Comments of the Intellectual Property Constituency on the Initial Report of the Technical Study Group on gTLD Integrations with Alternative Naming Systems

The Intellectual Property Constituency ("IPC") of ICANN's Generic Names Supporting Organization ("GNSO") appreciates the opportunity to comment on the Initial Report of the Technical Study Group on gTLD Integrations with Alternative Naming Systems (the "Report").

We thank ICANN's executive leadership for considering these issues and consulting the community about the technical and policy challenges that will inevitably accompany integration.

The IPC represents the interests of intellectual property owners and online users who depend on the accuracy and security of domain names within ICANN's multistakeholder coordinated domain name system ("DNS"). We appreciate the Technical Study Group's work in identifying technical conditions for the integration of global DNS gTLDs into alternative naming systems as a registry service. We offer these comments to help guide future discussions on the policy and rights-protection questions that the Report expressly leaves for the community to resolve.

Summary

1. The Report should be treated as intended, which is as technical advice to ICANN org. Open policy questions should be properly addressed through a community process. Community work should be completed before any request for integration of any alternative naming systems into the global DNS is approved as a registry service.
2. The report rightfully points out that the architectures described are not equivalent for policy purposes. Only enrollment through the Shared Registration System is described as bringing alternative names under existing ICANN policy.
3. Same-controller parity is insufficient rights protection. An applicant should be required to demonstrate that UDRP decisions, URS determinations, and court orders can be given effect in every integrated system, and such obligations should be imposed on the contracted registry operator. Legacy allocations in an alternative naming system should not be enrolled into any integrated gTLD without proper rights-protection requirements in place.

Response to the Question Posed

ICANN asks whether the technical requirements proposed in the Report are sufficient to protect the security and stability of the DNS. The IPC presents the following for consideration:

1. The Report is Intended as Technical Advice Only. Policy Advice Rightfully Comes from the Community Policy Development Process.

The Report describes its own status accurately. It was "written primarily to provide advice to ICANN org in evaluating a proposed registry service when that service is presented for review" (§2). It leaves out "[p]olicy and competition matters in general, and appropriateness of any particular ICANN policy to a given naming system in particular" (§11).

Still, there is concern that parts of ICANN's multistakeholder community are already treating the Report as if it were the result of a formal policy process. That is not the case. The Report itself notes that bringing legacy alternative names into the global DNS has "policy implications needing to be discussed with the community that are beyond the scope of this report" (§8.3). It also admits, for at least one architecture it covers, that a "significant challenge for this mode of operation is to demonstrate that it can meet all ICANN contractual requirements and consensus policies" where alternative naming systems do not provide ICANN-required contact data, and "it is not immediately obvious how policies like Uniform Rapid Suspension might work or how the Uniform Dispute Resolution Policy can operate in the absence of standard contact data" (§9.3).

Those questions matter because the Report is going to shape how ICANN org evaluates individual requests under the Registry Services Evaluation Policy ("RSEP"). Technical advice has its place in informing an RSEP review, but it can't take the place of the policy development process, especially when a proposed service brings up difficult questions about rights protection, registration data, DNS abuse, consumer confusion, or the actual scope of consensus policies.

Accordingly, the Technical Study Group's final report should more explicitly state that it is technical advice to ICANN org, that it neither establishes policy nor creates a presumption that a proposed integration should be approved, and that the policy questions it identifies remain for the community to resolve. The policy questions it identifies still need to be handled by the community. ICANN org should not approve any request for a registry service touching on those deferred policy questions until the community, including the GNSO, the ALAC, the GAC, and affected stakeholders, has had an opportunity to properly resolve relevant policy considerations.

2. Architectures Are Not Equivalent for Policy and Rights-Protection Purposes

The Report describes two enrollment models for an integration of alternative naming systems with the global DNS, namely enrollment of alternative names through a single shared registration system or "SRS" (§5) and distributed enrollment (§6), and sketches three modes of operation (§9). The Report concludes that enrollment through the SRS is "likely the easiest and most

straightforward" way to integrate an alternative naming system "under the umbrella of any policy that would otherwise apply to global DNS names under prevailing ICANN policies" (§5). Yet, even that approach is qualified as the Report notes that enrollment through the SRS only "supports all the existing ICANN consensus policies and contractual requirements to whatever extent an operator's DNS-name registry operation and contract supports all of that" (§9.1). As referenced above, for the bearer-token model, the Report concedes that the operation of the URS and the UDRP is not immediately obvious (§9.3). For distributed enrollment and the alternative-system-primary model, the Report does not address whether ICANN policies and contractual requirements can be supported, presumably because such requirements are not technically feasible for those models.

The Technical Study Group's final report should acknowledge, as its own analysis implies, that whether ICANN consensus policies and rights-protection mechanisms apply to integrated names depends on the architecture chosen, and that any integration of the global DNS with alternative naming systems needs to further consider how such integration will support existing ICANN consensus policies and contractual requirements.

3. Enforceability of Rights-Protection Mechanisms Should Be a Condition of Eligibility

The Report already treats candidacy for integration as something that must be established by an applicant. For example, where the string-and-controller criteria cannot be reliably satisfied, the naming systems "SHALL NOT be treated as candidates for integration" (§4.1) (emphasis in original); an applicant must demonstrate that participating parties "cannot break the string+controller integration without the instruction or approval of the controller" (§6.3); and where the burden of complying with ICANN policy "appears too high, the TLD in question might not be a good candidate for string+controller integration" (§9.3). The Report, however, does not resolve how ICANN policy may actually apply to, and be enforceable against, the integrated alternative names or naming systems, nor how any conflicting parallel requirements would be handled.

Same-controller parity is important, but it is not sufficient. The more significant rights-protection questions are whether UDRP decisions, URS determinations, and applicable court orders can be implemented in practice across all integrated alternative naming systems.

An applicant proposing anything other than SRS enrollment with registry-held controller data should be required to demonstrate, rather than assert, at least the following**:**

- UDRP decisions, URS determinations, court orders, registry locks during pending proceedings, and registrar transfers can be implemented across every integrated system without the cooperation of the losing registrant.
- An identifiable party subject to enforceable obligations controls the technical point at which the foregoing remedies take effect.

- Registration data meeting the Registration Data Policy will be maintained for each integrated name and made available through the Registration Data Access Protocol ("RDAP") on the same terms as any other gTLD registration. An "opaque but durable identifier" or wallet address (§6.2) may supplement that data but should not replace it.
- The DNS abuse obligations of the ICANN Registry Agreement, including an abuse contact and reporting channel, extend to alternative names and alternative naming systems. The Report currently contains no express abuse-contact requirement, no reporting channel, and no mitigation step short of disabling a name.
- Any string operated by the alternative naming system that collides with an existing gTLD or with a well-known mark is identified before enrollment and addressed through an automated, deterministic mechanism that prevents consumer confusion and cross-system brand hijacking across both resolution paths.

Given the rationale above, now may be the right time to consider expanding the definition of DNS abuse to meet technical realities. It could be something along the lines suggested by INTA, "any activity that makes, or intends to make, use of domain names, the Domain Name System protocol, or any digital identifiers that are similar in form or function to domain names to carry out deceptive, malicious, or illegal activity."[1] Similarly, a new definition of DNS abuse could reflect recent policy adopted by the American Bar Association (at ABA2025A502), which supports the amendment of ICANN's definition of DNS abuse "to encompass any deceptive use of trademarks in relation to domain names, the Domain Name System protocol, or any digital identifiers similar in form or function to domain names."

We support the Report's statements that a name deactivated for abuse or under a court order in one system is a danger to and must be disabled in all naming systems (§8.5), and that "[s]uspensions MUST apply to all naming systems simultaneously" (§8.6) (emphasis in original). We recommend including that URS determinations, UDRP decisions, etc. are also triggers for cross-system action. The obligations to comply with such triggers should be non-waivable as consistent with ICANN's current policy.

4. Control Should Include the Ability to Transfer

Section 4.6 requires an applicant to show that an alternative-system name "cannot drift from the DNS-name in terms of string or controller," and at a minimum that the registry can "deny all other possible controls" over the name. This is helpful. However, the principal remedy under the UDRP (and court orders, if applicable) is transfer.

Section 4.6 should therefore require an applicant to demonstrate that the registry can, without the current controller's cooperation: (i) transfer control of the alternative-system name to a third

[1] See https://www.inta.org/wp-content/uploads/public-files/advocacy/board-resolutions/INTA-Board-Resolution-on-Domain-Name-System-Abuse-May-2023.pdf

party; (ii) suspend any access to or use of the alternative name pending the resolution of an abuse report or proceeding under an ICANN rights-protection policy or mechanism such as the UDRP; and/or (iii) delete or permanently disable the alternative name, at the option of the applicable complainant or if option (i) is not technically feasible. While transfer of the integrated name to the rights holder remains the primary and necessary remedy under the UDRP, if an alternative naming architecture makes technical transfer verifiably impossible, the applicant must demonstrate that the registry can permanently burn, lock, or un-bind the alternative allocation so it can never be re-registered, re-linked, or resolved again. Merely suspending DNS resolution while leaving the underlying alternative asset under the infringer's control is insufficient.

5. Legacy Allocations

Under the Report's allocation rule, allocation of a name in any integrated system "MUST either withhold or allocate that same name in (all) the other system(s) as well, and only to the same controller" (§4.3) (emphasis in original). Where an existing alternative naming system is integrated, its existing or legacy names "*must be enrolled* and therefore *must be at least withheld from the global DNS*" (§8.3) (emphasis in original). The Report recognizes that this "may have policy implications needing to be discussed with the community" (§8.3), and the IPC agrees that such policy implications need more in-depth community discussion.

The implementation of any recommendations in the Report without further ICANN community discussion will have regrettable consequences where a party already holding a name in the alternative system could obtain, or block, the matching DNS name even where that party never passed a Trademark Clearinghouse check, received no Claims notice, and was never subject to the UDRP or the URS. Such consequences are not acceptable to the IPC.

Integration of a namespace containing pre-existing allocations therefore should require: (i) a published inventory of the legacy allocations proposed for enrollment; (ii) controller data for each allocation meeting the Registration Data Policy; (iii) a Trademark Clearinghouse check; and (iv) a time-limited procedure allowing rights holders to challenge conflicting legacy allocations before enrollment and before the corresponding DNS name is withheld.