Comments of D3 Global, Inc.

on the Initial Report of the Technical Study Group on gTLD Integrations w/Alt Naming Systems

Introduction

D3 Global, Inc. ("D3") appreciates the opportunity to comment on the Initial Report of the Technical Study Group ("TSG") on gTLD Integrations with Alternative Naming Systems.

D3 is building infrastructure to help the domain ecosystem unlock new technical and commercial value. Its work includes practical onchain capabilities for registries and registrars, including through Doma Protocol, that provide greater programmability, transparency, interoperability and user control for existing DNS domains while keeping them anchored to the established DNS registration ecosystem. D3 also develops products intended to improve domain distribution, liquidity, monetization and growth.

D3 also brings the perspective of direct experience working with registries, registrars, registrants, blockchain networks, wallets and application developers. Few organizations have comparable end-to-end experience addressing the technical, operational and commercial issues considered by the TSG as does D3. These comments therefore reflect practical implementation experience, not merely a theoretical position about how DNS and onchain systems might interact.

D3 supports the TSG's central conclusion that appropriately designed integrations can operate without creating a material risk to DNS security or stability. A clear evaluation framework could reduce uncertainty, delays, expense and duplicative review for registry operators seeking approval of these services. The current draft, however, risks moving beyond technical evaluation and establishing policy, contractual and product architecture requirements that the TSG was not chartered to resolve and, in certain cases, concern activity outside ICANN's remit altogether.

In short, the final report should be limited to integrations affirmatively proposed and controlled by the RO, and should make clear that an independently operated same string system creates no claim on DNS inventory or rights against an RO or applicant. For integrations within scope, new names should be anchored to a DNS registration while preserving flexibility for registries and registrars to use technically sound EPP and tokenization models. Any mandatory condition should be limited to addressing a demonstrated, material risk to DNS security or stability, while questions involving registration data, RPMs, fees, allocation rules and other policy or contractual matters should be left to the appropriate process. Nothing in the report should apply retroactively to 2026 Round applicants.

1. Integration Can Create Significant Value for the Domain Ecosystem

D3 agrees that responsible integration between the DNS and onchain systems can be achieved securely and reliably.

Onchain capabilities can make domains more programmable, portable and useful. They can improve the transparency of domain transactions, facilitate distribution across new platforms, support new identity and payment functions, reduce transactional friction and enable entirely new products built around domain names. Registries and registrars can use these capabilities to reach new users, create new revenue streams and increase the utility of existing DNS registrations.

The DNS and onchain systems should not be treated as competing systems that require one to replace the other. Properly designed services can preserve the DNS as the globally coordinated naming system while using onchain infrastructure to add functionality around a DNS registration.

The TSG's work can help make such services easier to evaluate. A common technical baseline should reduce

repetitive RSTEP review and give registries and registrars greater confidence about the evidence expected from a proposed integration.

That baseline must remain narrow, objective and focused on outcomes. It should not dictate a single commercial model or implementation architecture.

2. The Final Report Must Clearly Define What Constitutes an Integration

The most important issue in the report is its scope. The report should apply only when an RO affirmatively proposes to integrate an alternative naming system as part of a Registry Service and can demonstrate sufficient control over that system to provide the required assurances.

The report itself recognizes that third parties can operate individual names, same string namespaces or alternative roots without the involvement of the corresponding RO. Such independent activity is not an integration by the RO and should remain outside the report.

An RO should not be required to identify, monitor, reconcile, reserve or withhold DNS names merely because an affiliated project, community initiative or unrelated third party operates a same string namespace elsewhere. Commercial or community proximity is not registry control, and string overlap alone is not integration.

There is no authoritative or finite universe of alternative naming systems that an RO could reasonably be expected to monitor. Anyone can create a blockchain contract or database that purports to issue identifiers under an existing or proposed TLD string. If those identifiers could create obligations for the corresponding RO, a third party could manufacture claims against DNS inventory at essentially no cost.

That would create an obvious opportunity for abuse. It could also impose defensive withholding, registration data, rights protection, transition or liability obligations on an RO that has no relationship with and no control over the third party system.

That would create an obvious opportunity for abuse. It could also impose defensive withholding, registration data, rights protection, transition or liability obligations on an RO that has no relationship with and no control over the third party system. The appropriate technical boundary is straightforward: an alternative system should be treated as part of an integration only when the RO has affirmatively included it in a proposed service and can demonstrate effective control over it. Otherwise, the system should have no bearing on the RO's contractual rights or obligations, potential liability, DNS inventory, application or delegation.

This limitation follows directly from the TSG's charter, which is confined to same name integrations affirmatively undertaken under RO control. ICANN may evaluate the elements of a proposed Registry Service that affect the DNS. An independently operated alternative naming system remains outside that inquiry and does not come within ICANN's remit merely because it uses the same string.

3. An Alt Name Should Not Create an Automatic Claim on a DNS Name

Several public comments have proposed that existing alt name holders receive priority, reservation or grandfathering rights in the corresponding DNS namespace, including where the future RO is unrelated to the alternative system. D3 strongly opposes that approach.

An alt name registration should not create a claim on the corresponding DNS name unless the alt name is tied to a valid DNS registration or the relevant RO voluntarily chooses to recognize it as part of an integration plan. Otherwise, an alternative system becomes a parallel mechanism for reserving DNS inventory outside the normal registration process.

Automatic recognition is also unworkable:

- Alternative namespaces are permissionless to create.
- More than one alternative system may issue the same string to different parties.

- Registration volume does not establish legitimacy or identify a unique claimant.
- A third party could create or populate a namespace specifically to burden a current RO or pending applicant.
- Alt name allocations may not have followed the applicable DNS launch, reserved name, registration data or rights protection requirements.
- An RO that does not control the system cannot provide the assurances required by the TSG's own model.

The fact that a system describes itself as established does not solve these problems. Age, volume, claimed economic value and community size may be relevant to an RO deciding whether and how to integrate that system, but they should not create rights against an unrelated registry or applicant.

Where an RO voluntarily proposes to integrate its own existing and populated alternative system, a service specific transition plan may be appropriate. That plan could address controller verification, conflicting allocations, applicable rights protection requirements and the treatment of names that cannot be verified. Those measures follow from the RO's choice to integrate that system. They should not become rights that alt name holders can assert against every future operator of the corresponding DNS string.

The final report should expressly reject any automatic entitlement to DNS delegation, registration, reservation or priority arising solely from an alt name registration.

4. New Integrated Names Should Be Anchored to a DNS Registration

Section 8.2 contemplates an alt name operating while the corresponding DNS name is withheld. Under the SRS model, the alt name is enrolled through the registry's SRS even though the registrant does not activate or use the DNS name. D3 does not believe that model should be required or treated as the default.

For new names issued through an integrated service, D3 supports a DNS first model: the DNS name is registered through existing registry and registrar channels, and an onchain identifier or token is issued after the DNS registration is created and verified. This approach:

- preserves the established registry > registrar > registrant structure;
- prevents an alt only registration from becoming a claim against DNS inventory;
- applies existing registration, payment and lifecycle processes before onchain functionality is enabled;
- provides a clear registrant of record;
- avoids reliance on an alternative root or parallel allocation or registration system;
- prevents the issuance of onchain identifiers for SLDs that cannot be registered in the DNS;
- supports existing registration data and rights protection obligations; and
- makes it easier to disable or modify the onchain functionality without disrupting the underlying DNS registration.

An RO may choose to reserve or withhold names when voluntarily integrating a preexisting alternative system. That decision should belong to the RO and should be evaluated as part of the specific integration proposal. It should not be an obligation created by the prior existence of an alt name.

At minimum, Section 8.2 should be identified as an optional architecture requiring separate policy and contractual analysis, rather than a mandatory consequence of the TSG framework.

5. The Framework Must Preserve Registry and Registrar Innovation

The final report should distinguish among at least three different types of service:

1. A Registry Service through which an RO integrates a TLD with an alternative naming system.
2. A registrar service that provides an onchain representation or tokenization of an existing DNS registration without requiring an RO operated alternative namespace.

3. An independent alternative namespace operated without the participation of the RO or registrar.

Only the first category is the subject of this TSG and RSEP framework. Registries should remain free to propose EPP based integration models. EPP and the existing SRS can provide a practical control point through which registration, renewal, transfer, expiration, suspension and other lifecycle events are coordinated. The report should recognize this as a viable model without requiring every RO to offer it.

Registrar innovation must also remain possible. Where an RO has not established an exclusive registry integration program, registrars should be able to offer tokenization or other onchain capabilities for DNS registrations, subject to their existing contracts and the requirement that the DNS and onchain representations remain appropriately coupled.

A registrar service that creates a token or onchain representation of an existing DNS registration does not necessarily create a second namespace. A token may instead operate as a credential, representation, profile or programmable asset associated with the DNS name. As the TSG charter recognizes, registrar services that are not Registry Services are outside the scope of this report.

The final report should therefore state that it does not prohibit, regulate or create new requirements for registrar level tokenization services that do not involve an RO operated alternative namespace.

6. A Wallet or Token Holder Is Not Necessarily the DNS Registrant

The report correctly recognizes that a wallet or opaque identifier may be used as evidence relevant to control. It should not assume, however, that possession or movement of a token necessarily establishes the registrant or controller of the DNS name.

A token can move between wallets or blockchain networks without changing the registrant of record. A token transfer may represent custody, bridging, an authorization, a pending transaction or a contractual transfer that remains subject to verification. The DNS registrant should remain the registrant unless and until the transfer is completed through the applicable registrar process.

An onchain transaction may initiate or provide evidence supporting a domain transfer, but it should not automatically override registrar verification, transfer restrictions, dispute proceedings, court orders or other requirements applicable to the DNS registration.

The relevant technical question is not simply which wallet holds a token at a particular moment. The question is which party is authorized to control the DNS name and any integrated name resolution functions, and how that authority is verified and enforced.

The final report should:

- distinguish registrant identity from wallets and technical credentials;
- permit registrars to retain the authoritative registrant relationship;
- permit registries to rely on an opaque and durable controller reference where appropriate;
- recognize pending and intermediate transaction states;
- require a defined reconciliation process for failed or incomplete transfers; and
- avoid requiring every token movement to produce an immediate DNS registrant change.

This is an area where outcome based requirements are substantially more appropriate than a mandated architecture.

7. The Report Should Not Turn Policy Questions into Technical Requirements

Section 11 excludes policy and competition matters generally, as well as the appropriateness of applying a particular ICANN policy to an alternative naming system. Section 8.3 also acknowledges that requiring existing alt names to be enrolled and withheld from the DNS has policy implications beyond the report's scope.

Despite those acknowledgments, other portions of the report appear to reach conclusions about:

- registration through the SRS;
- registrar involvement;
- application of all existing Consensus Policies to alt-only names;
- required RDAP extensions;
- Registration data collection;
- URS and UDRP;
- mandatory DNS withholding;
- fees and other cost consequences; and
- allocation and lifecycle requirements.

These are not purely technical conclusions.

The use of MUST, SHALL and other RFC 2119 terms does not give the report contractual force. The final report should explain that its normative terminology describes proposed technical evaluation criteria only. Any binding requirement must arise through the applicable Registry Agreement, an approved and agreed service specific amendment, Consensus Policy or another authorized ICANN process.

An individual RSEP approval may include binding conditions accepted by the relevant RO. That possibility makes it especially important that each condition be justified by the facts and risks of the proposed service. Repetition of the same condition in several Registry Agreement amendments should not cause it to become a generally applicable obligation without the appropriate community and contractual process.

8. Registration Data and Rights Protection Questions Remain Unresolved

The report does not specifically require use of RDRS for alt-only names. Under the SRS model, however, it requires RDAP extensions and says prevailing ICANN policies would apply even to integrated names that are not activated in the DNS.

The final report does not adequately establish:

- what alternative system data must be collected;
- whether that data constitutes DNS registration data;
- which party must collect or maintain it;
- what data must be published through RDAP;
- whether disclosure mechanisms apply;
- how data minimization and privacy requirements are addressed; or
- whether an onchain wallet address should be treated as registrant data, technical data or publicly observable ledger data.

A technical desire to query information does not itself establish a requirement to collect or publicly disclose it. Any registration data requirement should be necessary, proportionate and tied to a defined purpose.

The same applies to RPMs. Existing alt name registrations should not bypass or displace applicable DNS launch and rights protection requirements. At the same time, the TSG should not conclude that URS, UDRP or every other DNS policy automatically governs an identifier that is not a DNS registration. That is a policy question requiring separate analysis.

The final report should identify these matters as unresolved and avoid presenting them as technical requirements.

9. Technical Requirements Must Be Risk Based and Architecture Neutral

The stated purpose of the TSG is to determine whether a proposed service can operate without creating a material risk to DNS security or stability. For each mandatory requirement, the report should identify the specific risk, its

likelihood and materiality, how the requirement addresses it, and why a less burdensome alternative would not adequately address it.

The report's suggestion that RSEP stability may include broad legal or social considerations is inconsistent with the more specific definitions in the RSEP. Legal, consumer protection, competition and social questions may warrant consideration through other processes, but they should not be characterized as DNS stability issues without a clear connection to the operation of the DNS, registry data, delegation information or provisioning services.

A useful technical baseline could require an RO or applicant proposing an integration to address:

- effective RO control over the integrated alternative system;
- continued use of existing DNS registration and registrant control processes;
- prevention of a parallel registration or ownership system for the underlying DNS name;
- the relationship between the DNS registrant and relevant onchain credentials;
- prevention of conflicting allocation within the systems included in the integration;
- transaction finality, pending states and reconciliation;
- lifecycle events including expiration, transfer, suspension and deletion;
- detection and correction of unintended divergence;
- auditability and event logging;
- system failure and recovery; and
- a proportionate plan for discontinuing the integration.

These are appropriate subjects for technical evaluation. Registration priority, rights in inventory, mandatory disclosure and the legal effect of token transfers are not resolved merely by labeling them security or stability issues.

Within that technical baseline, the report should define measurable outcomes rather than prescribe one implementation. An RO or applicant should be permitted to demonstrate compliance through existing DNS registration and provisioning mechanisms, including an SRS using EPP, supplemented by an onchain usage layer, or through another technically sound architecture that preserves the DNS registration as authoritative. Control may be demonstrated through technical measures, contractual controls, cryptographic proofs or a combination, depending on the systems involved. The onchain layer may support coordinated use of the domain across DNS and onchain environments and add new functionality without creating a separate registration or ownership system or changing the provenance of the underlying DNS registration.

The report should not assume that an integration requires a single database or that every operation must originate in the same system. It should not equate the token holder with the registrant of record or require every transaction to settle instantaneously across every system. Nor should it assume that every blockchain event must modify DNS data, that every implementation requires the same EPP or RDAP extensions, or that the registry must duplicate personal information already maintained by the registrar.

The proper test is whether the proposed service provides reliable and auditable control of the integration and whether any temporary divergence is subject to clear limits and correction procedures without creating a material risk to the DNS.

11. The Report Must Not Retroactively Affect 2026 Round Applications

The Initial Report was published on 10 August 2026, two days before the 2026 Round application window closed. Applicants selected their strings, developed their operating models and submitted their applications without the benefit of a final TSG report or the contractual language ICANN has stated it will develop. The report should not retroactively create:

- new application requirements;
- additional string contention or objection rights;

- priority for holders in an unrelated alternative system;
- mandatory reservations or withholding;
- new evaluation criteria;
- grounds for delaying an application or delegation; or
- additional applicant representations concerning systems the applicant does not control.

Any applicant that proposes an integration may appropriately be required to explain that service and demonstrate that it can operate securely and stably. An applicant that does not propose such a service should not be affected by the existence of an unrelated same string system. The final report and any associated contractual language should make that distinction explicit.

Conclusion

D3 supports ICANN's effort to establish an efficient and predictable evaluation path for responsible integration services. DNS domains can gain substantial new utility through onchain programmability, interoperability and commercial innovation without compromising the integrity of the DNS.

The final framework will best encourage that innovation if it remains voluntary, narrow, architecture neutral and tied to demonstrated technical risks.

Most importantly, an independently created alternative namespace is not an integration undertaken by the RO and should remain outside this framework. Its existence should not impose obligations on an RO, encumber DNS inventory or affect a pending application. Integration must begin with an affirmative decision by the RO and demonstrable control over the systems included in the proposed service.

D3 urges the TSG to revise the report consistent with the recommendations above.

SUBMITTED BY:

D3 Global, Inc.
Inder Singh, Chief Technology Officer
Kevin M. Kreuser, Senior Vice President & General Counsel