The ISPCP thanks the Technical Study Group (TSG) for their work and the initial report on gTLD Integrations with Alternative Naming Systems.

Executive Summary

The report does not fully answer the fundamental question for which the TSG was established: what are the actual security and stability implications of integrating a DNS name with an alternative naming system, and what concrete mitigations are required?

The ISPCP is supportive of the technical work and the potential model but asks for a substantially stronger and more explicit risk-assessment and assurance framework before such integrations are approved and incorporated into contractual requirements.

The ISPCP therefore recommends that any approval of such integration be conditional upon clearly defined security and stability risk assessments, enforceable consistency and controller-assurance mechanisms, appropriate dispute and abuse safeguards, continuous monitoring, and mandatory continuity and turn-down provisions.

ISPCP's response to Public Comment

The ISPCP recalls according to the TSG's mandate https://www.icann.org/tsg/alternative-naming-systems-integrations

TSG was formed to study the implications of integrating a generic top-level domain (gTLD) name into the same name in an alternative naming system. A thorough assessment of the potential impact to the security and stability of the Domain Name System (DNS) must be conducted before ICANN can approve this new type of registry service.
[…]
ICANN has received an increasing number of inquiries from generic top-level domain (gTLD) registry operators and potential New gTLD Program
[…]
ICANN is convening this TSG to assess these risks and suggest appropriate mitigation controls if possible.
[...]

the report may "*serve as the basis for ICANN to develop standardized contractual language for registry agreements covering this Registry Service with the goal of undergoing Public Comment together with the TSG report*"

The report does not fully answer the fundamental question for which the TSG was established: what are the actual security and stability implications of integrating a DNS name with an alternative naming system, and what concrete mitigations are required?

In particular, the report provides a useful technical framework around the “same string + same controller” model and the Unified Source of Truth (USoT). These are useful foundations. However, the report spends considerably more effort describing how consistency between the systems could be achieved than assessing the consequences and risks if that consistency, security, availability or policy coherence is not maintained. The report itself recognises that the integrated name must not be able to “drift” between naming systems, but the actual risk assessment of such divergence remains relatively underdeveloped.

As a result, the report should move from identifying questions and possible mechanisms towards a clearer framework which:

- list out the risk
- identify the resulting impact
- develop the associated mitigation plan
- specify the conditions of assurance/acceptance of that plan

The ISPCP suggests the following to strengthen the final report based on this draft:

- The implications of divergence between the DNS-name and alt-name deserve much more explicit treatment, particularly where the two systems differ in resolution, state, availability, security properties or policy enforcement.
- “Same string + same controller” should be regarded as a necessary condition for integration, but not by itself as sufficient assurance that the integration is safe and secure.
- The report should more clearly address how ongoing consistency will be verified and enforced, rather than relying primarily on the assumption that the relevant controls will remain in place.
- The report should explicitly address the implications of relying on an “eventually-consistent” source of truth. A clear maximum convergence/consistency window, detection mechanism and fail-safe behaviour should be defined to ensure that temporary inconsistency between the DNS and alternative naming systems cannot create a security or stability risk.
- The issue of multiple alternative naming systems deserves more attention. The report acknowledges that more than one alternative system may be involved and also recognises that the complexity of proving the Unified Source of Truth increases as the number and diversity of naming systems increases.
- The thin-registry/controller-identity issue is important. Where the registry does not itself hold sufficient information about the controller, there needs to be a reliable mechanism to establish that the DNS-name and alt-name are controlled by the same entity.

- there should be some distinction between the responsibilities of the DNS registry, the alternative naming-system operator and the risks that become shared/systemic because of the integration.

Principle of developing contractual language through this TSG

Regarding principle of a development of "*standardized contractual language for registry agreements covering this Registry Service*", the ISPCP notes the use of normative terms such as MUST and RECOMMENDED that are intended to contribute to the development of standardized contractual language, it is important that any such requirements are clearly supported by the underlying risk assessment and go through the appropriate ICANN community and public-comment processes before being translated into contractual obligations.

Further the ISPCP notes that if these normative elements evolve towards contractual language and appreciates the need to have guidance prior to the closure of the New Round application period - and in this respect, this TSG may have been the only way to have such guidance. In this respect, the ISPCP is supportive of this approach. However, we would like to make the following observations:

- if the intent is that the normative text serves as "policy recommendations" to develop contractual language in the RA or RAA, it should be treated with the same rigour as if it had been developed by a PDP:
- it should be given as much visibility in the final report, and highlighted as "recommendations". The current presentation of these "recommendations" (assuming they are) in the report gives way to interpretation
- the report should record how much support these recommendations received during the group's deliberations
- ultimately the ICANN Board should be consulted for next steps once/if the report is approved

The ISPCP notes that by design, the TSG was not intended to be a representative group of the ICANN Community in the first place and with a report developed in only a few weeks, its conclusions may not be as robust as if it had been developed by a PDP WG. Again, the Constituency is supportive of the approach but since Alternative Naming Systems operators are not part of the ICANN community, their representation in a PDP effort may have been challenging, let alone the timeline. The ISPCP recalls their letter to the ICANN Board, to assess the need for broader involvement in the community to make it more reflective of the ecosystem that may have an interest in the development of gTLD policies in particular.

Comments on proposed recommendations

Regarding the recommendations reproduced in annex of this statement, the ISPCP offers the following comments on the "proposed recommendations":

1. Equivalent security, integrity and authenticity assurance MUST be required for every integrated alternative naming system, with the specific mechanism determined by the technology of that naming system. Where applicable, DNSSEC-equivalent assurance

should be used so that the security and authenticity guarantees are commensurate with those expected of the DNS.
2. URS/UDRP-equivalent dispute and abuse mechanisms MUST be addressed as a precondition for approval, rather than being left as an open question. The report itself identifies URS/UDRP, consumer protection and anti-abuse as issues requiring resolution.
3. The turn-down/EBERO gap should be elevated from RECOMMENDED to REQUIRED. The report acknowledges that alternative-naming integration may fall outside the current EBERO critical functions and therefore proposes a turn-down plan. In my view, continuity, controlled shutdown, transition/recovery and protection of registrants and relying parties should be mandatory conditions of approval.

The ISPCP further considers that there should be continuous conformance monitoring and auditability, not just an assessment at the time the registry service is approved. The security and stability properties of the integrated system need to remain demonstrably valid throughout its operational lifecycle. Such monitoring should also include defined thresholds, incident notification, remediation timelines and appropriate consequences where the integration no longer satisfies the required security, stability or controller-consistency criteria.

Overall, the ISPCP is unsure the string+controller model itself is necessarily unsafe. Rather, the report should make it clear that it is only acceptable where there are demonstrable, enforceable and continuously verifiable security, stability, policy, abuse-management and failure-management controls.

On the structure of the report, The report could present its findings more clearly by separating the identified risks, conclusions and proposed mitigations, rather than leaving some of the most important issues as questions for the reader.

Annex - excerpts of the report that contain normative text

p9 As a general matter, for string+controller integration, naming systems are integrated if and only if a name that is made up of the same string in each such system is always either controlled by the same controller or else withheld for the exclusive possible control by that same party. These two criteria MUST always be reliably satisfied for the naming systems to be integrated. If the criteria are not reliably satisfied, the naming systems are not integrated; and if the criteria cannot be reliably satisfied, then the naming systems and their associated namespaces SHALL NOT be treated as candidates for integration

p9 The Integrating TLD: the string MUST be the same and the controlling entity MUST be the registry operator of the TLD.

p9 Integration of Subordinate Names: .

- Assuming, then, that an operator does not prohibit integration of subordinate names, then the allocation of a name in any of the naming systems MUST either withhold or

allocate that same name in (all) the other system(s) as well, and only to the same controller.
- For string+controller integration, an enrolled name MUST be the same string in each relevant naming system

p10 The “Same Party” or Controller: the requirement for an identical controller of the identical string MUST be met

p11 Establishing Registry Control of Alternative Systems. it MUST be able to provide all relevant control guarantees over any alt-name corresponding to an integrated DNS-name such that the alt-name cannot drift from the DNS-name in terms of string or controller.

p12 Policy and Operating Convention: Coherence

- The registry applying to offer such a service MUST demonstrate that the alternative naming system does not itself represent a risk to the security or stability of the Internet.
- the mapping MUST provide means to ensure the object is related to a domain object in the EPP repository.
- Extensions to RDAP necessary to access the new data in the registry MUST be specified.
- RDAP extensions for use with alternative naming systems MUST be
- published and MUST be registered in the Internet Assigned Numbers Authority (IANA)
- RDAPExtensions registry as defined in RFC 7480 (Newton et al. 2015a). Re-use of extensions, including extensions not produced by the registry service applicant, is RECOMMENDED

p14 The Unified Source of Truth:

- Given the requirement that the different naming systems match on multiple criteria, the registry wishing to provide integration of different naming systems MUST ensure that there is one, eventually-consistent source of truth
- Every name in any of the underlying naming systems MUST be under common control (even if that control is distributed

p22 Considerations for When Integrated Registry Ceases - Following RequirementsUntil there is a substantial body of experience with integrations of the global DNS and other naming systems, a mandatory “turn-down plan” for discontinuing the integration is RECOMMENDED as part of the evaluation of the registry service.

Example.org Comes Under Some Kind of Administrative Deactivation in any naming system

- If a service is deactivated for external reasons (e.g. abuse, court order) in one naming system, the registry MUST disable the name, on the prudential principle that a danger to the Internet from a given name in one naming system is a danger in all naming systems (particularly if the naming systems are integrated)
- A clientHold status (from the registrar) SHOULD NOT entail the disabling of a name, since it can be used on purpose only to stop global DNS resolution on a domain for

some other reason. This is an example of an area where EPP extensions seem likely to be necessary to make management of integrated names easier. If a registrar is adding a clientHold to undertake disabling a name, it SHOULD place the clientHold for the same name in every naming system.

p35 **Name Hierarchy and Naming Systems** - At the same time, it is RECOMMENDED that a public suffix (Mozilla Foundation, n.d.) either maintain the integration lower in the tree or else disable integration for the domains in question