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

Open for Submissions Date:
Monday, 10 August 2026

Closed for Submissions Date:
Monday, 21 September 2026

Summary Report Due Date:
Monday, 16 November 2026 (extended from Monday 05 October 2026)

Category: Technical

Requester: ICANN organization

ICANN organization contact(s): globalsupport@icann.org

Open Proceeding Link: https://www.icann.org/en/public-comment/proceeding/initial-report-of-the-tsg-on-gtld-integrations-with-alternative-naming-systems-10-08-2026

Outcome:
40 Public Comments were submitted in response to the Public Comment proceeding on the Initial Report of the Technical Study Group on gTLD Integrations with Alternative Naming Systems. These include: 16 organizational or group submissions, 22 individual submissions, and two entries that were removed by the submitter. This report accounts for all 40 entries and summarizes the 38 available submissions and their supporting materials.

The record includes support for the core technical model, requests for stronger operational safeguards, concerns about policy and contractual scope, and differing positions on existing alternative-name holders. The Technical Study Group (TSG) will consider the Public Comments when updating the TSG draft initial report. This summary records the views submitted; it does not establish consensus or determine which proposals the TSG will adopt.

Section 1: What We Received Input On

The proceeding sought feedback on the TSG initial report dated 10 August 2026, including whether its proposed technical requirements are sufficient for integrations of gTLDs with the same string in an alternative naming system to be done in a secure and stable manner.

The draft report focused on common strings and controllers across integrated systems. It discusses Shared Registration System (SRS) enrollment and a distributed Unified Source of Truth, effective control, lifecycle coordination, failure handling and turn-down, emergency continuity, and security considerations. It also identifies matters outside of the TSG's technical scope. Comments address both the mechanisms and the policy or contractual consequences of implementing gTLDs with alternative naming systems.

Reading this summary

Section 2 identifies all submitters using the listed reference IDs. Organizations and individuals are listed separately and sorted alphabetically by organization name or displayed name/portal identity, not by ID. SL and KR identify the retracted entries. These are editorial reference IDs, not official ICANN submission numbers.

Section 3 combines the overview of responses and additional comments into one column, "Summary of comments," alongside the topic column. Bracketed IDs link to the underlying submission records. They identify sources, not a tally of agreement. A submission may address several topics, and positions within a topic may conflict.

Appendix A gives a separate synopsis for each available submission and records the two retractions. It follows the organization and individual groupings in Section 2. Statements of support are distinguished from conditions, objections, and requests for additional work. The proceeding is not treated as a vote, and no consensus is inferred from repeated wording, signatory counts, or organizational labels.

Descriptions of rights, market size, historic use, technical performance, and implementations are attributed to commenters, not independently established by this report. The Thai-language submission is summarized in English without expanding ambiguous wording into a more specific position. Self-reported affiliations do not establish organizational endorsement.

Section 2: Submissions

The register accounts for all 40 entries: 16 organizations or groups, 22 individual submissions, and two retracted entries. Grouping is for navigation and does not assign greater weight to any comment. Submission dates below are in 2026.

Organizations and Groups:

Name	Submitted by	Initials
.ART Domain Registry	Kurt Pritz	ART
At-Large Advisory Committee (ALAC)	Policy Staff in support of the At-Large Community	ALAC
CleanDNS Inc.	Alan Woods	CDNS
D3 Global, Inc.	Kevin Kreuser	D3
ENS Foundation	Alexander Urbelis	ENSF
Intellectual Property Constituency (IPC)	Margaret Milam	IPC
International Association for Astronomical Studies (IAAS)	Chris Rand	IAAS
Internet Service Providers and Connectivity Providers Constituency (ISPCP)	Philippe Fouquart	ISPCP
Ministry of Electronics and Information Technology, Government of India	Dheeraj Dheeraj	GOI
Netnod	Ulf Fredrik Karl Lindeberg	NN
Registrar Stakeholder Group (RrSG)	Zoe Bonython	RrSG
Registries Stakeholder Group (RySG)	Registries Stakeholder Group	RySG
Security and Stability Advisory Committee (SSAC)	SSAC Staff	SSAC
Tucows Domains	Sarah Wyld	TUC
Unregistry	Ageesen Sri	UR
WIPO Arbitration and Mediation Center	Brian Beckham	WIPO

Individuals:

Name	Affiliation (if provided)	Initials
Alfredo Calderon-Serrano	Individual At-Large member	ACS
Boris Koren / Bora	Bora	BK
Eric Barrett	Individual	EB
Grzegorz Orchel	IETF (self-reported)	GO
Ha Nguyen Hong	Individual	HNH
Johan Poyhonen	Individual	JP
Jonathon Browne / APlusDomains.Crypto	APlusDomains.Crypto	JB
Juan David Aristizábal	Individual	JDA
Laura Ndubi	Individual	LN
Mark "Marcus" Martinez / estmcmxci.eth	Personal capacity	MM
Mark Edwards	Individual	ME
Matthew Bird	Individual	MB
Matthias Darwin	Individual	MD
nguyen duy / Nguyen Ngoc Duy	Individual	NND
Nhat Huy Nguyen	Individual	NHN

Omar Sayed	X: PopDomains_x	**OS**
Onovughakpo Oghenebrorie Avbenagha	Individual	**OOA**
Quynh Nguyen	Individual	**QN**
Tanawat Pinjaikul	ICANN (self-reported)	**TP**
Theo Geurts	Individual	**TG**
Thomas Clowes	Unruggable; personal capacity	**TC**
Tiranest Manoratana	Individual	**TM**

Retracted entries:

Name	Submitted by	Initials
Samuel Liu	Retracted; content removed	**SL**
Krypto@Recht on X	Retracted; content removed	**KR**

Section 3: Summary of Submissions

The following table consolidates recurring themes and material disagreements. Each source reference uses the ID defined in Section 2. The table is descriptive, not a disposition of recommendations or a tally of support. Individual detail and attachment notes appear in Appendix A.

Topic	Summary of comments
Technical feasibility and the evidence threshold	The core model receives support, often conditional on stronger assurance. UR considers the registry-side requirements largely sufficient; NN, GOI, ISPCP, ACS, HNH, NHN, and LN seek more demonstrable safeguards. OOA emphasizes security, stability, and interoperability, while SSAC makes protection of normal DNS operation central. There is no agreement that every proposed integration can be done in a secure and stable manner. [UR, NN, GOI, ISPCP, ACS, HNH, NHN, LN, OOA, SSAC] Requests include threat models, impacts, acceptance criteria, independent testing, realistic operating evidence, and post-launch review. NHN proposes testing foreseeable failures and interventions against conflicting control and unacceptable inconsistency. TG takes no position on permitting integration and does not dispute potential security/stability, but questions whether the proposed industry-wide requirements follow from the report's security argument. MM and TC provide prototype illustrations, not proof of production safety. [NHN, TG, MM, TC]

Topic	Summary of comments
Scope, authority, and adoption process	Commenters distinguish technical advice from policy and contractual obligations. ALAC calls for a full GNSO policy process before approvals; IPC seeks resolution of relevant deferred policy issues and an explicit statement that the report creates neither policy nor a presumption of approval. RySG, RrSG, TUC, and ART caution against creating obligations through advisory language. [ALAC, IPC, RySG, RrSG, TUC, ART] Requests address the meaning of MUST/SHOULD, the basis for Registry Services Evaluation Policy (RSEP) applicability, whether the service falls within the limited set of matters in which Consensus Policies can be created, and responsible implementers. ENSF, RySG, and D3 oppose duties for non-integrating registries and retroactive 2026 Round changes. ISPCP seeks visible community and Board consideration of normative outcomes. TG asks that competition effects excluded from the study be addressed or referred explicitly rather than left outside the evaluation. [ENSF, RySG, D3, ISPCP, TG]
Architecture, DNS authority, and system boundaries	ALAC and ACS prefer SRS-centered initial deployment. D3 favors DNS-first creation and authoritative DNS registration. UR, RySG, GOI, and LN seek technology-neutral outcomes rather than a prescribed database or implementation. IPC asks that differences in architectures' ability to support existing policy and rights protection be made explicit. TG questions the relationship between the single-operator scoping condition and the report's distributed model. [ALAC, ACS, D3, UR, RySG, GOI, LN, IPC, TG] Comments distinguish registry-wide integration, registrar tokenization, registrant-directed import or association, and domain-linked profiles that create no second namespace. They request accommodation of thin registries, outsourcing, and existing implementations. A wallet or token transfer need not itself change the DNS registrant. [MM, ENSF, ART, RrSG, D3, TC]

Topic	Summary of comments
Continuing control and independent evidence	Initial proof alone is insufficient for contributors seeking continuing control assurance. Proposed evidence includes cryptographic bindings, authoritative records, revocation, and auditable controller and credential changes. NND proposes risk-sensitive maximum evidence age and fail-closed handling of stale proof; TC favors event-triggered revocation over universal fixed-expiry rules that could interrupt valid names. [NN, GOI, HNH, NND, NHN, TC] TG distinguishes registry assertions from an independently readable alternative-system state and asks that this difference be explicit. TG proposes signed, append-only, publicly auditable enrollment and allocation commitments for continuous verification. RrSG similarly questions whether a registry-reported state is independent evidence. IPC asks for effective transfer and enforcement capability, not common-control assertions alone. [TG, RrSG, IPC]
Synchronization, pending operations, and failure recovery	Commenters ask for eventual consistency to be expressed as testable operating requirements: bounded divergence, visible pending states, completion or rollback, conflict detection, and behavior during partitions or partial failure. NHN asks applicants to specify measurable convergence and pending-state limits, including compensating actions and unavailable-system behavior. [UR, NN, GOI, ISPCP, QN, NHN] Clarifications concern who detects discrepancies, recovery intervals, notices to users and registrars, and when a name must stop operating or remain withheld. Comments also address shared dependencies, additional integrated systems, and material changes to integrations. Requirements should not silently assume instantaneous consistency or a single architecture. [RySG, RrSG, HNH, MM, TC]
Lifecycle, renewal, expiration, and release	Comments seek equivalent outcomes across creation, transfer, suspension, restoration, expiry, and release. NHN proposes a conformance matrix covering expected state, authoritative evidence, and failure and recovery behavior for each transition. GOI proposes cross-system expiration until continued-control safeguards are demonstrated. RrSG asks who sponsors and pays for renewals and how off-channel obligations are avoided. ART supplies an existing lifecycle model; D3 distinguishes credential movement from a DNS registrant change. [SSAC, GOI, TUC, RrSG, QN, NHN, ART, D3] TG identifies indefinite withholding where alternative names do not expire or their controllers lose access, and seeks a defined return-to-availability path. TG also asks whether control requires only denial of use or power to reassign a name, with different implications for irrevocable ownership and lost keys. IPC seeks transfer or permanent disabling remedies where required for rights protection. [TG, IPC]

Topic	Summary of comments
Turn-down, emergency continuity, and EBERO	Several submissions seek mandatory, demonstrated exit arrangements rather than an untested plan, preserving DNS continuity during operator or alternative-system failure, discontinuation, or an Emergency Back-end Registry Operator (EBERO). NHN specifies freezing new changes, reconciling inconsistent state, safely disabling alternative functionality, preventing conflicting reallocation, and notifying registrants. [UR, NN, SSAC, GOI, ISPCP, ACS, QN, NHN, LN] Comments request triggers, decision authority, residual name state, control proof, restoration procedures, and notices. RySG seeks proportionate obligations without requiring EBERO to operate alternative systems. TG stresses that live alt-names may remain after DNS-side turn-down and asks for wind-down or successor-transfer capability, including insolvency and loss of common control. [RySG, GOI, TG]
Existing holders: requests for priority	ME, BK, TM, JP, EB, OS, and JB seek protection for established alternative registrations before matching DNS registries launch, often regardless of who wins the DNS string. JP asks for protection for existing alternative-name holders generally, mentioning .crypto, .nft, and wallet as examples. Proposals include recognition of prior claims, exclusive claim windows, verification, privacy, and user choice. [ME, BK, TM, JP, EB, OS, JB] JDA emphasizes confusion and phishing when matching names have different controllers. MD proposes evidence of established use, snapshots, cutoff dates, and scalable reservation or correction mechanisms. These are requests for policy treatment, not rights established by this summary. [JDA, MD]
Existing holders: transition without automatic DNS rights	ENSF, RySG, D3, and TC reject automatic DNS rights based solely on prior alternative registration. MB and IAAS ask that established populations and collision-safe transitions be addressed without claiming automatic delegation rights. These positions differ materially from universal grandfathering. NN identifies allocation consequences without endorsing prior rights. [ENSF, RySG, D3, TC, MB, IAAS, NN] MB proposes a pre-launch plan documenting population and uses, contractual expectations, controller verification, temporary DNS-name protection and its duration or fees, activation paths, conflicts with ICANN rules, and treatment of unclaimed or unverifiable names. MB regards existing use as evidence of demand and potential interoperability benefits, not an entitlement. IPC and WIPO separately seek protections against importing infringing allocations. Assertions about population size or historic use are not independently verified here. [MB, IPC, WIPO, MD]

Topic	Summary of comments
Rights protection, DNS launch, and external orders	IPC, WIPO, ALAC, SSAC, and CDNS ask how remedies operate across systems, particularly for alternative-primary or alternative-only names. IPC seeks demonstrated implementation of UDRP, URS, court orders, locks, and transfers without the losing registrant's cooperation. Where transfer is verifiably impossible, IPC proposes permanent burning, locking, or unbinding; DNS-only suspension is insufficient. [IPC, WIPO, ALAC, SSAC, CDNS] For legacy enrollment, IPC proposes published inventories, compliant controller data, Trademark Clearinghouse checks, and time-limited challenges before corresponding DNS-names are withheld. WIPO proposes a challenge mechanism capable of preventing integration of infringing labels. ENSF and TC seek reconciliation with Sunrise and Claims. [IPC, WIPO, ENSF, TC] CDNS supports functioning equivalents to UDRP and URS where the alternative system is primary. NHN asks that redress gaps be addressed before approval, with broader questions carried into policy and contractual work. RySG resists automatic extension of all DNS policies to alternative-only activity. UR favors DNS-anchored enforcement rather than duplicative proceedings. [CDNS, NHN, RySG, UR]
Abuse response and enforceable accountability	CDNS strongly supports retaining reciprocal deactivation and simultaneous suspension without dilution. CDNS seeks acceptance of well-evidenced reports from either system, including qualified third-party providers, while keeping mitigation responsibility with the registry. CDNS proposes standardized cross-system reporting as an RSEP technical-approval condition and common evidencing fields, formats, and validation. [CDNS] CDNS requests mapping sinkholing and nameserver redirection to equivalent alternative-system action, or simultaneous alt-name suspension where equivalence is unavailable. IPC seeks abuse contacts, reporting channels, broader consideration of the DNS-abuse definition, and explicit UDRP and URS triggers for reciprocal action. ALAC, GOI, ACS, NN, and RrSG emphasize contactability, response times, responsibility, and demonstrable enforcement. A power to request action should not be confused with ability to complete it. [CDNS, IPC, ALAC, GOI, ACS, NN, RrSG]

Topic	Summary of comments
User disclosure, registration data, and privacy	Requests include understandable pre-registration disclosures, visible integration state, operational contacts, notices during failures, and clarity about reversibility or loss of advertised permanence. NHN asks for accessible trust-model and failure-mode documentation; ACS emphasizes multilingual accessibility. TP offers general observations on transparency and verifiability. [UR, ALAC, ACS, NHN, TP] NHN favors data minimization and opaque or cryptographic controller proofs while satisfying applicable obligations, with documented access, compromise, and rotation procedures. IPC says such identifiers should supplement, not replace, required registration data and RDAP access. RySG, ART, and RrSG question new data duties and request clearer distinctions among RDAP, registration-data services, and request mechanisms. Wallet possession should not automatically be equated with legal identity. [NHN, IPC, RySG, ART, RrSG, GOI, TC]
Collision risks and resolution behavior	Matching controllers do not necessarily ensure identical answers or user experiences. NN and ALAC seek attention to risks not visible in DNS logs; SSAC and CDNS identify unpaired-name risks. IAAS raises collision management for independent pre-existing namespaces without asserting a delegation veto. [NN, ALAC, SSAC, CDNS, IAAS] Comments distinguish allocation and control from resolution provenance, security assurance, and user expectations. Requests include wider monitoring, pre-activation assessment, disclosure, and mitigation sequencing. ENSF separates risk assessment from priority claims; OOA and LN emphasize predictable interoperability and preservation of global DNS operation. [ENSF, OOA, LN]
IDNs, variants, label boundaries, and security assurance	Comments request clearer treatment of internationalized names, normalization, variants, confusables, label comparison, and public-suffix boundaries. NHN proposes testable normalization profiles, A-label/U-label behavior, character repertoires, and evidence that incompatible normalization cannot lead related strings to different controllers. [UR, NN, SSAC, GOI, RrSG, ISPCP, ACS, NHN] Clarifications include multi-object provisioning, relevant IDN-policy work, lower-level integrations, and Public Suffix List entries. Common allocation should not be equated with equivalent DNSSEC assurance. NHN also proposes threat modeling, independent security testing, realistic-load evidence, divergence monitoring, and notification to ICANN when integration guarantees are materially at risk. [SSAC, RrSG, NN, NHN]

Topic	Summary of comments
Implementation burden, examples, and staged learning	Registry and registrar comments ask which requirements protect DNS security and which chiefly enable a commercial service, seeking proportionate costs and explicit responsibilities. TG requests an incidence analysis covering implementers, beneficiaries, and necessity, and highlights pricing asymmetry, off-channel transactions, and cheaper alternative allocations denying availability of more expensive DNS names. [RySG, ART, TUC, RrSG, D3, TG] MM and TC offer prototypes, ART describes an existing service, and UR proposes a complementary association mechanism. SSAC, NHN, and LN favor testing, monitoring, and post-launch learning. NHN proposes enhanced reporting for early approvals before routine wider deployment. GO's brief general observations are retained without assigning a more specific technical proposal. [MM, TC, ART, UR, SSAC, NHN, LN, GO]

Section 4: Analysis of Submissions

The submissions highlight four areas of consideration for the TSG: the scope and justification of its proposed technical requirements, how compliance with those requirements can be demonstrated, where technical recommendations intersect with broader policy and contractual considerations, and the assumptions about alternative naming systems underlying some of the comments. These themes emerge across submissions expressing different views on the proposed integration model.

The first concerns the relationship between the TSG's proposed requirements and the security and stability objectives they are intended to achieve. While some commenters seek additional safeguards, others question whether particular requirements are necessary for security or primarily support the implementation and delivery of the service. Taken together, these comments reflect differing views not only on whether the proposed requirements are sufficient, but also on which requirements are necessary to achieve the report's stated security and stability objectives.

A second and related issue is how compliance with the proposed requirements would be demonstrated and evaluated. Requests for independent verification, continuing proof of control, measurable synchronization limits, predictable failure recovery, and tested turn-down arrangements emphasize the distinction between describing how an integration is designed to operate and demonstrating that it can maintain the required security and operational outcomes. These comments also raise questions about what evidence would be sufficient to demonstrate compliance and whether that evidence should depend on the particular architecture used.

The third area concerns matters that technical requirements alone may not resolve, that, the technical ability to suspend, transfer, or disable a name does not itself establish the policy or contractual circumstances under which those actions must occur. These comments reflect a distinction between the technical capability to implement an integration and the policy or contractual decisions governing when and how that capability may be used.

A fourth consideration concerns assumptions about the characteristics and behavior of alternative naming systems. Some submissions appear to presume that integrated systems maintain equivalent records, provide comparable resolution behavior, or operate within similar performance constraints. However, alternative naming systems may differ substantially in the data they contain, the functions they perform, and their operational characteristics. This distinction helps explain the tension between requests for more specific technical requirements, such as uniform convergence limits, and the TSG's examination of integrations without presupposing a particular alternative-system architecture or implementation. While most use cases will *probably* converge around blockchain-based naming, there is nothing that guarantees that will be the only use. And even there, it is possible to observe divergence where some expect the alternative systems to duplicate the global DNS data and add to it, while others seem to expect DNS data to remain in the DNS and only additional data to appear in the alternative system. The TSG's task was to understand the security and stability characteristics in general, and to try to offer a similarly general understanding of the kind of design that can be safe.

As noted in its charter, the TSG was convened to evaluate and make technical recommendations for how integrations could be effected in a stable and secure manner. The TSG's recommendations are one aspect of the broader consideration of this new type of service. Determining how this service may be introduced will require collective consideration of the technical recommendations, contractual language, consensus policy requirements, and applicable ICANN processes.

Section 5: Next Steps

The TSG will consider all submissions as part of its continued examination of gTLD integrations with alternative naming systems and revise its report as appropriate. ICANN org will also consider the submissions in developing proposed contractual language for registry agreements. Some comments may be addressed through revisions to the TSG report, while others may inform the proposed contractual provisions.

The final TSG report will be published on the TSG webpage. The proposed contractual language will be published for Public Comment, with links to the final TSG report.

The finalized TSG report is intended to inform the evaluation of future requests to offer this integration service through the RSEP process or as part of the New gTLD Program application process. Any resulting contractual provisions would apply only to registries approved to offer the service through the applicable process and would not be imposed on registries that have not requested to offer the service.

Appendix A: Submission-by-Submission Summary

Each available submission is retained separately, including closely similar comments. The ID in each heading links to the official submission page; retracted IDs link to the relevant portal listing. Synopses describe submitter positions, not conclusions adopted by the TSG.

Organizations and groups

ART | .ART Domain Registry

20 Sep 2026 | Kurt Pritz

Supports a common baseline and offers its existing integration as an implementation example. Describes DNS-first verification and an alternative-first path that secures the DNS name for the holder, with alternative rights lost following specified DNS lifecycle or enforcement events. Says practical models can meet the core objectives without all proposed SRS, EPP, or registration-data changes. Questions whether parts of the report overreach into policy and contractual matters, and warns that excessive data requirements could drive users toward unregulated alternatives. Requests clearer distinctions among RDAP and other registration-data mechanisms.

ALAC | At-Large Advisory Committee (ALAC)

21 Sep 2026 | Policy Staff in support of the At-Large Community

Does not oppose exploration, but calls for a full GNSO Policy Development Process before approvals and favors the SRS plug-in approach. Emphasizes user confusion, differing resolution behavior, contactability, delayed enforcement, and abuse or collision activity invisible to DNS monitoring. Seeks meaningful consent for holders previously promised permanent names, effective rights protection, minimum verifiable contact information, maximum suspension-synchronization intervals, and ongoing compliance. Requests a separate SSAC collision review without waiting for that policy process, and transparency concerning potential conflicts of interest in the TSG.

CDNS | CleanDNS Inc.

21 Sep 2026 | Alan Woods

Strongly endorses the reciprocal deactivation and simultaneous suspension provisions in Sections 8.5 and 8.6 and asks that they be retained without dilution. Recognizes the technical, rather than policy or contractual, purpose of the report. Presents its concerns as operational matters for early attention, not insurmountable barriers to integration.

Recommends recognizing qualified third-party abuse mitigation providers and accepting well-evidenced reports originating from either naming system, while leaving mitigation responsibility with the registry operator. Proposes standardized cross-system reporting infrastructure as a condition of technical approval through RSEP, and interoperable evidence protocols specifying minimum fields, formats, and validation criteria. Relevant alternative-system evidence can include wallet and minter addresses, token and blockchain identifiers, namespace and record structures, registration dates, and associated DNS data.

Requests a mapping of reciprocal actions beyond holds, including sinkholing and nameserver redirection. Where an alternative architecture cannot implement an equivalent intervention, proposes simultaneous alt-name suspension so continued availability does not undermine DNS-side disruption. Supports functioning equivalents to UDRP and URS for alternative-system-primary integration, and stresses proactive evidence-based reporting where ordinary redress cannot operate. Identifies phishing, impersonation, and consumer-confusion risks from unpaired alt-names and asks that necessary mitigation infrastructure be identified for appropriate policy or contractual treatment.

D3 | D3 Global, Inc.

16 Sep 2026 | Kevin Kreuser

Supports voluntary, registry-controlled, risk-based integration while preserving DNS registration authority. Favors DNS-first creation through established registrar channels and optional, not default, alternative-only withholding. Rejects automatic rights from independently operated alternative namespaces and retroactive 2026 Round changes. Distinguishes registrar-level tokenization without a second namespace from the TSG model, and distinguishes token or wallet movement from a change of DNS registrant. Requests architecture-neutral treatment of custody, bridging, and pending states, with proportionate turn-down and appropriate community or contractual handling of data, rights-protection, and policy questions.

ENSF | ENS Foundation

21 Sep 2026 | Alexander Urbelis

Supports the string-plus-controller model and Unified Source of Truth. Asks that the framework apply to voluntary, registry-controlled integration, not independently operated namespaces merely sharing a string. Rejects automatic DNS priority, reservation, or grandfathering based on prior alternative registrations, and obligations on non-integrating registries or retroactive changes to the 2026 Round. DNS activation should respect Sunrise and Claims requirements. Distinguishes genuine collision risks from allocation rights and treats verifiable blockchain evidence as a risk-assessment input, not an entitlement. Identifies registrant-elected DNSSEC import as outside the framework under discussion.

IPC | Intellectual Property Constituency (IPC)

21 Sep 2026 | Margaret Milam

Treats the report as technical advice to ICANN org, not policy or a presumption of approval. Requests community resolution of relevant deferred policy issues before affected integration services are approved. Asks the TSG to distinguish architectures by their ability to support existing consensus policies, contractual requirements, and rights-protection mechanisms; same-controller parity alone is insufficient.

For proposals other than SRS enrollment with registry-held controller data, seeks demonstrated implementation of UDRP decisions, URS determinations, court orders, proceeding-related locks, and registrar transfers across all integrated systems without the losing registrant's cooperation, with an identifiable, obligated enforcement party. Requests compliant registration data and RDAP access, abuse contacts and reporting channels, and deterministic handling of conflicting strings. Opaque identifiers or wallet addresses should supplement, not replace, required registration data. Suggests considering a broader definition of DNS abuse and expressly making UDRP and URS outcomes non-waivable triggers for reciprocal action.

Asks that control include effective transfer, suspension, or permanent disabling of an alt-name without its controller's cooperation. Transfer remains the primary remedy; where technically impossible, the operator should demonstrate permanent burning, locking, or unbinding that prevents re-registration, relinking, and resolution. DNS-only suspension is insufficient. Before legacy names are enrolled or corresponding DNS-names withheld, proposes a published inventory, compliant controller data, Trademark Clearinghouse checks, and a time-limited rights-holder challenge process.

IAAS | International Association for Astronomical Studies (IAAS)

17 Sep 2026 | Chris Rand

Asks the TSG to address independently controlled, pre-existing alternative namespaces, using .iaas as an example. Does not claim automatic DNS rights or a veto over delegation. Proposes distinguishing genuine established use from manufactured claims, identifying collision risks before activation, and considering voluntary coexistence, disclosure, controller verification, sequencing, and monitoring. Suggests deferring activation where identified risks remain unmitigated. Separates technical protection from allocation priority and acknowledges that an acronym can have multiple legitimate users.

ISPCP | Internet Service Providers and Connectivity Providers Constituency (ISPCP)

15 Sep 2026 | Philippe Fouquart

Supports the technical work but considers the risk assessment incomplete. Requests a stronger mapping of threats, impacts, mitigations, acceptance criteria, and shared responsibilities, including bounded convergence, multiple alternative systems, and proof in thin-registry arrangements. Calls for security and integrity assurance appropriate to each technology, effective rights-protection remedies, mandatory continuity and turn-down arrangements, and post-launch monitoring with incident and remediation thresholds. Seeks explicit community and Board consideration of recommendations that would become normative or contractual, with rigor and visibility appropriate to their consequences.

GOI | Ministry of Electronics and Information Technology, Government of India

21 Sep 2026 | Dheeraj Dheeraj

Supports exploration subject to measurable, verifiable approval conditions. Proposes a technology-neutral control-assurance dossier covering roles, interfaces, privileged access, key custody, revocation, and recovery. Requests defined pending, committed, failed, and rollback states; justified limits on unresolved operations; and safeguards against partial completion. Seeks mandatory tested turn-down, clear triggering authorities, independent security and cryptographic audits, load and partition testing, abuse-response service levels, and stop-work criteria. Until continued-control safeguards are demonstrated, recommends expiration across integrated systems and no DNS reallocation while the alternative name remains active.

NN | Netnod

21 Sep 2026 | Ulf Fredrik Karl Lindeberg

Regards common string and controller as necessary but insufficient. Distinguishes allocation and control from equivalent resolution behavior, and seeks public convergence limits, cryptographic proof of exclusive control, and explicit treatment of correlated failures and additional integrated systems. Requests DNSSEC-assurance clarity, mandatory tested turn-down, predictable dispute and lifecycle effects, and collision monitoring that is not confined to DNS observations. Notes the allocation consequences of withholding existing alternative names without taking a position on whether those names create prior rights. DNS continuity, rather than operation of alternative systems by EBERO, should remain the emergency objective.

RrSG | Registrar Stakeholder Group (RrSG)

18 Sep 2026 | Zoe Bonython

Asks whether proposed requirements are advisory, necessary, sufficient, or indicative, and how they would be adopted or applied to pending applications. Requests a requirement-by-requirement explanation of DNS necessity, responsible implementers, beneficiaries, and costs. Raises registrar participation, renewal sponsorship and payments, potentially indefinite withholding, contact verification, status notifications, and data responsibilities. Warns that registry attestations do not constitute independent verification of alternative-system state. Seeks better treatment of additional integrated systems, changes of controller, resolution behavior, rights protection, and enforcement. Questions obligations outside the Picket Fence and on parties without relevant alternative-system contracts.

RySG | Registries Stakeholder Group (RySG)

21 Sep 2026 | Registries Stakeholder Group

Supports a clear, efficient, risk-based framework for voluntarily proposed registry services. Questions automatic assumptions about RSEP applicability and asks that requirements be tied to material DNS risks and proportionate mitigation. Rejects automatic rights arising from independent alternative namespaces and duties for non-integrating registries. Requests architecture neutrality, a clear distinction between advisory language and binding obligations, and optional rather than default alternative-only withholding. Seeks appropriate processes for data, policy, and contractual changes; no retroactive 2026 Round obligations; and proportionate turn-down without expanding EBERO responsibilities. Differentiates RDAP, registration-data services, and the Registration Data Request Service.

SSAC | Security and Stability Advisory Committee (SSAC)

21 Sep 2026 | SSAC Staff

Broadly supports the report subject to alternative-system dependencies not impairing normal DNS operations. Requests clearer status terminology, continual control assurance, predictable emergency handling, and working rights-protection outcomes where the alternative system is primary. Recommends post-launch review. Raises unpaired-name and collision risks, ambiguity around lower-level integrations and the Public Suffix List, and implementation questions concerning IDN variants and multi-object provisioning. Treats broader registration-data evolution as related work rather than automatically part of integration evaluation criteria.

TUC | Tucows Domains

18 Sep 2026 | Sarah Wyld

Endorses the RrSG submission. Regards the report as a useful technical starting point, but raises policy and contractual-scope concerns, including the Picket Fence. Seeks a clear distinction between technical advice and binding obligations, with registrar data, technical, and lifecycle duties adopted through appropriate community and contractual processes. Requests clearer implementation responsibilities and treatment of renewal and release.

UR | Unregistry

21 Sep 2026 | Ageesen Sri

Supports the core model and considers the registry-side requirements largely sufficient. Requests visible integration state, bounded divergence, a fail-safe response to irreconcilable state, and tested turn-down. Calls for clearer user disclosures and an accountability floor for alternative-only or DNS-expired names. Separates Section 8.3 policy questions from technical requirements and opposes obligations on non-integrating operators. Proposes complementary, registrant-directed DNS TXT/DNSSEC associations, including different labels, with a clear distinction between declaring an association and proving common control. Suggests further standards work without making it a prerequisite for the registry-integration framework.

WIPO | WIPO Arbitration and Mediation Center

21 Sep 2026 | Brian Beckham

Calls for attention to the interaction between integration and rights-protection mechanisms, including Sunrise and UDRP. Warns against automatically mapping existing alternative-system registrations into the DNS where those registrations may infringe trademark rights. Suggests a challenge mechanism with consequences such as blocking, withholding, or prohibiting integration of a successfully challenged label.

Individuals

ACS | Alfredo Calderon-Serrano

25 Aug 2026 | Individual At-Large member

Supports the foundational model as necessary but insufficient and favors DNS/SRS-centered initial deployment. Requests independent, public assurance addressing failures, forks, and keys; complete lifecycle equivalence; effective rights protection and timed abuse response; and continuing registry accountability for outsourced components. Proposes accessible, multilingual pre-purchase disclosures and public integration-state information, stronger privacy-preserving control proof in thin models, strict IDN and variant testing, and tested, funded exit arrangements.

BK | Boris Koren / Bora

19 Sep 2026 | Affiliation stated as Bora

Supports integration on condition that existing Web3 registrations are treated as legitimate prior claims. Requests a transparent, exclusive opportunity for existing holders to claim corresponding DNS names, including under .crypto, .wallet, .nft, and .dao, instead of treating those names as unallocated inventory.

EB | Eric Barrett

6 Sep 2026 | Individual submission

Requests protection for existing registrants across .crypto, .bitcoin, .wallet, .nft, .dao, .polygon, .zil, and .blockchain regardless of the future DNS registry operator. Proposes recognition of prior rights, a time-limited claim and verification process, privacy and choice, and grandfathering to avoid loss of established names, identity, and economic interests.

GO | Grzegorz Orchel

30 Aug 2026 | Affiliation stated as IETF

Offers brief general observations about security, self-control or automation, individual input, and participation. The posted wording does not identify a specific amendment to the draft or a sufficiently defined technical proposal to summarize more narrowly. The stated IETF affiliation is not treated as evidence of an institutional IETF submission.

HNH | Ha Nguyen Hong

19 Aug 2026 | Individual submission

Supports the direction of the report and its effective-control and lifecycle principles. Requests practical guidance on responsibilities, detection and communication of material changes, escalation during synchronization failures, recovery, and auditable operational evidence. Emphasizes demonstrating continued common control rather than relying only on initial verification.

JP | Johan Poyhonen

14 Sep 2026 | Individual submission

Asks for protection for existing alternative-name holders, mentioning .crypto, .nft, and wallet as examples. Requests recognition of existing registrations as prior claims rather than free inventory and proposes a defined window to verify control and claim matching DNS names, with privacy protections and grandfathering instead of reallocation to new purchasers.

JB | Jonathon Browne / APlusDomains.Crypto

31 Aug 2026 | Affiliation stated as APlusDomains.Crypto

Requests prior-claim protection and grandfathering for existing .crypto registrants, independent of which entity later operates the DNS registry. Proposes a transparent verification and claim window, preservation of privacy and user choice, and protection of established identity and economic interests. The position closely parallels other .crypto-holder submissions but is retained as a separate entry.

JDA | Juan David Aristizábal

4 Sep 2026 | Individual submission

Argues that assigning the same human-readable name to different controllers across established alternative systems and the DNS creates foreseeable confusion, phishing, and rights-related harms. Requests structural protection for existing registrants across multiple namespaces and application of the same-string, same-controller principle in a way that protects established users.

Attachment note: Although the comment refers to an attachment, no attachment was included in the submission, as confirmed by the report requester.

LN | Laura Ndubi

11 Aug 2026 | Individual submission

Supports conditional, incremental exploration with demonstrable security, reliability, and predictability. Requests enforceable evidence of a Unified Source of Truth, attention to user expectations and consistent meaning, and adequate redress, abuse response, and data safeguards before broad deployment. Favors measurable outcomes within ICANN's remit rather than rigid architecture, together with safe exit and emergency continuity arrangements.

MM | Mark "Marcus" Martinez / estmcmxci.eth

21 Sep 2026 | Personal capacity; not ENS Labs or ENS Foundation

Presents TLD Oracle, a testnet prototype binding a gTLD to a registry-controlled Ethereum address through a DNSSEC-authenticated record. The proposal addresses the TLD-level binding, not the full subordinate-name lifecycle. It contemplates use only for approved integrations, revalidation following operator changes, continued SRS authority, and demonstrated turn-down capability. The submission describes a possible technical approach rather than an institutional commitment by ENS.

ME | Mark Edwards

19 Sep 2026 | Individual submission

Requests protection for existing .crypto registrants regardless of which entity operates a future DNS registry. Proposes recognition of prior claims, grandfathering, and a transparent, time-limited process to verify control and claim matching DNS names. Emphasizes continuity of identity and economic interests, privacy and user choice, alongside a viable registry business model.

MB | Matthew Bird

8 Sep 2026 | Individual submission

Supports the string+controller principle and requests explicit treatment of alternative namespaces that are already substantially populated before the corresponding gTLD launches. Proposes a mandatory pre-launch transition plan, or at least an evaluation criterion, covering the existing alt-name population and uses; contractual entitlements and expectations; proof of common control; protection of matching DNS-names during launch, including duration, fees, and conditions; a clear claim, enrollment, or activation process; conflicts with reserved names, trademark protections, and other ICANN rules; and unclaimed or unverifiable names.

Warns that absent a workable transition, many DNS-names could remain withheld or operationally uncertain. Treats active communities, applications, and services as evidence of demand and utility, and as a possible foundation for interoperability and DNS adoption. Explicitly rejects an automatic entitlement to DNS delegation or allocation: applicable security, stability, rights-protection, reserved-name, and consensus-policy requirements still apply.

MD | Matthias Darwin

14 Aug 2026 | Individual submission

Argues for protecting demonstrably established alternative namespaces, rather than mere speculative claims, when matching DNS strings are delegated. Suggests criteria based on use and registration history, and a verified priority opportunity for existing holders subject to ICANN rules. Proposes scalable mechanisms such as cryptographic snapshots, cutoff dates, data exchange, automated reservations, and correction or dispute procedures. Cites Freename namespaces and personal holdings as examples; this report does not independently validate the submission's registration figures or asserted rights.

NND | nguyen duy / Nguyen Ngoc Duy

16 Aug 2026 | Individual submission

Proposes treating controller evidence as current, renewable assurance rather than a fact established once. Requests measurable maximum evidence age, revalidation after expiry, transfer, key changes, or recovery, and traceable authoritative proof. Stale or broken evidence should trigger a fail-closed alternative-system state rather than continued reliance. Allows risk-sensitive durations, including longer validity where effective revocation exists. Uses previously observed integration failures to illustrate failure classes, not to establish their prevalence in future TSG-compliant systems.

NHN | Nhat Huy Nguyen

12 Aug 2026 | Individual submission

Conditionally supports the model, subject to clear, testable, auditable, and enforceable requirements before approval. Requests measurable limits for synchronization, pending states, conflict detection, rollback or compensation, and system unavailability. Proposes a lifecycle conformance matrix identifying expected state, authoritative controller evidence, failure behavior, and recovery for each transition; equivalence should be judged by security outcomes, not identical status labels.

Seeks a mandatory tested exit plan covering frozen changes, state reconciliation, safe disabling of alternative functionality, protection against conflicting reallocation, registrant notices, and DNS continuity during turn-down or EBERO. Requests understandable integration-status and lifecycle disclosures, clear support and abuse-handling responsibility, and public explanations of trust and failure modes. Favors data minimization and opaque or cryptographic controller proofs where compatible with applicable ICANN obligations, with documented storage, access, compromise, and identifier-rotation procedures.

Requests testable IDN normalization profiles, A-label/U-label behavior, and variant safeguards; documented threat models, independent testing, operational-maturity evidence, divergence monitoring, and incident notification to ICANN; and clear abuse, suspension, dispute-resolution, lawful-order, and support arrangements for alternative-only models, with out-of-scope matters carried into later policy and contractual work. Proposes enhanced reporting and review for early approvals. The evaluation should reject an integration if reasonably foreseeable events can produce conflicting controllers or unacceptably prolonged inconsistent state, or if the applicant cannot demonstrate protection against those outcomes.

OS | Omar Sayed

1 Sep 2026 | Affiliation stated as X: PopDomains_x

Requests protection of existing .crypto names regardless of the eventual DNS operator. Favors recognizing prior claims, a transparent time-bound control-verification and matching-name claim process, privacy, user choice, and grandfathering. Seeks continuity for existing holders alongside a viable future registry.

OOA | Onovughakpo Oghenebrorie Avbenagha

21 Sep 2026 | Individual submission

Supports the report while emphasizing strict safeguards for DNS security, stability, and interoperability. Highlights collision prevention, clear provenance, consistent resolution, and preservation of the integrity of the global DNS.

QN | Quynh Nguyen

15 Aug 2026 | Individual submission

Supports common control, the SRS-centered approach, and distributed Unified Source of Truth arrangements with auditable evidence. Requests clearer handling of the full lifecycle, including pending or partially completed operations. Emphasizes data integrity, abuse and dispute handling, operational failures, and situations where DNS rules do not translate directly. Calls for exit and EBERO arrangements that protect existing users and avoid divergent control.

TP | Tanawat Pinjaikul

12 Sep 2026 | Individual submission

The posted Thai-language comment emphasizes accurate, transparent, unambiguous, and verifiable integration and operation. It does not identify a specific technical amendment. This is an English synopsis of the posted text, not an inference of an official ICANN organizational position.

Attachment note: The report requester reviewed the PDF and confirmed that it is a copy of the TSG initial report, not a separate original comment.

TG | Theo Geurts

15 Sep 2026 | Individual submission

Offers a technical critique without taking a position on whether integration should be permitted or disputing that the model can be safe with adequate controls. Argues that the report's single-operator scope makes exclusivity an internal invariant, and asks whether Section 6's treatment of differently controlled distributed components is actually within that scope. Says external EPP and RDAP mechanisms neither create that invariant nor independently verify it; they principally make the service transactable through the registrar channel.

Requests either independently readable alternative-system state or an explicit statement that the coupling is registry-attested. Calls for a requirement-by-requirement account of implementers, beneficiaries, costs, and necessity for security, distinguishing those needs from commercial enablement. Identifies competition implications of off-channel registration, low-cost alternative allocations withholding higher-priced DNS names, and legacy allocations determining DNS availability; asks that these be addressed or explicitly referred to the appropriate process.

Requests a defined reclamation path for coupled names where the alternative system has no expiry cycle or the controller loses access. Asks whether required control means denial of use or actual reassignment, including consequences for irrevocable ownership and lost keys. Seeks wind-down or successor-transfer capability for the alternative system, addressing EBERO, operator failure, insolvency, and residual live alt-names. Proposes signed, append-only, publicly auditable commitments to enrollment and allocation state so continued string+controller compliance can be independently checked after approval.

TC | Thomas Clowes

9 Sep 2026 | Unruggable; personal capacity

Supports the model and presents the Altname prototype as an implementation illustration, not an approved production system. Describes normalized lifecycle events, opaque identifiers, cryptographic proofs, pending states, monitoring, audits, and turn-down. Requests explicit reconciliation of existing-name withholding with Sunrise and Claims, and rejects universal prior rights over future DNS registries. Favors continuing, event-triggered proof and revocation rather than a universal fixed-expiry rule. Calls for resetting or reaffirming records and credentials after controller changes, and distinguishes a second namespace from simpler domain-linked profiles.

TM | Tiranest Manoratana

16 Sep 2026 | Individual submission

Requests recognition of existing alternative .nft registrations before delegation of a matching DNS registry. Proposes grandfathering and a transparent, time-limited verification and claim process, with privacy safeguards and user choice. Seeks to protect established identities and economic interests while allowing a sustainable registry model.

Retracted entries

SL | Samuel Liu

17 Sep 2026 | Retracted submission

KR | Krypto@Recht on X

1 Sep 2026 | Retracted submission

Appendix B: Abbreviations

Term	Meaning
A-label / U-label	ASCII / Unicode representations of an internationalized domain-name label
ANS	Alternative naming system
DNS / DNSSEC	Domain Name System / DNS Security Extensions
EBERO	Emergency Back-End Registry Operator
EPP	Extensible Provisioning Protocol
GNSO / PDP	Generic Names Supporting Organization / Policy Development Process
gTLD / TLD	Generic top-level domain / top-level domain
IANA	Internet Assigned Numbers Authority
IDN	Internationalized domain name
NS	Nameserver
RDAP	Registration Data Access Protocol
RDRS	Registration Data Request Service
RSEP	Registry Services Evaluation Policy
SRS	Shared Registration System
TMCH	Trademark Clearinghouse
TSG	Technical Study Group
UDRP	Uniform Domain Name Dispute Resolution Policy
URS	Uniform Rapid Suspension System
USoT	Unified Source of Truth