11 Collyer Quay
No. 17-11, The Arcade
Singapore 049317

Public Comment of ENS Labs, Ltd.

Re: Name Collision Procedure Documentation
New gTLD Program: 2026 Round

Submitted by: Alexander Urbelis, General Counsel & CISO, ENS Labs, Ltd.
Date: March 16, 2026
Proceeding: Name Collision Procedure Documentation (Opened January 29, 2026)

Introduction

ENS Labs, Ltd. (ENS) is submitting this public comment on the Name Collision Procedure Documentation for the New gTLD Program: 2026 Round. ENS – developer of the Ethereum Name Service (.eth), the first large-scale Web3 domain platform, operating since 2017 with approximately 1.6 million active registrations – has been a consistent participant in the ICANN community, commenting on the Applicant Guidebook proceedings and the DNS Abuse Mitigation Policy Development Process, among others.

ENS supports ICP-3 and the single authoritative DNS root. It does not seek preferential treatment for .eth and has committed not to create additional TLDs outside ICANN. ENS has created bridges between blockchain naming and the DNS through DNSSEC verification, CCIP-Read, and partnerships with DNS registries and registrars.

On the topic of name collision, we have been very pleased to see that ICANN has made significant progress: implementing NCAP Study 2, earning SSAC's endorsement in SAC130, launching the Name Collision Observatory ("NCO"), and forming the Technical Review Team ("TRT"). These are meaningful steps toward safeguarding the DNS in the 2026 round.

However, the Procedure Documentation has a critical gap. It defines name collision correctly: "a resource name that is intended to be resolved in one naming system is inadvertently resolved in a different naming system." That definition covers collisions between the DNS and alternative naming systems. But the 2026 procedures focus almost entirely on traditional private-namespace collisions. They apply methods developed for intranet leaks: the accidental query leakage that flagged .corp, .home, and .mail as high-risk in 2012. The main risk in this round is different: alternative naming systems have sold registrations under dozens of TLD strings now expected to appear as new gTLDs. These are not misconfigured routers; they are commercial systems with millions of registrations.

This comment identifies the specific procedural gaps, proposes concrete and implementable remedies, and urges ICANN to complete its own framework before the Application Submission Period opens. What worked for detecting intranet leakage will not work for detecting millions of active registrations in a parallel namespace. The procedures need to account for that reality before the application window opens, and this comment seeks to offer a practical path to do so.

I. Two Models of Web3-DNS Integration

For the first time, operators of blockchain-based and other alternative naming systems will participate as gTLD applicants. They should. The question is whether the Name Collision framework can assess the distinct collision risks they bring.

Two models have emerged since the 2012 round:

Model 1: Responsible Integration

Model 1 assumes operators will respect the DNS root, and build technical bridges (DNSSEC, gateway resolution) that cooperate with the DNS rather than run parallel to it. They commit to the strings they operate over a period of years. They do not create new TLDs outside ICANN. They apply in the 2026 round as standard applicants, on the same terms as everyone else.

Model 2: "Create First, Claim Later"

Model 2 operators launch dozens of TLD strings outside the DNS in rapid succession, sell registrations under them, then apply for a subset as gTLDs, bringing their parallel namespace into the DNS after the fact. The result is a collision scenario that was not accidental but was the foreseeable consequence of launching a parallel namespace and selling registrations under it.

The collision risk under Model 1 is manageable. Existing strings can be evaluated, bridges assessed, and reservation through proper channels minimizes confusion. Model 2 is categorically different. The applicant has already sold potentially hundreds of thousands of names under a string that, if delegated in the DNS, would resolve to entirely different resources depending on which naming system a user's device or browser queries. The collision is not a hypothetical from root server log analysis. It is an existing condition the applicant created.

ICANN's Office of the Chief Technology Officer has recognized this risk. OCTO-034 (April 2022) found that when alternative naming systems use strings that overlap with DNS TLDs, "name collisions must be expected" and "software defects and misconfigurations will likely result in names leaking from one system to another." The Procedure Documentation has not developed operational procedures to act on this finding.

This is not a theoretical risk. Name collisions between alternative naming systems and ICANN-delegated TLDs have already occurred. The Handshake naming system auctioned TLD strings including .music, .kids, .hotel, and .亚马逊 (xn--jlq480n2rg). ICANN subsequently delegated .music to DotMusic Limited and .亚马逊 to Amazon. The Handshake registrations under those strings remain active; the conflicts are unresolved. As one Handshake core developer stated publicly: "Handshake is, by design, on a collision course with ICANN." (See https://github.com/handshake-org/hs-names/issues/6#issuecomment-628658791.) These are not edge cases. They are the first documented instances of the collision scenario the 2026 procedures must be designed to address, and the current framework had no mechanism to prevent or mitigate them.

The policy implications extend beyond any single applicant. If the Name Collision framework permits an operator to accumulate registrations outside the DNS and then leverage that installed base as evidence of demand in a gTLD application, it creates a rational incentive for every prospective applicant to do the same. The logical endpoint is a race to establish fait accompli: any entity considering a 2026 round application would be better served by launching its desired string immediately, collecting as many registrations as possible, and presenting the result to ICANN as a market reality requiring accommodation. If this strategy is not discouraged by the framework, the rational course for every prospective applicant — ENS included — would be to adopt it. ENS has chosen not to operate this way. But the framework should not rely on voluntary restraint.

II. The Lifecycle of Speculative Namespace Creation

The "create first, claim later" model is not hypothetical. During approximately eighteen months, one operator launched 70+ TLD strings outside the DNS, sold registrations under each, then abandoned most of them. It issued refunds through a web form and pursued ICANN applications for a fraction of the surviving strings.

This lifecycle generates collision risk at every stage, including stages the current framework does not contemplate.

Stage 1 – Mass Creation: Dozens of TLD strings are launched in rapid succession, not through years of protocol development, but as commercial offerings sold as domains people can buy and own.

Stage 2 – Commercial Sale: Registrations are sold under each string as blockchain tokens, entirely outside the ICANN ecosystem. Brand owners may find their marks registered by third parties in a blockchain namespace, and later discover this predates and complicates their ability to secure the same name in the DNS.

Stage 3 – Abandonment: The operator finds most strings aren't commercially viable and aren't worth the $227,000 ICANN application fee; high-risk strings can cost $377,000+. Most are abandoned. Registrants were refunded via a web form; no public harm assessment or remediation process has been disclosed beyond the fee refund.

Stage 4 – Selective Application: The operator applies to ICANN for the subset of strings with the largest user bases or commercial potential, using the existing registrations as evidence of demand.

This lifecycle creates several distinct name collision risks that the Procedure Documentation does not address:

- *Orphaned collision risk.* When an operator lets a TLD string go, on-chain registrations remain active permanently. If a different applicant later applies for the same string, those orphaned registrations create collision risk that neither the original operator nor the new applicant has the ability or incentive to mitigate. The TRT has no documented process to detect or evaluate orphaned registrations.

- *Surviving-string collision risk.* For strings the operator does apply for, the TRT must assess a pre-existing namespace built without coordination with the DNS and without the phased delegation approach the ICANN framework envisions. This is not a latent risk to be discovered through log analysis. It is a known, quantifiable condition.

The framework should be capable of identifying and assessing these risks. It is not.

III. The Quantitative Data Gap

The NCO tool, root server logs, and recursive resolver data referenced in AGB Section 6.7.2 are essential for name collision assessment. But they do not account for strings with extensive pre-existing registrations in alternative naming systems.

Alternative naming systems resolve via blockchain smart contracts, peer-to-peer networks, or browser extensions, bypassing DNS entirely. ENS names, for example, resolve via Ethereum smart contracts (CCIP-Read) or integrated applications, not the DNS root. The same is true for blockchain TLDs like .wallet, .crypto, .nft, .blockchain, and .agent.

A string may show moderate magnitude in the NCO tool – residual query leakage from browsers that attempt DNS resolution before falling back to alternative resolvers – while carrying enormous actual collision risk from hundreds of thousands of registrations the NCO cannot see.

Consider: an operator has sold over one million registrations under a single TLD string. People access them through browser extensions, dedicated apps, or wallets. Those resolution paths never generate DNS queries. If the same string is delegated as a gTLD, every device without the alternative resolver will resolve it through the DNS, to an entirely different destination.

The magnitude data would have caught only the leakage, not the installed base that creates the collision. NCAP Study 2 itself recognized this problem from the opposite direction: Recommendation 8.1 states that ICANN should not reject a TLD solely based on the volume of name collisions, because volume alone does not tell the full story of risk.

The same logic applies here. A string with low DNS magnitude but hundreds of thousands of alternative namespace registrations presents real collision risk that volume-based metrics will miss.

The TRT's quantitative data miss an important class of collision risk. Without supplemental data sources, it lacks the ability to evaluate it. The SSAC has identified this same gap: SAC130 Recommendation 3 urges that the AGB explicitly authorize the TRT to evaluate potential collisions with "known, widely used alternative naming systems and other external sources," finding that constraining the TRT to DNS query data alone prevents it from identifying collisions of this type.

The data gap is not a future concern; it is a present limitation that will affect every application involving a string already in use outside the DNS.

IV. The Qualitative Evidence Gap

AGB Section 6.7.2 says the Initial Assessment will consider "qualitative evidence that can help deduce the severity of harm" alongside quantitative data. Good. But the Procedure Documentation gives no examples of what qualitative evidence will be gathered, how it will be weighted, or what sources the TRT will use.

Section 6.7.2 lists specific quantitative sources – "root server logs, and DNS recursive server logs" – but omits examples of qualitative evidence entirely. In the Final AGB Proceeding (May–July 2025), commenters asked for those examples to be provided before the application window. ENS agrees.

This is not just a transparency problem. Without defined qualitative sources, the TRT lacks the tools to assess collision risk from alternative naming systems. ICANN should enumerate the following as qualitative evidence for the Initial Assessment:

1. Pre-existing registrations: approximate number and how long they have been active.
2. Active users: how many people currently resolve names through alternative resolution for the string.
3. Applicant involvement: whether the applicant or its affiliates operate an alternative naming system using the string, which creates a distinct risk profile.
4. Browser and app integration: native browser support, resolution extensions, or middleware that resolve the string outside the DNS.
5. Consumer confusion history: documented cases of misdirected traffic, phishing, or asset loss between DNS and alternative resolution.
6. Technical resolution path: whether the system uses DNS query interception, browser extensions, smart contract resolution, or other mechanisms, each carrying different collision risk.
7. Applicant track record: strings previously launched, strings abandoned, and what happened to registrants. An operator that launched and abandoned dozens of TLD strings presents a materially different risk profile than one that has maintained a single string for years.

These are knowable, verifiable data points directly relevant to collision risk. Enumerating them gives the TRT clear authority to gather this evidence and puts applicants on notice that their alternative naming system activities will be part of the assessment.

V. The Asymmetric Risk Problem

Traditional name collision is a coordination problem. Organizations using private namespaces (.corp in Active Directory, for instance) did not intend to create collision risk. The risk emerged when the DNS root expanded into previously undelegated space. The harm was accidental, the actors diffuse, and the mitigation (controlled interruption, magnitude monitoring) was designed for that reality.

Model 2 collision risk is a strategic problem. The parallel namespace was created deliberately, registrations were sold commercially, and the installed base is now presented as a market reality ICANN must accommodate. When the entity that created the collision is also the entity applying for the DNS string, the risk becomes asymmetric:

- Information asymmetry. The applicant knows its full registration count, resolution architecture, and user base. The TRT does not. The Procedure Documentation does not require disclosure.
- Competing incentives. A large alternative namespace strengthens the commercial case for the application but increases the collision risk the TRT must evaluate. The framework does not account for this tension.
- Self-created collision. Unlike traditional collisions discovered through passive observation, these are the direct consequence of the applicant's commercial decisions. The framework should account for that.

This does not mean alternative naming system operators should be disqualified. Their participation through the ICANN process is a positive development, preferable to continued operation outside the governance framework. But the framework must be able to assess the collision risk that arises when an applicant has already sold registrations under the string it seeks to operate in the DNS.

VI. Public Trust, Consumer Protection, and Program Integrity

These collision risks are technical, but they carry consequences for public trust, consumer protection, and the integrity of ICANN's new gTLD program.

Consumer Harm from Speculative Namespace Practices

People who buy a domain name, DNS or otherwise, expect it to work as an identifier over time. They do not treat domains as speculative instruments. The average buyer of a blockchain domain expects it to resolve, to be an identity, and to have permanence.

Mass creation and abandonment of TLD strings contradicts those expectations. Registrants under abandoned strings were left with non-functional identifiers. In documented cases, the only remedy was a fee refund through a web form: no disclosed harm assessment, no apparent accounting for reliance interests like branding, wallet associations, published links, or professional identities.

This is not just a commercial dispute. It directly affects the collision assessment. Registrants who don't claim refunds, or aren't aware refunds exist, keep blockchain registrations that pose ongoing collision risk. Those registrations exist on-chain whether or not the operator supports them. The TRT must account for this residual installed base, even where the operator has walked away.

Declining Public Confidence in Domain Names

A core reason for ICANN's governance framework is to keep the Domain Name System trustworthy, stable, and predictable. Registry Agreements include continuity safeguards. EBERO procedures

protect registrants if a registry operator fails. These structures distinguish the DNS from an unregulated namespace.

When 2026 round applicants have a documented history of launching TLD strings without these protections and then abandoning them, the questions go beyond technical collision risk. ICANN must consider the reputational and trust implications of delegating DNS strings to operators whose track record includes the mass creation and disposal of namespaces. To be clear: this concern isn't about alternative naming systems existing, or a protocol developing a single string over time as part of its core infrastructure. The concern is with a specific practice: the quick, commercial creation of dozens of TLDs outside any governance framework, abandoning most of them, then applying to bring a curated subset into the DNS. That practice, regardless of the operator, presents both a technical collision risk and a trust risk the Procedure Documentation should address.

VII. TRT Capacity and Methodology

SAC130 recommended that ICANN "clarify the TRT's ability to adapt to future name collision challenges." ENS strongly endorses this and urges ICANN to act before the application window opens.

The appearance of large-scale alternative naming systems with millions of registrations is exactly the "emerging challenge" SAC130 contemplated. The TRT's current toolkit (root server logs, recursive resolver data, NCO magnitude scores) was built for a threat landscape without commercial alternative naming systems. The TRT requires both authority and funding to evaluate the collision risks these systems pose. SAC130 Recommendation 4 makes this point directly: the AGB should state that while the TRT may utilize the four NCAP2 data collection methods, it is authorized to evolve its testing and analysis framework to address new and unforeseen sources of data. ENS agrees, and urges ICANN to act on this recommendation before the application window opens.

ENS recommends:

- Add experts who understand alternative naming systems, blockchain resolution, and major operators' technical architectures. The TRT cannot assess what it does not understand.
- Publish the TRT's assessment methodology before the application window so applicants and the public know how alternative naming system data will factor into the Initial Assessment.
- Set up a data collection process that requires applicants to self-report and that adds independent verification steps.

The 2026 round will be the first in which applicants bring pre-existing namespaces with millions of registrations into the ICANN process. That is not a speculative scenario; applications are being prepared now. If the TRT enters the assessment period without the authority, expertise, or data sources to evaluate collision risk from alternative naming systems, the framework will produce assessments that are technically incomplete. Incomplete assessments will either clear applications that carry unaddressed collision risk or generate challenges that the "clearly erroneous" standard makes difficult to sustain. Neither outcome serves the program or the public interest.

VIII. Concrete Recommendations

ENS submits the following recommendations:

Recommendation 1: Amend AGB Section 6.7.2 to list qualitative evidence types.

Specify concrete evidence: existing alternative-name registrations, user counts and browser support, past confusion, and the applicant's track record with other namespaces, as detailed in Section V.

Recommendation 2: Require alternative namespace disclosure.

Applicants should disclose whether they or affiliates operate an alternative naming system using the applied-for string, the approximate registration count, the resolution mechanism, and any strings previously launched and abandoned. This should serve as a standard element of the application, not an optional addition.

Recommendation 3: Expand the TRT's data sources.

Supplement root server logs and resolver data with alternative namespace registration data, browser and app resolver status, and blockchain records. The TRT needs the authority and the means to gather data beyond the DNS query ecosystem.

Recommendation 4: Publish the assessment methodology before the application window.

As previously stated in ENS comments on transparency and cost predictability, and as multiple commenters noted in the Final AGB Proceeding, ICANN should publish the TRT's assessment methodology before the application period opens on April 30, 2026. Applicants planning to spend $227,000 or more should understand the criteria.

Recommendation 5: Create a "pre-existing alternative namespace" risk factor.

Strings with pre-existing registrations in alternative naming systems should not automatically trigger a high-risk designation, but should prompt evaluation of collision risk from overlapping strings and any required mitigation if the application moves forward.

Recommendation 6: Require overlapping namespace mitigation plans.

When an applicant already has registrations in another naming system using the same string, require them to submit, with the application (not later), a mitigation plan that covers: user notification, conflict prevention, coexistence architecture, and consumer protections. This is particularly important given that the Procedure Documentation's challenge mechanism applies a "clearly erroneous" standard of review. If the TRT's Initial Assessment is flawed because it lacked alternative namespace data, an applicant's ability to challenge that determination is limited by design. Getting the data sources right at the outset avoids reliance on a narrow appellate process.

Recommendation 7: Make certain the TRT has or can consult experts on alternative naming and blockchain resolution.

Collision risks in the 2026 round can't be evaluated with just 2012-era tools.

11 Collyer Quay
No. 17-11, The Arcade
Singapore 049317

Recommendation 8: Evaluate applicant track record.

Where an applicant has launched and abandoned TLD strings, the TRT should weigh that history as evidence of operational commitment. An applicant who has created and discarded dozens of TLDs, leaving registrants with non-functional identifiers, poses a different risk than one with a demonstrated record of long-term commitment. Willingness to maintain and take responsibility for the namespaces you create is an indicator that collision risks will be addressed in good faith.

Conclusion

ENS Labs supports ICANN's mission, the single authoritative DNS root, and the principle that new TLD strings should be created through the ICANN process, not outside it. The Name Collision framework for the 2026 round has a strong foundation.

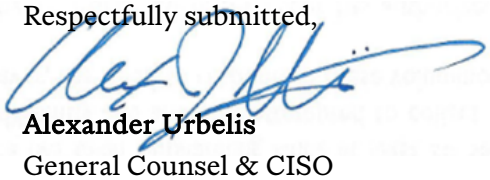
But it is incomplete. The procedures define the problem correctly – collision between the DNS and other naming systems – yet provide assessment tools calibrated for the last round. The 2026 round will face a new form of collision risk: many strings already registered in commercial alternative naming systems, some applied for by the operators who created those parallel namespaces and abandoned others. The procedures must be ready.

Responsible integration of Web3 naming with the DNS is possible. ENS has demonstrated it as the first large-scale Web3 naming platform, over eight years of continuous operation, DNS registry and registrar partnerships, and consistent ICANN engagement. ICANN should distinguish long-term, governance-minded operators from those with a transient, speculative record.

This comment offers actionable recommendations for the 2026 timeline and asks ICANN to complete the existing operational framework.

ENS Labs can provide technical expertise, data, and further input as ICANN finalizes these procedures. We appreciate the opportunity to participate and look forward to productive discussions.

Respectfully submitted,



Alexander Urbelis
General Counsel & CISO
ENS Labs, Ltd.