SuComments on the Initial Report of the Technical Study Group on gTLD Integrations with Alternative Naming Systems

By: Alfredo Calderon

I submit these comments as an individual Internet end user member of the At-Large Community.

I welcome the Technical Study Group's careful work and its central conclusion: integration of a gTLD with an alternative naming system may be technically feasible without unacceptable DNS security or stability consequences **only** where the identical string remains under the control of the identical party, throughout its lifecycle and across every integrated system. The report appropriately identifies this as "string+controller integration."[ppl-ai-file-upload.s3.amazonaws]

From an end-user perspective, this principle is necessary but not yet sufficient. The DNS succeeds in part because users generally expect a domain name to lead to a consistent, accountable, and predictable result. Integration must not create situations in which users, registrants, rights holders, security responders, or public-interest organizations cannot determine who controls a name, which system governs it, how abuse can be reported, or what happens when a domain is suspended, transferred, expires, or is subject to emergency registry transition.

I therefore recommend that ICANN approve this type of registry service only after the requirements below are made mandatory, objectively testable, and enforceable under the Registry Agreement and the RSEP process.

Support for core safeguards

I support the report's foundational requirements that:

- The gTLD string and the alternative-system string must be the same under clear technical comparison rules, including proper treatment of A-labels, U-labels, Unicode normalization, and label boundaries.[ppl-ai-file-upload.s3.amazonaws]
- The gTLD registry operator must retain effective control over the corresponding alternative-system name and prevent divergence in either the string or controller.[ppl-ai-file-upload.s3.amazonaws]
- A name allocated in one integrated system must be allocated to, or withheld exclusively for, the same controller in all other integrated systems.[ppl-ai-file-upload.s3.amazonaws]
- Registries using a distributed architecture must demonstrate a Unified Source of Truth that prevents inconsistent allocation or control across systems.[ppl-ai-file-upload.s3.amazonaws]
- A registry service applicant must demonstrate that the alternative system itself does not create security or stability risk.[ppl-ai-file-upload.s3.amazonaws]

These should be baseline requirements, not aspirational standards or matters addressed principally through confidential commercial assurances.

Required improvements

1. Prefer the DNS registry/SRS as primary

For initial deployments, ICANN should strongly prefer—and ordinarily require—a model in which the DNS registry's Shared Registration System is the authoritative transaction-control point. This model is more compatible with existing registrar workflows, EPP, RDAP, consensus-policy implementation, contractual compliance, auditability, and user expectations. The report itself observes that an alternative naming system being primary is more difficult because it does not naturally build on the familiar registry–registrar–registrant infrastructure while still needing to meet its obligations.[ppl-ai-file-upload.s3.amazonaws]

Highly decentralized or blockchain-centered approaches should not be approved merely because a conceptual Unified Source of Truth can be described. They should first demonstrate, in realistic production-like conditions, that the system can meet equivalent guarantees for lifecycle operations, rights-protection mechanisms, abuse response, data integrity, and registrant accountability.

2. Require independent, public technical assurance

Before launch, each proposed integration should undergo an independent security, stability, and interoperability assessment. At minimum, this assessment should include:

- A complete architecture and data-flow description, identifying every system, interface, privileged role, and dependency within the Unified Source of Truth.
- Threat modeling covering malicious insiders, compromised keys, registrar failure, blockchain or network forks, transaction finality delays, denial-of-service conditions, race conditions, and failures of synchronization.
- Evidence that an unauthorized party cannot create, transfer, reactivate, or retain control of the alternative-system counterpart of an integrated DNS name.
- Public test results for registration, renewal, expiry, transfer, registrant changes, suspension, abuse action, dispute action, restoration, registry failure, and system partition.
- Periodic independent audits after launch, with non-sensitive findings published.

The report correctly recognizes that a distributed model can become considerably more complex and that the complexity of proving consistency rises as more disparate naming systems are added. Therefore, the burden of proof should rise with the number, heterogeneity, and decentralization of participating systems.[ppl-ai-file-upload.s3.amazonaws]

3. Make lifecycle parity mandatory

The current report gives useful operational scenarios, but ICANN should translate them into mandatory lifecycle requirements and measurable service-level commitments.

An integrated name must have predictable, synchronized treatment for:

- Initial allocation and activation.
- Renewal and expiry.
- Redemption, restoration, and deletion.
- Registrant changes and registrar transfers.
- Suspension, deactivation, and reactivation.
- Court orders, dispute-resolution outcomes, and abuse-related actions.
- Registry termination, insolvency, or emergency transition.

The report recognizes that a DNS name may expire while an alt-name remains active, with the DNS name merely withheld. While technically coherent under the proposed model, this outcome is potentially confusing for ordinary users. A user who sees the same string may reasonably assume that it has a common operational status and common accountability across systems.[ppl-ai-file-upload.s3.amazonaws]

ICANN should therefore require clear user-facing disclosure whenever the DNS and alternative-system instances have different activation or resolution status. It should also assess whether continuing an alt-name after expiration of its DNS counterpart creates consumer-confusion, fraud, or rights-protection risks that demand additional restrictions.

4. Preserve abuse response and accountability

Integrated alternative names must not become a path for evading DNS abuse mitigation, law-enforcement cooperation, incident response, or existing public-interest obligations.

The report asks the right questions: What integrity assurance is provided for lookup data? Does the alternative system provide an adequate anti-abuse regime? Who can be contacted when it is a source of malicious Internet activity? And how will UDRP or URS function if an alt-name is active without standard registrant data?[ppl-ai-file-upload.s3.amazonaws]

These questions should become explicit approval conditions. Every integration proposal should provide:

- A clearly identified, continuously available abuse contact.
- An abuse reporting channel that is accessible to users and security researchers.
- Published response-time commitments and escalation paths.
- Equivalent or stronger procedures for malware, phishing, fraud, child-safety harms, botnets, and other harmful activity.
- The technical capability to take timely action across all integrated systems where necessary to protect users and the Internet.
- A documented process for applying UDRP, URS, court orders, and other applicable rights-protection outcomes.

The registry should remain fully accountable even when technical components or data are operated by registrars, wallet providers, smart-contract systems, registry service providers, or other third parties.

5. Require meaningful transparency for users

The report recognizes that users may already find DNS hierarchy and policy relationships difficult to understand, and that operating multiple naming systems makes these distinctions even less apparent. This human-factor risk deserves more prominence.[ppl-ai-file-upload.s3.amazonaws]

Users should not have to understand resolver configuration, wallets, blockchain settlement, or naming-system architecture in order to know what a name means. ICANN should require registries and registrars to provide clear, accessible disclosures that explain:

- Whether a name is integrated with an alternative naming system.
- Which systems are included.
- Whether the name resolves differently depending on the user's software, resolver, browser, wallet, or application.
- The current operational status of the DNS-name and each integrated alt-name.
- How to report abuse or seek support.
- What happens on expiry, transfer, suspension, or dispute.
- Whether personal information, wallet identifiers, or other persistent identifiers are processed and shared.

These disclosures should be plain-language, multilingual, and accessible. They should be available to registrants before purchase and to Internet users through a public lookup mechanism.

6. Strengthen RDAP and public data requirements

The report appropriately states that necessary RDAP extensions must be specified, published, and registered in the IANA RDAP Extensions registry. I support this requirement, but recommend that ICANN go further.[ppl-ai-file-upload.s3.amazonaws]

A public RDAP response, subject to applicable privacy law and redaction requirements, should disclose:

- That the name is integrated.
- The relevant alternative naming system or systems.
- A stable integration identifier.
- Current status in each system, such as active, withheld, suspended, disabled, or pending.
- The authoritative abuse contact.
- The registry operator responsible for the integration.
- A reference to applicable policies and the approved turn-down plan.

This transparency is essential for security researchers, consumer-protection organizations, incident responders, and end users. It should not require proprietary tools or access to a blockchain explorer.

7. Treat thin-registry arrangements cautiously

The report identifies an important gap: in a thin registry, the registry may not possess the information necessary to technically verify that the DNS-name and alt-name have the same controller at all times. It may depend on the registrar and contractual compliance, and may not learn of internal registrant changes.[ppl-ai-file-upload.s3.amazonaws]

For this new category of registry service, contractual assurances alone should not be enough. ICANN should require a durable, privacy-preserving, cryptographically verifiable controller identifier that is available to the registry for each integrated name and is maintained through all lifecycle events. The registry need not retain unnecessary personal data, but it must have sufficient evidence to enforce the same-controller requirement and to audit compliance.

If an operator cannot provide such proof, it should not be eligible to offer integration under the string+controller model.

8. Treat IDNs and variants as high risk

The report properly notes that IDN variants and Label Generation Rules must be processed before integration, and cautions against using multiple normalization forms simultaneously.[ppl-ai-file-upload.s3.amazonaws]

I recommend that ICANN initially restrict approval of integration involving IDNs, scripts with variant-management requirements, or names prone to visual confusion unless the applicant can show rigorous compliance with applicable IDN tables, variant policies, normalization rules, and user-protection measures. This should include robust testing for confusable strings, A-label/U-label equivalence, cross-script spoofing, and inconsistent rendering in browsers, wallets, applications, and alternative-system interfaces.

The risk is not merely technical inconsistency; it is user deception and loss of trust.

Emergency and exit safeguards

The report recommends a mandatory “turn-down plan,” especially because alternative-system integration may fall outside the critical functions covered by EBERO. I strongly support making this mandatory, but a plan is not enough unless it is tested and enforceable.[ppl-ai-file-upload.s3.amazonaws]

Each application should include a public, independently tested continuity and exit plan that specifies:

- The trigger conditions for suspension or termination of integration.
- How the registry will preserve the DNS service if the alternative system fails.
- How names will be safely disabled, withheld, migrated, or delinked.
- How registrants and users will be notified.
- How historical records and evidentiary data will be retained.
- Who bears operational and financial responsibility.

- How ICANN can direct or execute the plan if the registry fails, becomes insolvent, or becomes non-compliant.

Registrants should not lose their DNS names, suffer an involuntary transfer of control, or face a surprise change in the meaning or availability of their names because an alternative system fails.

Conclusion

I support continued work on narrowly defined string+controller integration, but only under a precautionary, evidence-based framework. The proposed requirements are a strong technical starting point; however, they should be supplemented by mandatory independent testing, lifecycle parity, transparent RDAP disclosures, enforceable abuse and rights-protection mechanisms, privacy-preserving proof of controller identity, strict IDN safeguards, and tested emergency exit procedures.

The primary test should be simple from an end-user perspective: integration must not make an Internet identifier less predictable, less accountable, less secure, or harder to remedy when something goes wrong. The technical design must serve that public-interest outcome, not merely establish that synchronization is theoretically possible.