PUBLIC COMMENT SUBMISSION

Initial Report of the TSG on gTLD Integrations with Alternative Naming Systems

Submitted by Unregistry | 21 September 2026

1. Where we stand

Unregistry builds integrations between web3 naming systems and the DNS, so the questions this Technical Study Group (TSG) was convened to examine are the questions we work on every day. We write from the perspective of end users and merchants rather than registry operations, and that perspective runs through everything below as we evaluate the framework by its effect on the people who actually use names.

Our overall position is supportive. The string+controller principle (Sections 2 and 4) answers the threshold question put to the TSG, and we agree that same-string integration can be carried out safely under it. The principle is demanding in the right way. The same string must be controlled by the same party in every system, at all times, in every state, or else set aside for that party's exclusive use; if that guarantee cannot be maintained, the result is not an integration but two names trading on the appearance of one. The report then does careful work translating the principle into registry-side requirements, including the name-state model (3.1), the requirements for registry control of the alternative system (4.6), and the lifecycle scenarios in Section 8.

Our principal observation is that the requirements are strongest where registries deal with one another and thinnest where end users interact with integrated names. Integration state is not required to be public. The user experience during synchronization failures is unspecified. Communication with registrants at lifecycle events is largely absent. Section 3 of this submission takes each of these in turn.

Finally, we develop a broader proposal in Section 6. In our view, a registrant should be able to associate a DNS domain with matching names on any web3 network of their choosing (any alternative naming system, in the report's terms) including with one network or several, existing providers or those yet to come, and without any requirement to own every name associated. This can be done with ordinary DNS records, under minimal registry requirements and entirely within the system that already exists.

2. What the report gets mostly right

2.1 Section 4.1: names are integrated if and only if the same string is always either controlled by the same controller in every integrated system, or else withheld for that controller's exclusive possible control; at the TLD itself, the controller must be the registry

operator (4.2). This is the only property that keeps a user's mental model of a name intact when multiple naming systems are running at once and the registry operator has chosen to integrate its own alternative services. The report acknowledges in 1.1 that users cannot be expected to tell naming systems apart; the principle means they do not have to.

2.2 It stays neutral on technology. Blockchain is treated as one subset of a broader class (6.4 covers thin registries generally), and both enrollment through the shared registration system (5) and distributed modes with a unified source of truth (6) are allowed.

2.3 The lifecycle work is thorough and it protects users. If a name is deactivated in one system, the registry must disable it in the other (8.5). Suspension applies everywhere at once (8.6). A name that is dangerous in one system is treated as dangerous in all of them. We support this, with the DNS as the anchor.

2.4 It is honest about its limits. Integration is not expected to survive EBERO (7.1). Overly burdensome process pushes activity into "shadow operation" (9.3). There is a clear out-of-scope list (11). That candor makes the report a reliable base for the contract and policy work that follows.

3. Transparency and verifiability

3.1 Make integration state public. Section 5 requires RDAP extensions for the alternative naming systems to be published and registered with IANA, and expects EPP extensions for provisioning. If that path is chosen, we suggest going further and exposing integration state itself through RDAP: which systems a name is integrated into, and its current state in each. Users, resolvers, registrars, and researchers could then check on their own that the DNS state and the alt-system state agree. Letting anyone verify this is one of the cheapest protections for user confidence available, and it directly answers 4.6's concern that controls be comprehensible to ordinary users.

3.2 Define what the user sees when sync fails. Section 6.1 requires the integrated systems to behave as one eventually consistent unified source of truth, and the worked example in 6.5 leans on optimistic locking, pending statuses, and failing or undoing conflicting writes. But the report says nothing about what the user experiences while states have not yet converged. The final report should require that divergence is detected within a defined window, that a maximum inconsistency period is tolerated, and that a fail-safe default exists. A name whose states cannot be reconciled should stop resolving everywhere rather than resolve differently in different places. A name that silently resolves differently in two systems is precisely the harm string+controller exists to prevent.

3.3 Disclose at enrollment, in plain language. Anyone enrolling an integrated name should be told where the name works and where it does not, what happens to the alt-system name on expiry, suspension, or deactivation (8), and that the integration ends if the service is discontinued or EBERO is invoked (7, see also 4.2 below). Registrants who understand what an integrated name actually does are the first line of protection for everyone they serve.

4. Lifecycle and abandoned integrations

4.1 Turn-down plans should be a MUST. Section 7 says a registry proposing an integrated service should develop a turn-down plan. The report's own cited research, including the 2026 study of abandoned integrations (Valapu et al., "Zombies in Alternate Realities"), documents real harm from "zombie" integrations. Make it a MUST, and define the minimum contents: notice to affected registrants, the post-integration state of names, communication channels, and timing.

4.2 Define the EBERO transition for users. Integration is not expected to survive EBERO (7.1). Registrants relying on alt-system functionality will therefore likely lose it, possibly abruptly, and possibly in contexts like wallet-linked names where silent failure has security consequences. The turn-down plan should address this directly, and enrollment should disclose up front that the alt-name's lifetime is bounded by the registry service's lifetime.

4.3 The 8.3 corollary needs its own policy discussion. Names already present in an alternative system when integration begins must be enrolled and at least withheld from the global DNS. Nothing in the framework obliges a registry to integrate any alternative system at all; a registry can equally create and manage its own alternative system, or launch on existing ones. The report flags that this has policy implications beyond its scope. We encourage ICANN to open that discussion promptly, with attention to the people holding names on existing alternative systems today: possible transition periods, communication obligations, and criteria for whether a name is enrolled, withheld, or excluded. These holders are also the group most likely to take up integrated DNS usage with alternative systems, and they carry the potential for new use cases for users and businesses. We see the intersection of DNS, web3 names, and e-commerce payments, for example sending 100 USDC to a verified example.com, as one such use case.

Web3 naming systems have sold millions of names over the years, including entire TLD strings, typically with no identity verification, no registrant data, and no trademark or dispute process of any kind. Any integration policy has to reckon with that reality rather

than reason as though integration starts from an empty system. It is a central reason we believe anchoring trust in the existing DNS is the correct path forward.

5. Abuse response and rights protection

5.1 Make enforcement follow the anchor. Section 10 asks, as one of its open issues, whether consumer-expectation protections such as URS and UDRP will work under integration, and if not how. Our answer is that enforcement should follow the anchor rather than be duplicated inside every system. An integrated or associated name with a live DNS name behind it already sits inside the full DNS accountability stack: registrant data at the registrar, UDRP and URS, court orders, and the report's own principle in 8.5 that a danger from a name in one system is a danger in all. Acting on the DNS name can propagate the effect: the association is withdrawn and the alt-name loses its proven association status. That reuses machinery that already works instead of building a parallel rights-protection mechanism inside every alternative naming system. The installed base described above cannot realistically be retrofitted unless holders link to a DNS domain, and even then enforcement operates through the DNS stack alone.

The narrow residual case is an active alt-name with no active DNS-name: the report's 8.2 scenario, and 8.4's expiry path. There, no DNS anchor exists to act on, so a minimum abuse-response floor does need to be set at the service: enough registrant and contact data for a complaint to be filed and enforced, cure and suspension semantics that carry across both systems the way 8.5 and 8.6 do, and restore-name mechanics after a decision. The accountable party is the registry operator, which sits inside ICANN's contractual system. Make the floor a requirement on any registry operator offering the service under an ICANN agreement and choosing to launch its own alternative integrations.

For the registrant-directed model in Section 6, no separate enforcement is needed at all, and that is a feature of the design. No association exists without a live DNS zone, and a DNS domain already carries the identity and dispute machinery. If the DNS name is lost, to expiry, a dispute decision, or a court order, the association dies with it: the records go with the zone, and even if a stale copy of them persists somewhere, the reciprocal control-proof no longer validates. The web3 name reverts to what it was before, a pseudonymous name on its own network, no more reachable than any name that was never linked. The proven association is the value, and keeping the DNS name in good standing is the price.

5.2 Spell out anti-abuse functionally. Section 10 also asks what anti-abuse regime covers alt-names, and whether it is enough. The answer should be functional rather than a label: receive reports, act within defined timeframes, and ensure that a name found abusive is disabled across all integrated systems, in anchored cases by acting on the DNS name and

letting the effect propagate (5.1), and in the residual case through the registry-operator floor.

5.3 Answer Section 10's DNSSEC question as a property. Section 10's first bullet asks, in effect, why DNSSEC isn't needed for the alt-name. The final report should answer by stating the property required, origin authentication and integrity of the alt system's records, and leaving the mechanism to the implementing system. That leaves each system free to meet the property its own way.

6. A registrant-directed, multi-network model (main suggestion)

6.1 The report's model is registry-bilateral. Sections 5 and 6 contemplate a registry operator integrating its TLD with an alternative system. SRS plugins or a unified source of truth, choice made at the registry level. 4.3 gives registries flexibility over subordinate-name rules, but whichever system is officially integrated is chosen for the whole TLD. A registrant gets whatever the registry's rule allows: no integration, integration by requirement, integration by permission, or integration by end-user choice. As the report is written, a registrant can only choose among the networks their registry has integrated, and a registrant under a non-integrating registry has no path the framework recognizes unless integration by end-user choice is developed.

6.2 Let registrants associate any matching name, on any network. The registrant publishes machine-readable records in their own DNS zone that associate the domain with matching or non-matching names on the web3 networks of their choice. The holder of example.com could associate the matching label on any web3 network where it exists, from any provider, today or in the future. One network, several, or all of them, changed at will, with no registry involvement.

Nor should they have to hold every asserted name themselves. DNS operators point their names at resources they do not own every day: MX records at a mail provider, CNAMEs at a hosting platform, TXT records for third-party verification. The association is the registrant's declaration, made in their own zone, pointing where they intend. A registrant could link names they hold across several networks, or point their domain at a name run by a service, platform, or party they have chosen to trust. Requiring unified ownership would exclude all of those legitimate uses, and would import to the second level the same exclusive-control rigidity the report reserves for the TLD level.

In record format terms, little is needed. Ordinary TXT records at reserved owner names in the existing zone. A dedicated RRType or a new w3n: ("web3-name") URI scheme could refine it later.

Why this deserves the TSG's attention:

- **User choice and portability.** The registrant picks the networks: one, several, or none, changed unilaterally. Nobody is locked into whatever their registry operator selected, even where an operator chooses to work officially with only some networks. Non-official integrations still work through the records.
- **Network-neutral competition.** Web3 networks compete for users on merit, not on which TLD-level deal a registry happened to negotiate.
- **Near-universal availability.** It works for ordinary domains under any gTLD, not just TLDs that completed integration, and no network has to clear its own costly evaluation before it can serve those users.
- **DNS-anchored authenticity, through DNSSEC.** The assertion lives in a zone the registrant already controls, and DNSSEC is what makes it trustworthy. In a signed zone, anyone can verify that the record was published by the registrant and was not altered in flight. That is a far better anchor than out-of-band claims on websites or social profiles. Other commenters in this proceeding have argued DNSSEC must not be optional for integrated registry services. We agree, and it applies here with equal force: for registrant-directed association, DNSSEC is the trust anchor.
- **Opt-in accountability.** A DNS domain comes with registrant data held at the registrar, and with established legal and dispute processes behind it. A holder who links a web3 name to their domain is, in effect, opting that name into their DNS identity: anyone relying on a proven association knows there is a reachable, answerable party behind it. For merchants and users who want verifiable counterparties, that is exactly the point. And it is voluntary: nobody who prefers pseudonymity has to link anything.

6.3 Use what DNS already has, and ask little of registries. The best version of this model is the one that needs the least new machinery. It runs entirely through the DNS as it exists today. TXT records at reserved owner names, using the same conventions that already carry SPF, DKIM, DMARC, and domain-verification records across the Internet. Nothing here requires a registry operator to change its systems, apply for anything, or take on a new obligation. That is a feature of the design, not a shortcut.

Three things follow:

- **Deployment does not wait on anyone.** A registrant with zone access can publish associations now, and resolvers, wallets, and other software can read them now. There is no TLD integration to approve first and no evaluation to clear.
- **One clarification would unlock all of this.** Registries have no role in registrant DNS records today, and it should stay that way: these records live in the registrant's

zone, managed by the registrant's DNS operator and not the registry. ICANN org should clarify that a TLD whose registrants publish such records is not thereby offering a new registry service, so this path does not trigger the evaluation the TSG framework reserves for TLD-level integration.

- **The security anchor is already deployed.** DNSSEC gives the records origin authentication and integrity. Associations in unsigned zones should be treated as unauthenticated, on the same fail-safe logic as our 3.2, where a claim whose origin cannot be checked is worse than no claim at all. Registrants and their DNS operators already sign zones, and registries already accept the DS records that anchor that signing in the parent zone.

A dedicated RRType, a w3n: scheme, or other URI schemes are worth standardizing (see our 6.7), but as an upgrade path, not a gate. The convention that wins will be the one people can use without friction.

6.4 How this relates to string+controller. Where the same party holds the DNS name and the asserted web3 name, this model delivers string+controller at the second level. Same string, same controller, verifiable from a signed DNS zone, across whatever networks the registrant names. Where the registrant points at a name held by someone else, the record is an assertion of association, not of identity. Still useful and legitimate, but a different kind of claim, and the format should make the difference visible (see our 6.5). Either way, no alternative name appears at a delegation point and no TLD-level control changes hands, so the top-level risks the report's requirements guard against, a TLD string drifting or its control splitting, do not arise.

The report's Section 2 defines its scope with four conditions: the operator operates the parent level; only that operator operates the alternative naming systems; names in the registry must integrate; and the name is always the same name in every system. A registrant-directed association is not that case. No registry operator operates the target networks, association is voluntary rather than required, and the DNS name and the web3 name remain different names even when the label matches. That is why it should need no registry service evaluation. The report also acknowledges, in a footnote, that alternative naming systems for individual DNS names already operate today without registry involvement, while noting they lack the global reach and scaling properties of the coordinated DNS. We agree, and that is the point: anchoring such a system to a DNSSEC-signed zone is exactly what gives it a verifiable, globally coherent handle. We are proposing the safe, verifiable version of what already happens informally.

The user-facing recommendations in our Sections 3 through 5 apply here too. A record pointing at an abandoned or transferred name is exactly the "zombie" pattern the report's cited lifecycle research identifies. Records should carry expiry or validation semantics, or

at least clear deletion guidance tied to domain lifecycle events, and resolvers should treat stale or unverifiable assertions as absent.

6.5 Proven vs declared associations. A record in a DNSSEC-signed zone proves the registrant published it. By itself, it does not prove they hold the asserted name on the target network. So support two clearly distinguishable classes. A proven association carries a reciprocal control-proof: challenge-response signature, on-chain verification, or the target network's own control-verification mechanism, in line with the domain-control-validation techniques the report itself points to in 9.3. A declared association is simply the registrant's published choice, no proof attached, and should be presented as such. A verified public association, whether proven through blockchain signing or otherwise, can carry its own market-developed benefits.

This is exactly why we do not support requiring ownership of every asserted name. Such a requirement bans legitimate uses, like pointing a domain at a name run by a chosen service, while giving users nothing they do not already get from the proven class. What users need is the ability to tell the two apart. A proven association answers "is example on this network the same party as example.com?" with a mechanical yes. A declared association answers a different question: "the registrant of example.com says this is where the name should point." Both are useful. Only verifiable truth about which is which keeps the mechanism from becoming an impersonation vector.

6.6 Precedence when several networks are associated. If a domain is associated with matching names on several networks at once, applications need deterministic precedence: an explicit order or priority field in the record format, not resolver heuristics. Without it, the same domain's associations get consumed in a different order in different software, which is the application-layer version of the divergence string+controller forbids at the registry layer.

6.7 Standardization. Record formats, any new RRType, and any w3n: URI scheme belong in the IETF. Established DNS practice for RRTypes and usage, RFC 7595 procedures for URI scheme registration. Several TSG members are authors of the IETF drafts the report cites, and we encourage the final report either to sketch such a convention or to recommend it as a separate standardization work item. Standardization should mature the format over time, not delay its use. One common standard matters here. If every web3 network invents its own ad hoc convention, the fragmentation lands on users and resolver developers, and none of the verifiability in our Section 3 ever materializes.

7. Scope and process

7.1 Bind only integrating registries. Registries that do not officially integrate or launch alternative systems, and their registrants, should see no change. Anything else imposes costs on users who get no benefit.

7.2 Do not over-prescribe, or you get shadow operation. 9.3 warns that burdensome process pushes integration activity outside any ICANN framework. In one form, that shadow already exists: the installed base described in our 4.3 operates entirely outside any ICANN process, including strings that match or resemble DNS TLDs. From an end-user perspective this is the strongest process argument in the document, as users are least protected where no requirements apply at all. Keep each requirement to the minimum needed for string+controller and lifecycle coherence, and make the evaluation criteria measurable and verifiable so applicants can predict outcomes.

7.3 Variant policy, symmetrically. We support 10.2 requiring IDN variant policies to be settled before integration. Add that the registry's registered variant set applies in both systems, and that variant states like blocked variants propagate to the alternative system. Without symmetry, confusable lookalikes kept out of the DNS come back in through the integrated alt system.

7.4 User-facing requirements need contractual hooks. Disclosure at enrollment, turn-down and EBERO communication, and the enforcement approach in our Section 5. These only have force if they land in the registry agreement. ICANN org has said contractual amendments will follow in a later proceeding. As they are drafted, carry these forward explicitly rather than leaving them as report-level guidance.

8. Universal Acceptance

The report does not directly address Universal Acceptance. Integrated names will be handled by software of widely varying capability, and an integrated name that is valid in the DNS but behaves inconsistently elsewhere invites exactly the confusion 1.1 identifies as grounds for caution. Integration guarantees coherence between naming systems, not uniform behavior of every piece of software that consumes names. Coordination with the UA community, plus the disclosure obligations in our 3.3, are the right mitigations.

9. Final Thoughts

The report answers the question it was asked, and answers it well. Same-string TLD integration can be safe. String+controller, plus the operational controls specified, is the

right foundation. Registry-side, the requirements are largely sufficient. The remaining work is user-side: transparency of integration state, bounded failure behavior, lifecycle and turn-down communication, rights enforcement that follows the anchor, and third-party verifiability.

Take up the registrant-directed model in Section 6 as a complementary work item. Not every connection between the DNS and web3 has to be negotiated at the TLD level. Let registrants publish associations in their own zones, through the DNS as it already works, under minimal registry requirements. That alone connects the DNS to every web3 naming network, existing or yet to come, one or many at a time, with names the registrant holds or names they have chosen to trust. And ICANN org can unlock it with a single clarification: that registrant-published association records are not a new registry service. It works within the existing system, and it meets users where they actually live.

Submitted,

Unregistry
Ageesen Sri
Strategy/R&D
a@unregistry.com