India's comments on ICANN TSG Initial Report: gTLD Integrations with Alternative Naming Systems

The ICANN Technical Study Group's Initial Report (referred to below as *the Report*) examines whether a gTLD registry should be permitted to integrate a DNS-name to the identically-named identifier in an alternative, non-DNS naming system for example, a blockchain-based naming system.

The Report's central proposal is ***"same string+same controller integration"*: the same text string must remain linked to the same controlling party across every integrated system, at all times**. The TSG considers this model potentially workable from a security and stability perspective, provided that appropriate operational controls are in place, however the **report has not clearly identified these controls and their implementation/enforcement.**

The Report is written as technical advice to ICANN org for its evaluation of any resulting Registry Services Evaluation Policy (RSEP) application; **it does not resolve the policy, competition or institutional questions that adopting this model raises at scale**.

India's overall approach is not to object to alternative naming technology, or to prescribe any particular architecture. India's interest is in making sure that the broad assurances in the Report are turned into conditions that ICANN can actually check before, not after, a Registry Service is approved.

Section	Comment	Rationale
Section 4.6 — Establishing Registry Control of Alternative Systems	India supports the TSG's requirement that the registry operator maintain effective control over the corresponding name in the alternative naming system. To make this requirement easier to verify and apply consistently, India recommends that the final framework require the applicant to submit a standard, technology-neutral **control-assurance document before activation.** This document	The TSG establishes the correct same-controller invariant but leaves the evaluation method architecture-dependent. That flexibility can become a verification gap when the report is used for standardised Registry Services Evaluation Policy (RSEP) treatment. A common outcome-based evidence dossier would allow ICANN to verify the required security outcomes without

	should identify all possible ways through which the name or its controller can be changed, the persons or systems authorised to make such changes, key privileged roles, and any material third-party dependencies. The applicant should also demonstrate, through **independent testing**, that unauthorised changes cannot alter the name or controller. Where **cryptographic mechanisms** are used, the evidence should cover **key custody, rotation, revocation and recovery in case of compromise**. The control should be **re-validated periodically** and following any material change to the system	prescribing a database, blockchain, identity system or consensus mechanism.
Section 6.1 — The Unified Source of Truth	India recommends that the **final framework clearly define the states for operations** involving string allocation, controller identity and activation, including pending, committed, failed and rollback states, along with clear rules for moving between these states. It should also define a measurable and objectively justified maximum unresolved period for completing such operations. Changes affecting the same string and controller should be	These safeguards would prevent conflicting controller or allocation states across integrated naming systems, protect the "string+controller" invariant, and reduce risks from synchronization failures.

	atomic across integrated naming systems, so that either all systems recognise the change or none treats it as final. Where consistency cannot be verified, further changes should be temporarily frozen (fail-safe lockout) until the correct state is confirmed and consistency is restored.	
Section 7 — Registry Ceases Following Requirements	India recommends that the turn-down plan, currently recommended in Section 7, be made mandatory pre tested requirements for Registry Services Evaluation Policy (RSEP). The plan should demonstrate that integration can be safely discontinued without disrupting critical DNS functions, creating controller ambiguity, unintended reallocation, or stranded alternative representations. The plan should define clear triggers, designated initiating authorities responsibilities and exit procedures, and should be tested before launch and periodically thereafter, including following material architecture changes.	Because Emergency Back-end Registry Operator *(EBERO)* protocols cannot maintain non-DNS alternative systems, registry failure risks leaving integrated names active indefinitely in secondary namespaces without ICANN technical oversight or abuse controls.

Section 8 — Registration, Allocation and Operational Scenarios	India recommends that Section 8 establish clear and deterministic transaction procedures for lifecycle operations such as domain and registrant transfers. Where operations involve multiple naming systems or external registration data, the framework should define coordinated transaction processing, cross-system locking during transfers, and clear rollback procedures where an associated update fails.	Asynchronous updates across independent settlement layers invite timing attacks and race conditions. If a DNS transfer completes while the corresponding alt-name transfer fails or lags, control of the string is fractured between two different entities

8.4 Registrant Uses example.org as a DNS-name and alt-name; DNS-name is Permitted to Expire	India recommends that where a DNS-name expires while the corresponding name in any Alternative Naming System (ANS) remains active, the DNS-name should not be reallocated to another controller. Until clear safeguards are established to ensure continuity of the same-controller relationship, the corresponding names should expire across both the DNS and relevant ANS(s)	Clarification on this would help establish how **string+controller integration is preserved throughout the lifecycle of the name**, including when the DNS-name is no longer active but the alt-name remains operational.

Section 10 — Additional Security and Stability Considerations	India recommends that Section 10 move beyond open-ended questions and establish objective, evidence-based acceptance criteria for integrated Registry Services. Applicants should be required to provide specific evidence, including independent security/cryptographic audits, network failure and load stress testing, and documented anti-abuse Service Level Agreements (SLAs). The framework should also define clear pass/fail thresholds and stop-work criteria requiring integration to be paused where defined security or stability requirements are not met.	An inquiry-based framework creates subjective, unpredictable RSEP reviews. Without explicit technical benchmarks, applicants cannot know what constitutes sufficient proof of safety, and ICANN evaluators lack objective grounds to deny or require specific mitigations for high-risk integrations.