Group defer all name collision recommendations to NCAP?

Question	2.7.8.e.2: In the event that the NCAP work is not completed prior to the next application round, should the default be that the same name collision mitigation frameworks in place today be applied to those TLDs approved for the next round?
Question	2.7.8.e.3: The Work Track generally agreed to keep the controlled interruption period at 90 days due to lack of consensus in changing it. Some evidence indicated a 60-day period would be enough. Though no evidence was provided to require a longer period, other Work Track members argued for a longer 120 days. What length do you suggest and why? Note that the preliminary recommendation to have ICANN org conduct CI as early as possible would likely mitigate potential delays to applicants in launching their TLD. Are there concerns with ICANN org being responsible for CI?
Question	2.7.8.e.4: During the first 2 years following delegation of a new gTLD string, registry operators were required to implement a readiness program ensuring that certain actions be taken within a couple of hours in the event that a collision was found which presented a substantial risk to life. The 2-year readiness for possible collisions was kept as determined in the Name Collision Management Framework, but some in the Work Track felt that the service level for 2012 was too demanding. What would be a reasonable response time?
Question	2.7.8.e.5: If ICANN were initially required to initially delegate strings to its own controlled interruption platform and then later delegate the TLD to the registry, would that unreasonably increase the changes to the root zone?
Question	2.7.8.e.6: What threat vectors for name collisions in legacy gTLDs should the Working Group consider, and what mitigation controls (if any) can be used to address such threats?
Question	2.7.8.e.7: Regarding the “do not apply” and “exercise care” lists, how should technical standards for these categories be established? Should experts other than those involved in NCAP be consulted?
Question	2.7.8.e.8: As applicants are preliminarily recommended above to be allowed to propose name collision mitigation plans, who should be evaluating the mitigation frameworks put forth by applicants? Should RSTEP be utilized as preliminarily recommended above or some other mechanism/entity?

> "The term “name collision” refers to the situation in which a name that is properly defined in one operational domain or naming scope may appear in another domain (in which it is also syntactically valid), where users, software, or other functions in that

> domain may misinterpret it as if it correctly belonged there. The circumstances that may cause this can be accidental or malicious."[18]

The SSAC is currently investigating the topic of name collisions in its role as facilitator of the Name Collision Analysis Project (NCAP). The scope of NCAP is to identify suggested criteria for determining whether a specific undelegated string should be considered a string that manifests name collisions, (i.e.) placed in the category of a Collision String. The distinction is important to establish clear expectations of the output of the project.

The NCAP consists of three studies. The goal of the first study, as set out in the project plan, is to review all previous work on the subject of Name Collisions. The goals of the second study are to understand both the root cause of a majority of the name collisions, and impact of any choice made regarding .CORP, .HOME, and .MAIL, including leaving them undelegated.

The goals of the third study are twofold. First to identify all the possible mitigation options, particularly those proposed by applicants or other interested parties, and examine each in depth to assess the potential mitigation each can offer. The second goal is to produce guidance on the delegation of .CORP, .HOME, and .MAIL and other strings where name collisions will occur.

The SSAC does not believe it is its role to determine the dependency between NCAP and the next round of new gTLD applications. That decision rests with the ICANN Community and ICANN Board. SSAC provides the following advice to those deciding on the dependency:

> a) If delegation takes place before the risks are understood (i.e. Study 2 is complete) then it is highly likely there will be significant problem in some unspecified TLDs.
>
> b) If application begins before the risks are understood then when the names are known it is possible that the data collection will be compromised through such mechanisms or gaming or preparatory use, and the NCAP will be unable to produce a result.

[18] See SAC062

6 Evaluating Providers

Questions and Preliminary Recommendations from the PDP Initial Report

Question	2.2.6.e.5: Existing RSPs: Should existing RSPs be automatically deemed "pre-approved"? Why or why not? If not automatically pre-approved, should existing RSPs have a different process when seeking to become pre-approved? If so, what would the different process be? Are there any exceptions to the above? For example, should a history of failing to meet certain Service Levels be considered when seeking pre-approval? Please explain.
Preliminary Recommendation	2.7.2.c.2: Single registrant TLDs (including those under Specification 13) should be exempt from EBERO requirements.
Preliminary Recommendation	2.7.2.c.3: Continue to allow publicly traded companies to be exempt from background screening requirements as they undergo extensive similar screenings, and extend the exemption to officers, directors, material shareholders, etc. of these companies.
Question	2.7.2.e.2: Should specific types of TLDs be exempt from certain registrant protections? If yes, which ones should be exempt? Should exemptions extend to TLDs under Specification 9, which have a single registrant? TLDs under Specification 13, for which registrants are limited to the registry operator, affiliates, and trademark licensees? If you believe exemptions should apply, under what conditions and why? If not, why not?
Preliminary Recommendation	2.7.7.c.7: For Technical and Operational Evaluation: Do not require a full IT/Operations security policy from applicants.
Preliminary Recommendation	"2.7.7.c.12: For Financial Evaluation: Substitute the 2012 AGB evaluation of an applicant's proposed business models and financial strength with the following: - An applicant must identify whether the financials in its application apply to all of its applications, a subset of them or a single one (where that applicant (and/or its affiliates have multiple applications). - ICANN won't provide financial models or tools, but it will define goals and publish lists of RSPs, organizations (like RySG and BRG) and consultants. - The goals of a financial evaluation are for the applicant to demonstrate financial wherewithal and assure long-term survivability of the registry. Therefore, the evaluation should look at whether an applicant could withstand not achieving revenue goals, exceeding expenses, funding shortfalls, or inability to manage multiple TLDs in the case of registries that are dependent upon the sale of registrations. However, there should also be a recognition that there will be proposed applications that will not

	be reliant on the sale of third party registrations and thus should not be subject to the same type of evaluation criteria. In other words, although the goals of the financial evaluation are to determine the financial wherewithal of an applicant to sustain the maintenance of a TLD, the criteria may be different for different types of registries. Criteria should not be established in a "one-size-fits-all" manner. - If any of the following conditions are met, an applicant should be allowed to self-certify that it has the financial means to support its proposed business model associated with the TLD: If the applicant is a company traded on an applicable national public market; If the applicant and/or its Officers are bound by law in its jurisdiction to represent financials accurately; If the applicant is 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. - The applicant is required to provide credible 3rd-party certification of those goals if self-certification above is not used or achievable."
Question	2.7.7.e.6: In Financial Evaluation, subsection 2.d, an exemption for public-traded companies is suggested. The Work Track hasn't considered whether to include affiliates in that exemption; should it be changed to also allow exemption in such cases?
Preliminary Recommendation	2.11.1.c.3: Rely on Service Level Agreement (SLA) monitoring for most if not all overall registry service provider testing.

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.

6.2 EBERO Exemption

The implications of exempting any TLD from Emergency Back-end Registry Operator (EBERO) requirements should be considered carefully. For example, it is possible for domains in other TLDs to rely on nameservers in a single-registrant gTLD. If any gTLD is exempted from EBERO requirements, there must first be some assurance that no other domain outside the exempted gTLD can ever rely upon the exempted gTLD for resolution.

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 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.

For Technical and Operational Evaluations, a full IT/Operations security policy from applicants must be required. The goal of the technical evaluation is for the applicant to demonstrate its expertise and assure the secure and stable operation of the registry.

6.4 Provider Testing

Recommendation 2.11.1.c.3 is to "Rely on Service Level Agreement (SLA) monitoring for most if not all overall registry service provider testing." 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.

7 Acknowledgments, Disclosures of Interests, 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 Disclosures 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 sections, this document has the consensus approval of all of the members of SSAC.

7.1 Acknowledgments

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

SSAC members
Greg Aaron
Lyman Chapin
kc claffy
Patrik Fältström
James Galvin
Julie Hammer
John Levine
Danny McPherson
Rod Rasmussen

ICANN staff
Andrew McConachie (editor)
Kathy Schnitt
Steve Sheng

7.2 Disclosures of Interest

SSAC member biographical information and Disclosures of Interest are available at: https://www.icann.org/resources/pages/ssac-biographies-2018-03-02-en

7.3 Dissents

There were no dissents.

7.4 Withdrawals

There were no withdrawals.