Stockholm 2026-09-21

Internet Corporation for Assigned Names and Numbers
Technical Study Group on gTLD Integrations with Alternative Naming Systems

In response to: Technical Study Group on gTLD Integrations with Alternative Naming Systems
Our ref: 26-030

Netnod welcomes the opportunity to provide feedback on the Initial Report of the Technical Study Group on gTLD Integrations with Alternative Naming Systems, published 10 August 2026 by the Internet Corporation for Assigned Names and Numbers.

ICANN asks whether the technical requirements proposed in the report are sufficient to protect the security and stability of the DNS. Netnod's answer begins from a distinction the report does not draw. The requirements govern the **allocation** of names; they do not govern their **resolution**. The report itself grounds ICANN's role in "the need for uniform or coordinated resolution in the unique identifiers of the Internet" (section 1), and then specifies control equivalence — that a string is allocated to, or withheld for, the same controlling entity in every integrated naming system — without requiring that a query for that string return the same answer in each of them, or that the querying party be able to determine which system answered.

Read that way, the requirements are a competent and necessary treatment of the question the TSG was asked, and Netnod supports the string+controller model as a floor. They are not **sufficient on their own** — not because the engineering is wrong, but because they secure only one of the two properties that make a name mean a single thing on a single Internet. Netnod recommends nine additions before the model is relied upon in Registry Services Evaluation Policy determinations.

Netnod submits the following comments.

Fredrik Lindeberg, PhD
Chief Information Security Officer

Tel: +46-76 511 32 72
Email: flindeberg@netnod.se

Netnod AB
Greta Garbos väg 13
169 40 Solna
Sweden

Attachment 1 - Detailed comments

1. Netnod's role and the broader context

Netnod is a Swedish Internet infrastructure operator. Netnod operates Internet exchange points in Sweden, one of the world's thirteen DNS root server identities (i-root), authoritative DNS services, and national time distribution on behalf of the Swedish Post and Telecom Authority.

Netnod is neither a gTLD registry operator nor an ICANN accredited registrar, and has no commercial interest in whether any particular integration is approved. Netnod's interest is in the property that makes the Internet a single network: that a name resolves to the same thing for everyone, everywhere. Netnod has argued this consistently, including in its responses to the Root Server System Governance Structure document (2025) and the RIR Governance Document v2 (2025), and in its response to the European Commission's targeted consultation on Internet governance (2025).

That last response deserves a correction here, in the interest of candour. In January 2025 Netnod assessed that blockchain-based alternative naming systems had no effect at the infrastructure level. Netnod maintains that assessment for alternative naming systems operating alongside the global DNS. It does not hold for the mechanism this report describes. String+controller integration is the first mechanism Netnod is aware of that gives an alternative naming system a position inside the delegated DNS hierarchy, under a name that end users will read as an ordinary domain name. That is a change in kind, not in degree, and it is the reason Netnod is commenting at all.

Netnod offers the comments below as an operator of DNS infrastructure rather than as a registry, a registrar or a rights holder: from the position of a party that answers queries and must be relied upon to answer them consistently.

2. The report secures allocation but not resolution

Netnod agrees with the framing in the report's own section 1, quoted above: what ICANN coordinates is uniform or coordinated *resolution*. The technical requirements that follow it are requirements on allocation and control.

The string+controller model guarantees that a name is allocated to, or withheld for, the same controlling entity in every integrated naming system. It does not guarantee that a query for that name returns the same answer in every system, nor that the querying party can determine which system answered. The report does not discuss resolution consistency, and it does not reference RFC 2826 or the requirement for a unique namespace with a common root.

This matters because uniqueness of allocation and uniqueness of resolution are different properties, and it is the second one that users, applications and dependent infrastructure rely on. Two systems may agree perfectly on who controls example.tld and still return different

addresses for it. Nothing in the report prevents that, and nothing in the report requires it to be visible.

Netnod recommends that the report state explicitly that string+controller integration delivers control equivalence and not resolution equivalence, and that this distinction be carried into any RSEP determination that relies on the model. Netnod further recommends that the report note that representing an integrated name to end users as a single name with a single meaning is a claim the technical requirements do not support.

3. Divergence must be detectable and disclosed, and convergence must be bounded

Section 6.1 requires a unified source of truth that is eventually consistent, and states that where such a USoT genuinely underlies all registrations “there is no logical possibility that … matching strings could end up allocated or reserved to different entities in different naming systems”. Netnod accepts the logic and notes its scope: it holds for the converged state. Eventual consistency is precisely the admission that the system passes through states that are not yet converged. The report acknowledges pending states and settlement delays in the underlying systems but sets no maximum convergence time, and imposes no obligation to detect divergence during that window or to disclose it when it occurs.

Same-controller is also a property that holds at a point in time. The report addresses expiry (8.4), transfer (8.8) and administrative suspension (8.5–8.6), but does not address bankruptcy, loss of cryptographic keys, or the case it raises itself and leaves open — a legal authority compelling a change in one system that cannot be effected in the other. In each of those cases the integration does not fail loudly; it fails silently, and the failure state is precisely the one the model exists to prevent: matching strings under different controllers in different systems.

The Emergency Back-End Registry Operator (EBERO) mechanism addresses the disorderly exit for DNS-only registries: if a registry operator fails, ICANN can transfer DNS operations to an EBERO. The report observes (Section 7.1) that integration with an alternative naming system "appears to fall outside the category of 'critical registry functions,'" which it suggests means integration cannot survive EBERO operation. Netnod notes that the report does not state what operational state the integration is expected to reach during an EBERO period, nor how registrants in both systems are to be protected while normal registry operations are suspended. This is the disorderly exit the report’s turn-down plan does not cover.
Netnod recommends four additions:

1. A published, bounded maximum convergence time per integration, declared in the RSEP application and monitorable from outside.
2. A requirement that the registry operator be able to detect divergence and that divergence be disclosed, on a defined timescale, to ICANN and to affected registrants.

3. That the report treat divergence as an incident to be reported by its consequence rather than by a threshold metric — consistent with how availability incidents are handled elsewhere — while still requiring that a bound exist and be published.
4. That the turn-down plan be REQUIRED rather than RECOMMENDED, and tested before launch; and that the report state what operational state an integration is expected to reach if the registry operator fails, and what protections apply to registrants in both naming systems during that period. Netnod does not suggest that EBERO be extended to operate an alternative naming system.

4. The withheld-name mechanism displaces DNS registrations

The string+controller model requires that a name registered in one integrated naming system be withheld in every other integrated system. Netnod observes that this mechanism has an asymmetric effect the report does not address at the allocation level.

Where an alternative naming system registration predates or is created independently of a DNS registration attempt, the withheld-name state prevents DNS registration of the same name by any party, including parties with an established right to that name. The report acknowledges this in Section 8.3, noting that such cases present “policy implications” that are “beyond the scope” of the initial report.

Netnod notes that at scale this effect is significant before integration begins. ICANN's own Office of the Chief Technology Officer recorded in April 2022 (OCTO-034 Section 2.3.3, Challenges with Alternative Name Systems) that individual blockchain-based naming systems already held registrations at scale: over 800,000 names on ENS and over 2,100,000 on Unstoppable Domains as of 28 March 2022, and over 3,500,000 registered over time on Handshake as of February 2022, of which ICANN notes some 115,000 were reported to be in use. A string+controller integration applied to any such system would withhold all pre-existing registrations from DNS on the first day of integration, as a structural consequence of the model rather than as the outcome of any individual registration decision.

Netnod takes no position on whether a pre-existing registration in an alternative naming system should confer any claim in the global DNS, and notes that several commenters have argued forcefully that it should not. The point here is narrower: the string+controller model produces the displacement as a structural consequence, and the report identifies no framework under which the resulting competing claims are to be resolved. Netnod's concern is the absence of the framework, not the outcome it would produce.

Netnod recommends that the Final Report address the displacement effect explicitly, including the question of which rights framework governs when a pre-existing alternative naming system registration prevents DNS registration of a name to which a third party holds a legitimate claim, and whether the RSEP is the appropriate venue for that determination.

5. The collision detection framework does not cover alternative naming systems

ICANN's 2026 Round Applicant Guidebook (Module 7.7) implements a name collision risk framework based on DNS traffic data: root server logs, DNS recursive server logs, and Identifier Technologies Health Indicators (ITHI) data sets. This framework identifies strings whose use in private namespaces causes leakage into the public DNS; it identified .corp, .home, and .mail as high-risk strings in the 2012 round.

Netnod observes that this framework does not detect collision risk arising from blockchain-based alternative naming systems. Blockchain names resolve via their native protocol and generate no signal in DNS root server logs. ICANN's own SSAC made the same observation in July 2025 (SAC130, Recommendation 3), recommending that the Technical Review Team be authorised to evaluate potential collisions with known, widely used alternative naming systems. Recommendation 3 has not been implemented in the current Applicant Guidebook (V2-2026.04.24).

Netnod recommends that the Final Report note this gap and recommend that ICANN update the collision detection framework to cover alternative naming system registrations before any integration of that type is evaluated under the RSEP.

6. Control should be demonstrated cryptographically

Section 4.6 permits an operator to demonstrate exclusive control either by documenting every interface and its access controls, or by proving that changes cannot be processed without an authorisation the operator alone holds. These are not equivalent forms of evidence. Interface documentation is a description of a configuration at a moment in time; it ages, it is not independently verifiable, and it does not survive a change the operator did not intend. Cryptographic proof of exclusive authorisation is a property of the system rather than a statement about it.

Netnod's general position is that requirements should be written as verifiable functional requirements rather than as process artefacts. Applied here, that means the cryptographic demonstration should be the requirement, with interface documentation available only where the target system genuinely offers no cryptographic control point — and in that case the residual risk should be stated in the RSEP application rather than absorbed into it.

As Netnod argued in its response on the RIR Governance Document, it is vital that an external observer can understand and to a lesser extent verify the mechanisms being relied upon. The same applies here.

Netnod notes that other commenters in this proceeding have questioned whether Section 4.6 reaches beyond the point of integration into the operation of the alternative naming system. Netnod shares the concern about scope and suggests that it argues for the cryptographic demonstration rather than against it. Documenting every change interface and

its access controls requires an account of how the alternative system is operated; proving that no change can be processed without an authorisation the registry operator holds requires nothing about how it is operated at all. The cryptographic route is the less intrusive of the two, as well as the more verifiable.

7. Integration couples systems that were previously independent

The report observes that operating many disparate naming systems “appears to increase the risk to the overall integration due to complexity”, and places no limit on the number of alternative systems a TLD may integrate with, noting that a name might exist in 1..n such systems. Section 6.1 states the coupling directly: “None of the naming systems can be truly fully independent of one another because they all rely on the USoT for their data.”

Netnod would put the point more strongly. Resilience in distributed systems comes from nodes that fail independently. A unified source of truth spanning n naming systems is a shared dependency deliberately introduced across systems that previously had none — a single point of failure reintroduced at the coordination layer. This holds irrespective of whether the unified source of truth is implemented centrally or in a distributed fashion. It is not an argument that the coordination problem requires an adversarial-consensus treatment; it is the observation that scoping the arrangement to a single controlling entity is precisely what makes the failure correlated rather than diversified. This is the standard caveat on diversity arguments: common provisioning or control systems undo the independence that made diversity valuable. It applies with full force to a USoT.

Netnod recommends that each RSEP application for an integration be required to analyse its unified source of truth explicitly as a single point of failure, and that adding an nth naming system to an existing integration be treated as a new registry service requiring its own evaluation rather than as an extension of an approved one.

8. Partition behaviour is unspecified

Section 10 asks what potential there is for "a network split that leaves some of the naming systems partly isolated," and what to do about it. The report puts the question to prospective applicants and does not answer it. The SSAC has asked (SAC134) that failure, delay, partition or loss of consensus in an alternative naming system not impair the DNS registry's own operations. Netnod supports that, and addresses the further question the report puts: what each integrated system should do while partitioned, and how they reconcile on recovery.

The global DNS has a well-understood answer. Authoritative data continues to be served from the last published state; resolvers cache; TTLs bound how stale an answer can be; anycast means a partition removes instances rather than the service. The root server system is served by thirteen identities and their backing organisations, with the failure independence that implies. The design intent is that partitioned operation degrades predictably, and that a stale answer is bounded in time rather than indistinguishable from a current one.

An integrated naming system has no equivalent specified behaviour, and the two classes of system do not degrade alike. Under partition a unified source of truth is by construction unavailable to at least one side, and eventual consistency gives no guidance on what each side should do in the meantime: continue to answer from local state, decline to answer, or answer while indicating that the state may be stale. Each choice has a different failure mode and the choice is presently left to the implementer. Integration therefore couples systems whose partition behaviour is not merely different but unspecified on one side.

Netnod recommends that each RSEP application be required to state the intended behaviour of every integrated naming system under partition — whether names continue to resolve, whether allocation and transfer operations continue to be accepted, and how the systems reconcile on recovery without allowing an assertion of control that has aged out to survive it.

9. DNSSEC creates an asymmetry the report does not resolve

A gTLD zone in the global DNS must be signed with DNSSEC, and the operator must maintain a DNSSEC practices statement. The report notes that these obligations are DNS-specific. There is no equivalent requirement on the alternative system side.
An integrated name therefore has validatable provenance in one naming system and, potentially, none in the other, while presenting to the user as one name. Netnod does not suggest that ICANN impose DNSSEC on systems outside its remit — that would be neither possible nor appropriate. Netnod does recommend that the report record the asymmetry, and that where it exists the integration not be represented as delivering equivalent assurance.

10. Dispute resolution outcomes create states the integration model does not address

Standard ICANN dispute resolution mechanisms — the UDRP, the URS, and registry-initiated abuse suspension — are designed to produce outcomes that modify or terminate domain name registrations. Netnod observes that several of these outcomes, when applied to an integrated name, produce a state that the string+controller model does not contemplate.

Transfer. A UDRP transfer moves a DNS registration from one party to another. Where the corresponding alternative naming system registration is held on a permissionless blockchain, ownership is determined by possession of a private cryptographic key; no mechanism available to the registry or to ICANN can effect a transfer of that key. The integration is therefore left, after a concluded UDRP proceeding, in the state the string+controller model exists to prevent: the same name under different controllers in different systems, with no stated path to convergence.

Cancellation. A UDRP cancellation deletes a DNS registration and returns the name to the available pool. Where the corresponding blockchain registration persists — as it will in any system without an operator-controlled removal mechanism — the withheld-name logic of the string+controller model applies: the name remains unavailable for DNS registration by any party, including the complainant whose cancellation request was upheld.

Suspension and abuse mitigation. A URS suspension or a registry-initiated abuse suspension removes a name from active DNS resolution. A blockchain registration of the same name continues to resolve via the alternative system's mechanism. Netnod notes that integration gives the alternative resolution path a formally recognised position within the name's infrastructure, which is a different situation from an entirely external circumvention of a DNS-only suspension.

Expiry. DNS registrations expire upon non-renewal. Several major blockchain-based naming systems operate without a renewal obligation or on materially different renewal timelines. A name whose DNS registration has lapsed, and that is nominally available for re-registration, may remain withheld under the string+controller model for as long as the blockchain registration persists, which in some systems is indefinite.

These are not edge cases; they are the normal operation of mechanisms ICANN requires all registry operators to support. Netnod recommends that the Final Report note that the string+controller model does not specify a convergence path following any of these outcomes, and that this be addressed before integrations of this type are approved under the RSEP.

11. What Netnod does not ask for

Netnod does not ask ICANN to prohibit alternative naming systems, to regulate them, or to treat their existence as a threat to be managed. Nor does Netnod ask that these questions be referred to national regulators or legislators. Actors and functions pertaining to Internet names and the technical coordination required to operate them should be held accountable by structures within the multistakeholder framework. The TSG's work is an example of that framework doing what it should, and Netnod's recommendations are offered as strengthening it rather than as objections to it.

Netnod also notes, so that its own standing is not overstated, that nothing in the report affects the root zone or the operation of the root server system. The report does not discuss them, and Netnod does not claim that it should. The risks Netnod identifies arise at the TLD level and below.

12. Concluding remarks

Netnod supports the TSG's technical requirements as a necessary minimum and agrees that they should not be weakened. Netnod recommends that the Final Report add the following:

1. An explicit statement that string+controller integration delivers control equivalence and not resolution equivalence, with the consequence that integrated names should not be represented to end users as having a single unambiguous meaning.
2. A published, bounded maximum convergence time per integration, together with an obligation to detect and disclose divergence, and a turn-down plan that is REQUIRED

and tested rather than RECOMMENDED, stating what operational state an integration reaches if the registry operator fails.

3. Cryptographic demonstration of exclusive control as the requirement rather than as one of two options.
4. A requirement that each integration analyse its unified source of truth as a single point of failure, and that each additional naming system require a separate registry service evaluation.
5. An acknowledgement of the DNSSEC provenance asymmetry between the global DNS and integrated alternative systems.
6. An explicit treatment of the withheld-name displacement effect, including the rights framework that applies when a pre-existing alternative naming system registration prevents DNS registration of a name to which a third party holds a legitimate claim.
7. A recommendation that ICANN update the collision detection framework in the Applicant Guidebook to cover alternative naming system registrations, as recommended by SSAC SAC130 Recommendation 3.
8. A statement that the string+controller model does not specify a convergence path following standard UDRP, URS, abuse suspension, or expiry outcomes, and that this be resolved before integrations of this type are approved under the RSEP.
9. A requirement that each RSEP application state the intended behaviour of every integrated naming system under network partition, and the reconciliation path on recovery.