CleanDNS Inc. Public Comment on the Initial Report of the TSG on gTLD Integrations with Alternative Naming Systems

1. Introduction

CleanDNS Inc. (https://www.cleandns.com) respectfully submits this comment in response to the public comment proceeding on the Initial Report of the TSG on gTLD Integrations with Alternative Naming Systems.

CleanDNS was developed by a team of cyber security and investigative professionals to provide a systemized, customizable process for mitigating and disrupting domain name abuse and other online harms. Infrastructure providers use CleanDNS systems to identify, track, and report abuse activity. CleanDNS also is the backend of the Netbeacon Reporter platform (http://www.netbeacon.org) for the Netbeacon Institute, the centralized abuse reporting facility.

2. Support for the Reciprocal Takedown Principle Under Sections 8.5 and 8.6

Although we express our general support for the conclusions of the TSG Report and appreciate the work being undertaken, our comment should be limited in its breadth, specifically to those aspects with direct relevance to our own area of expertise. As such CleanDNS strongly supports the reciprocal takedown requirements set forth in Sections 8.5 and 8.6 of the TSG Initial Report. These provisions reflect a sound operational principle aligned with CleanDNS' prior work on harms in the Web3.0 and alternative namespace ecosystem. CleanDNS recognises that this is a technical study and not a policy or contractual document as such the observations that follow are intended to identify areas where the technical integration contemplated by the Report may give rise to policy or contractual considerations, particularly within the RSEP process, that would benefit from early identification. None of these observations are intended to be insurmountable; rather, they flag matters that merit attention as the framework develops.

Section 8.5 of the Initial Report concludes that "if a service is deactivated for external reasons (e.g. abuse, court order) in one naming system, the registry MUST disable the name, on the prudential principle that a danger to the Internet from a given name in

one naming system is a danger in all naming systems." CleanDNS endorses this conclusion without reservation. A domain name that has been disabled due to abuse or legal process in one naming system should not remain active and exploitable in another. Permitting such an outcome would undermine the very purpose of the takedown action and expose Internet users to continued harm.

CleanDNS likewise supports Section 8.6's requirement that "suspensions MUST apply to all naming systems simultaneously." Simultaneous application is operationally necessary to prevent bad actors from exploiting timing gaps between systems to continue abusive activity during a staggered suspension process.

Taken together, these provisions establish a practical reciprocal takedown principle. CleanDNS urges the TSG to retain them in the Final Report without dilution.

3. Define a Role for Third-Party Abuse Mitigation Providers

We note specifically that sections 8.5 and 8.6 articulate the reciprocal takedown expectation, and accept this is framed exclusively from the registry operator's perspective. In practice, however, DNS abuse takedowns are frequently identified and escalated, not by registry operators themselves but by qualified third-party abuse mitigation providers who detect, evidence, and report abuse to registries and registrars. The Report should acknowledge this operational reality.

CleanDNS does not suggest that the obligation for mitigation or disruption itself should shift away from the registry operator, after all where a registry operator chooses to work with a third-party provider to discharge its abuse mitigation obligations, that is merely their means of dealing with the obligation. The more fundamental point is that in an integrated naming system, the expectation to receive and act upon well-evidenced reports of abuse should extend equally to both the DNS-name and alt-name sides. Abuse reports must be capable of being submitted from either side of the reciprocity divide, and the registry operator's obligation to act should apply regardless of which naming system generated the report.

CleanDNS recommends that the TSG's final Report indicate that an integrated registry operator should maintain the same obligation to receive and action well-evidenced reports of abuse on the alt-name side as exists on the DNS side, with reciprocal effect across both naming systems. To an extent this could mirror the expectations of the traditional ICANN namespace, insofar as the applicability of obligations found in Specification 6(4) of the Registry Agreements. Although contemplated, and indeed acknowledging this is a technical assessment and not a legally focused document, greater enumeration of such an expectation within the alternative namespace would

ensure that the operational infrastructure supporting the reciprocal takedown principle reflects the way abuse mitigation actually functions in the DNS today.

4. Standardized Abuse Reporting Infrastructure Is Essential

The reciprocal takedown obligation set out in Sections 8.5 and 8.6 of the Initial Report cannot function in practice without a common abuse reporting infrastructure that spans both the DNS-name and alt-name layers. A registry operator that receives a takedown request through its existing DNS abuse channels must have a corresponding mechanism on the alt-name side to execute the reciprocal suspension. Without such infrastructure, the obligation remains aspirational.

CleanDNS' prior work on Web3.0 harms directly addressed this gap and recommended a centralized reporting facility through which reports can be submitted, validated, verified, and routed for action.

CleanDNS recommends that the TSG require any registry operator seeking to integrate with an alternative naming system to demonstrate the availability of a standardized abuse reporting mechanism that covers both naming systems. This requirement should be a condition of technical approval under the Registry Services Evaluation Policy (RSEP) process.

5. Interoperable Evidencing Standards

The principle of reciprocal takedown can only be put into practice at an operational level if a takedown action in one naming system carries verifiable evidence sufficient to support reciprocal action in the other. Without standardized evidencing protocols, a registry operator receiving a reciprocal request will lack the information necessary to validate the underlying abuse determination.

Recalling our past commentaries on Web3.0 harms, we identified data points necessary to substantiate abuse across alternative naming systems, including:

- Wallet addresses associated with the registrant or minter
- Token IDs and blockchain network identifiers
- Namespace and record key structures
- Minter address and registration date
- Associated DNS resolution data, where applicable

These data points differ materially from the evidence typically compiled in traditional DNS abuse reports. An integrated registry operating across both naming systems must

be capable of receiving, interpreting, and acting upon evidence formatted for either system.

CleanDNS suggests that the TSG consider whether standardized evidencing protocols enabling cross-system abuse verification should form part of the expectations for any registry operator seeking to integrate with an alternative naming system. Such protocols, defining minimum evidentiary fields, acceptable formats, and validation criteria applicable to both DNS-name and alt-name abuse reports, may add a degree of complexity to the integration process but are not insurmountable and would materially strengthen the reciprocal takedown framework.

6. Mapping Disruption Actions Beyond Holds

Sections 8.5 and 8.6 refers broadly to disabling and suspending names. In practice, however, DNS abuse mitigation is not limited to serverHold or clientHold status codes. Two additional forms of intervention are operationally significant and, in certain contexts, preferable to holds.

First, sinkholing, in which DNS queries for an abusive domain are redirected to a controlled server, is a widely used and often preferred mitigation action at the DNS level. Sinkholing allows abuse to be disrupted while preserving forensic visibility into the scope and nature of the threat, an advantage that outright suspension does not provide.

Second, redirection of a domain's nameserver (NS) records is a required registry-level action in the case of a successful proceeding under the Uniform Rapid Suspension (URS) system. NS redirection is distinct from a hold in both its mechanism and its operational effect.

The TSG's final Report should also address how these non-hold-based interventions map to reciprocal action in an integrated naming system. Specifically, the Report should consider whether a sinkhole or NS redirect applied on the DNS-name side should trigger a reciprocal action on the alt-name side, and if so, what form that reciprocal action should take given the technical characteristics of the alternative naming system in question. Different alt-name architectures may not support a direct equivalent of sinkhole or NS redirection. In those cases, the Report should express the need for the registry operator apply a sympathetic and simultaneous suspension on the alt-name, ensuring that disruption on one side of an integrated namespace is not undermined by continued availability on the other.

CleanDNS recommends that the TSG consider expanding its treatment of reciprocal action to address disruption mechanisms beyond holds, including at a minimum

sinkholing, NS redirection, and their equivalents or fallback actions within alternative naming systems. Mapping these mechanisms may introduce additional complexity, but without it the reciprocal takedown framework risks applying only to the simplest form of intervention, leaving operational gaps in cross-system abuse mitigation that would benefit from early consideration.

7. The URS and UDRP Gap Strengthens the Case for Proactive Abuse Mitigation

Section 9.3 of the TSG Draft acknowledges that it is "not immediately obvious how policies like Uniform Rapid Suspension might work or how the Uniform Dispute Resolution Policy can operate" when registrants rely solely on an alt-name with no standard registrant contact data. This candid assessment identifies a significant gap in the rights protection framework that will govern integrated naming systems.

Noting from the currently published comments, there is support to suggest that registry operator seeking alt-naming-system-primary integration should demonstrate a functioning equivalent to URS and UDRP as a condition of RSEP approval. CleanDNS supports this position. Where traditional dispute resolution mechanisms cannot operate due to the absence of registrant contact information or the pseudonymous nature of blockchain-based identifiers, alternative safeguards must be in place before integration is permitted.

CleanDNS submits that this gap makes proactive, evidence-based abuse reporting and reciprocal takedown mechanisms all the more important to consider. Where traditional dispute resolution cannot operate effectively, a well-defined abuse reporting and takedown pipeline functioning across both naming systems may be the practical alternative, and its requirements are worth identifying at this stage.

8. Consumer Confusion and Unpaired Alt-Names

The TSG Draft itself observes that "few controls exist in the alternative name space to guarantee the uniqueness of a string" and that "alt-names unpaired with DNS-names creates a new area for significant consumer confusion, exploitation, and abuse." CleanDNS agrees with this assessment and considers it one of the most operationally significant findings in the Initial Report.

Unpaired alt-names present a direct and measurable risk of phishing, brand impersonation, and consumer deception. Where an alt-name exists without a corresponding DNS-name, there is no established registrant verification, no WHOIS/RDAP equivalent lookup, and no reliable mechanism for rights holders or abuse

mitigation providers to identify the party responsible for the name. These conditions are precisely those that malicious actors exploit.

This risk reinforces the need for clear standing and defined mechanisms for abuse mitigation providers to action reports across the integrated namespace. Where traditional rights protection mechanisms cannot operate effectively, qualified providers must be able to detect, evidence, and report abuse across both naming systems.

CleanDNS encourages the TSG to consider the consumer confusion risk identified in the Draft as a basis for identifying the abuse mitigation infrastructure that may be needed within any integrated naming system, and to flag this for appropriate policy or contractual treatment.

9. Conclusion and Recommendations

CleanDNS Inc. respectfully urges the TSG to strengthen the final Report by adopting the following four recommendations:

(a) Define a role for qualified third-party abuse mitigation providers within the reciprocal takedown framework established by Sections 8.5 and 8.6. For integration to function, integrated registries should be required to accept and act upon qualified abuse takedown requests from recognized providers, with reciprocal effect across both naming systems.

(b) Require standardized, cross-system abuse reporting infrastructure as a condition of integration with an alternative naming system. No registry operator should be permitted to integrate without demonstrating the availability of a reporting mechanism that spans both the DNS-name and alt-name layers.

(c) Recommending the establish interoperable evidencing standards that enable a takedown action in one naming system to carry verifiable evidence sufficient to support reciprocal action in the other. Without such standards, the reciprocal takedown principle will remain aspirational rather than operational.

(d) Expand the reciprocal action framework to include a structured mapping of disruption mechanisms beyond serverHold and clientHold, addressing sinkholing, NS redirection, and their equivalents or fallback actions within alternative naming systems, so that the full range of operational abuse mitigation tools is accounted for in an integrated namespace.

CleanDNS stands ready to contribute its operational expertise to the development of these mechanisms, including centralized abuse reporting and interoperable evidencing frameworks for DNS and alternative naming systems.

Contact: Jeffrey Bedser, Chris Lewis-Evans, Alan Woods. CleanDNS Inc., https://www.cleandns.com – hello@cleandns[.]com