4.6.1 Security and Stability

- *4.6.1.1 Explanation of the Subject*

  In the AGB there are three aspects of the Initial Evaluation that involve security considerations. The first is part of the string review and determines whether the applied-for gTLD string might adversely affect DNS security or stability. The second and third relate to the applicant review and determine:

  - Whether the applicant has the requisite technical, operational, and financial capability to operate a registry; and
  - Whether the registry services offered by the applicant might adversely affect DNS security or stability.

  DNS Stability

  According to the AGB:[1]

  > *The DNS Stability Review determines whether an applied-for gTLD string might cause instability to the DNS. In all cases, this will involve a review for conformance with technical and other requirements for gTLD strings (labels). In some exceptional cases, an extended review may be necessary to investigate possible technical stability problems with the applied-for gTLD string.*
  >
  > *Note: All applicants should recognize issues surrounding invalid TLD queries at the root level of the DNS.*
  >
  > *Any new TLD registry operator may experience unanticipated queries, and some TLDs may experience a non-trivial load of unanticipated queries. For more information, see the Security and Stability Advisory Committee (SSAC)'s report on this topic at http://www.icann.org/en/committees/security/sac045.pdf . Some publicly available statistics are also available at http://stats.l.root-servers.org/.*
  >
  > *ICANN will take steps to alert applicants of the issues raised in SAC045, and encourage the applicant to prepare to minimize the possibility of operational difficulties that would pose a stability or availability problem for its registrants and users. However, this notice is merely an advisory to applicants and is not part of the evaluation, unless the string raises significant security or stability issues as described in the following section.*

[1] See Module 2, 2.2.1.3 DNS Security Review, at https://newgtlds.icann.org/en/applicants/agb/evaluation-procedures-04jun12-en.pdf

Concerning the String Review Procedure the AGB states:

> *New gTLD labels must not adversely affect the security or stability of the DNS. During the Initial Evaluation period, ICANN will conduct a preliminary review on the set of applied-for gTLD strings to:*
>
> - *ensure that applied-for gTLD strings comply with the requirements provided in section 2.2.1.3.2, and*
> - *determine whether any strings raise significant security or stability issues that may require further review.*
>
> …
>
> *The panel will determine whether the string fails to comply with relevant standards or creates a condition that adversely affects the throughput, response time, consistency, or coherence of responses to Internet servers or end systems, and will report on its findings. If the panel determines that the string complies with relevant standards and does not create the conditions described above, the application will pass the DNS Stability review.*[2]

It was noted in the AGB that a string that complies with the technical requirements detailed in Section 2.2.1.3.2 String Requirements, largely enforced by the TLD Application System, would have a very low probability of requiring additional review,

In the event that the evaluation panel determines that the string does not comply, the application will not pass the Initial Evaluation, and no further reviews are available. In the case where a string is determined likely to cause security or stability problems in the DNS, the applicant will be notified as soon as the DNS Stability review is completed.

<u>Registry Services Review</u>

According to the AGB:

> *…ICANN will review the applicant's proposed registry services for any possible adverse impact on security or stability. The applicant will be required to provide a list of proposed registry services in its application.*

Section 2.2.3.1 in the AGB provides definitions of registry services, security, and stability as they relate to the Registry Services Review. Section 2.2.3.2 defines customary services and states that:

> *The applicant must describe whether any of these registry services are intended to be offered in a manner unique to the TLD.*

[2] Ibid

> *Any additional registry services that are unique to the proposed gTLD registry should be described in detail.*

The review methodology is as stated in 2.2.3.4 of the AGB:

> *Review of the applicant's proposed registry services will include a preliminary determination of whether any of the proposed registry services could raise significant security or stability issues and require additional consideration.*
>
> *If the preliminary determination reveals that there may be significant security or stability issues (as defined in subsection 2.2.3.1) surrounding a proposed service, the application will be flagged for an extended review by the Registry Services Technical Evaluation Panel (RSTEP), see http://www.icann.org/en/registries/rsep/rstep.html). This review, if applicable, will occur during the Extended Evaluation period (refer to Section 2.3).*
>
> *In the event that an application is flagged for extended review of one or more registry services, an additional fee to cover the cost of the extended review will be due from the applicant. Applicants will be advised of any additional fees due, which be received before the additional review.*

Technical/Operational Review

Again, according to the AGB:

> *In its application, the applicant will respond to a set of questions (see questions 24 – 44 in the Application Form) intended to gather information about the applicant's technical capabilities and its plans for operation of the proposed gTLD.*
>
> *Applicants are not required to have deployed an actual gTLD registry to pass the Technical/Operational review. It will be necessary, however, for an applicant to demonstrate a clear understanding and accomplishment of some groundwork toward the key technical and operational aspects of a gTLD registry operation.*
>
> *Subsequently, each applicant that passes the technical evaluation and all other steps will be required to complete a pre-delegation technical test prior to delegation of the new gTLD. Refer to Module 5, Transition to Delegation, for additional information.*

Pre-Delegation Testing

Once an applicant completes the evaluation portion of the process, there are several final steps remaining, including Pre-Delegation Testing, which is a pre-requisite to being delegated into the root zone. In section 5.2 of the AGB, it states the following regarding Pre-Delegation

Testing:

> *The purpose of the pre-delegation technical test is to verify that the applicant has met its commitment to establish registry operations in accordance with the technical and operational criteria described in Module 2.*
>
> *The test is also intended to indicate that the applicant can operate the gTLD in a stable and secure manner. All applicants will be tested on a pass/fail basis according to the requirements that follow.*
>
> *The test elements cover both the DNS server operational infrastructure and registry system operations. In many cases the applicant will perform the test elements as instructed and provide documentation of the results to ICANN to demonstrate satisfactory performance. At ICANN's discretion, aspects of the applicant's self-certification documentation can be audited either on-site at the services delivery point of the registry or elsewhere as determined by ICANN.*

- *4.6.1.2 Questions and Concerns Related to Subject*

In regards to the DNS Stability review, the expectation was that strings complying with the string requirements would have a very low probability of presenting a risk to the DNS, and the evaluation results bore out this expectation. However, challenges did exist, and a risk that was identified after program launch by the Security and Stability Advisory Committee (SSAC) via a report titled SAC 057: SSAC Advisory on Internal Name Certificates, noted the possible issue of "name collision" and provided suggestions on how the issue could be mitigated[3].

In August of 2014, ICANN published the Name Collision Occurrence Management Framework (see further discussion in section 4.6.3.1 below), intended to provide a long-term solution for all registry operators to mitigate the risk of name collision. The study Name Collision in the DNS[4] and the Name Collision Occurrence Management Framework[5] identified three high-risk strings (HOME, CORP, MAIL) that were applied for in this application round. However, before the Framework can be adopted for use in future application rounds, a process for identifying additional high-risk strings (which may not have been applied for in this round) should be developed and agreed upon.

Though only three high-risk strings were specifically identified to pose a significant risk to the DNS if delegated, other strings were noted to possibly pose a lesser risk. If policy development on Name Collisions is envisioned, collaboration with the SSAC is advised.

[3] Report available here: : https://www.icann.org/en/system/files/files/sac-057-en.pdf

[4] Interisle Consulting Group, LLC. (2 August 2013). Name Collision in the DNS. Retrieved from https://www.icann.org/en/system/files/files/name-collision-02aug13-en.pdf

[5] ICANN. (30 July 2014). Name Collision Occurrence Management Framework. Retrieved from https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf

From an operational perspective, the portion of the review that was most intensive related to IDNs was the DNS Stability review. Label Generation Rules for IDNs are in the process of being established and should be leveraged for the DNS Stability review in the future to reduce the amount of review required for IDNs.

Regarding the Registry Services Review, a high percentage of applications received a clarifying question, indicating perhaps that guidance provided to applicants could be improved. However, a vast number of applicants employed the services of a limited few RSPs, which may account for the high number of clarifying questions. The Registry Services Review could possibly be improved with knowledge that most applicants will use a RSP, allowing for efficiency gains, consistency. In addition, the potential creation of RSP accreditation program would also likely simply this review process without sacrificing the security and stability of DNS.

In regards to the Technical and Operational Capability Evaluation, it was designed to evaluate the applicants' knowledge and understanding of the criteria, as they were not required to have their infrastructure deployed for actual testing. With experience from the 2012 New gTLD Program round, with the majority of applicants engaging a RSP, the evaluation process could be structured differently, since infrastructure would likely be available and could actually be tested during evaluation, as opposed to during pre-delegation testing. Or, if an accreditation program was developed and deployed, the evaluation process could potentially be greatly simplified, again, without sacrificing the security and stability of the DNS.

In regard to Pre-Delegation Testing, the scope of testing may warrant analysis to ensure that applicants are tested for readiness on all requirements in their Registry Agreement, as well as any referenced technical specifications.

Finally, public comments identified the Emergency Back-end Registry Operator (EBERO) as an additional possible subject for consideration, where for instance, criteria for approving EBERO providers and the monitoring the EBERO's long-term ability to continue to meet those requirements could be examined, among other elements[6].

- *4.6.1.3 Relevant Guidance*
  - Principle D
  - Recommendation 4
  - Recommendation 7
  - Recommendation 18
- *4.6.1.4 Rationale for Policy Development*

[6] See full comment here: http://forum.icann.org/lists/comments-new-gtld-subsequent-prelim-31aug15/msg00000.html

The concerns identified regarding the DNS Stability Review, Registry Services Review, and Technical & Operational Capabilities Evaluation tended to be more in regards to operational efficiency as opposed to concerns about security and stability. As such, implementation guidance could be provided to streamline and optimize the evaluation processes, although the DG did not anticipate that policy development would be needed.

However, a PDP-WG could consider looking at security and stability beyond the more operationally focused analysis above and could investigate for instance, the impact on the DNS from delegating additional TLDs at a similar scale and pace as the 2012 round. If this topic is undertaken, collaboration with the SSAC is advisable.

In addition, it should be noted that ICANN staff is performing Security and Stability Reviews in support of the CCT and the findings from these reviews may be useful during possible PDP-WG deliberations[7].

[7] See: http://newgtlds.icann.org/en/reviews/ssr