NTAG Public Comment on “Mitigating the Risk of DNS Namespace Collision”

The NTAG (New TLD Applicant Group), an interest group of the RySG (Registry Stakeholder Group) representing 99 applicants for new TLDs, respectfully presents the following comments about the above mentioned report, a study (currently in draft) contracted by ICANN in order to create the “Namespace Collision Occurrence Framework” as specified in the new gTLD agreements.

Summary

1. We agree that the bar for invoking removal of DNS labels should be established as clear and present danger to human life (C&PDHL) instead of just “harm”.
2. We disagree with the suggested length of 120 days for the controlled interruption period for reasons explained below. In particular, the 120 day period is not sufficiently supported by data or analysis, and does not mirror similar processes either in the domain name space or across other relevant industries.
3. In fact, a similar need in the telecommunication industry typically warrants the use of a transition period lasting up to 60 days, and the operational experience of applicants suggested that no longer than 45 days would be required for DNS infrastructure.
4. NTAG members are doing additional data analysis to determine whether even shorter periods would provide acceptable levels of notice. Additional findings may be provided during the reply period.
5. We welcome the idea of wildcarding the TLD, but disagree with it being mandated as the only available remediation for all yet to be delegated TLDs.
6. We also request that any wildcarding solution be implemented immediately upon signature of the Registry agreement for the particular TLD to allow for the maximum opportunity for third parties to assess unlikely leakages while minimizing the disruption of the Registry’s business model.
7. We ask that wildcarding and alternate path to delegation both be allowed to all registries so that they can select what solutions fits their technical systems and business needs.
8. We agree that the Emergency Back-End Registry Operator (EBERO) should be used instead of de-delegation in extreme cases requiring remediation affecting the resolution of the TLD.
9. We ask that the .home, .corp and .mail decision be addressed in a more comprehensive technical discussion regarding these 3 strings and unapplied-for labels to be possibly used as local DNS spaces.

In-full Comment

We welcome the production of the report, which we found suitable for a framework addressing residual risks involved in delegating new TLDs. It's in every new gTLD applicant best interest that the framework works effectively, in order for isolated cases to not overshadow the introduction of competition, consumer choice and innovation, and we see such effectiveness in the controlled interruption method.

Notably, we wholeheartedly agree with the first finding of the report: **"We [JAS] do not find that the addition of new Top Level Domains (TLDs) fundamentally or significantly increases or changes the risks associated with DNS namespace collisions"**. This conclusion is consistent with the experience of registries that introduced new gTLDs in the 2000 and 2004 rounds, the introduction of IDN ccTLDs, the delegations of recent ccTLDs such as .SX, and the experience of community members that have run end-user networks.

We also agree with two refinements proposed by the report that (1) EBERO (Emergency Back-End Registry Operator) be used instead of de-delegation in extreme cases requiring remediation affecting the resolution of the TLD and (2) that the bar for invoking removal of DNS labels is raised to clear and present danger to human life instead of just "harm".

We do not agree, though, with the period that has been defined to make controlled interruption mandatory. The report authors are on record in ICANN-organized and external events on this topic saying it was largely based on the 120-day certificate revocation period, requested by CA/B Forum due to the large number of .corp internal certificates; we see no connection between such internal business processes of certificate authorities and the day to day operations of real networks. Even taking into account a quarterly period (that would be no more than 92 days in length), it would be too long considering that quarterly processes are likely purely related to reporting functions rather than critical operational components. NTAG has started some data processing activities that could better show operational cycles of real DNS traffic that we hope to provide during the reply period.

Operational experience from applicants, gathered either from running end-user networks or TLD registries that launched in the past few years, indicated that 31 days plus two weeks, totalling 45 days, would be able to provide ample buffer to address any problems.

The only domain industry related period cited was eight days for the ERRP (Expired Registration Recovery Policy), so we would like to offer a reference from the ICT sector: Common Short Codes (CSC) used in the United States Mobile Phone System have a 60-day period from being used by one company before the next one uses it. Considering that the practical effect of a collision in the reuse of a CSC is equivalent to a collision in the DNS from the perspective of an organization, we find it applicable and relevant to defining the DNS equivalent of it.

Finally, we note that there is no reason to wait through the current testing and delegation procedure in order to begin controlled interruption. ICANN could immediately delegate the TLD upon the signing of the registry agreement, either to name servers operated by ICANN solely to provide controlled interruption responses, or to the registry operator's name servers on the condition that only responses required to implement controlled interruption are allowed, much as ICANN limits the addition of names other than nic.TLD to the zone file in the first 120 days after contract signing today.

On the method of implementing the controlled interruption, we welcome the idea of wildcarding the TLD, but disagree with it being mandated for all yet to be delegated TLDs. We note that there are 3 options to implement controlled interruption: (1) wildcarding with no other record besides the wildcard; (2) adding a wildcard record to the TLD but also provisioning SLD labels, provided they are not part of the Alternate Path to Delegation (APD) list and (3) delegating the labels that are in the APD list to wildcarding DNS servers that are different from the DNS servers in the root for that TLD.As wildcarding will not be feasible for all registries, we propose that those 3 implementation options, which actually map to 2 policy options (wildcarding or APD), are all allowed so registries can elect what solutions fits their technical systems and business needs.

We have depicted those 3 options in Annex I of this comment.

Also on the technical side, since DNSSEC is still required despite the wildcard, we note that some back-end DNS publishing systems used by registries do not support DNSSEC wildcards, since wildcarding was prohibited by AGB and the final registry agreement. We also see the possibility of registries not willing to run bleeding-edge versions of DNS server software, which for some DNS code bases is required to have correctly working DNSSEC wildcarding.

We note that some parties mentioned "entropy" referring to collisions with new labels happening every day suggesting a possible lack of effectiveness of the APD. However, the authors of the report identified at least 10, possibly more, algorithmic sources of queries from botnets or similar rogue applications, that easily account for such increases. A look at the APD lists is very revealing of such algorithmic activity, even after removing labels said to be Google Chrome-10 characters requests, and blocking registration of labels so command and control channels of such activities keep operating their abusive purpose, is not positive to the security, stability and resilience mission of ICANN.

In addition to these technical considerations, from a business planning perspective, the proposed draft creates an extra level of uncertainty for undelegated registries as some would only know whether to implement either the APD or wildcard depending on how their contracting and delegation processes proceeded simultaneous to the ICANN Board decision making process.

Moreover, since applying controlled interruption to only those names included in SLD block lists[1] is considered sufficient in the report for registries that have already proceeded through the APD[2], even though some had so-called “collision lists” much longer than TLDs that have yet to be delegated, there seems to be no compelling technical reason to enforce a higher standard upon subsequent TLDs. As a matter of equality and fairness the same option should still available for TLDs no matter the delegation date.

Keeping APD as an option would not preclude willing registries to choose wildcarding. For some technical implementations, wildcarding may actually be simpler and scale better, and the NTAG does not want this option to be removed from the framework.

Lastly, we note that although the draft report recommends that .mail, .home and .corp are permanently reserved, the reservation of TLDs for specific purposes is a function that has generally fallen to the IETF.[3] Although we believe more discussion is needed on whether to permanently reserve these particular TLDs versus creating a new namespace for internal use, we suggest that ICANN engages in the IETF process co-authoring a BCP-track RFC, adding ICANN authority over the name space with expertise from IETF community. ICANN can continue to hold applications for these three strings, although applicants who elect to do so should be given the opportunity to withdraw for a full refund.

Sincerely,
NTAG

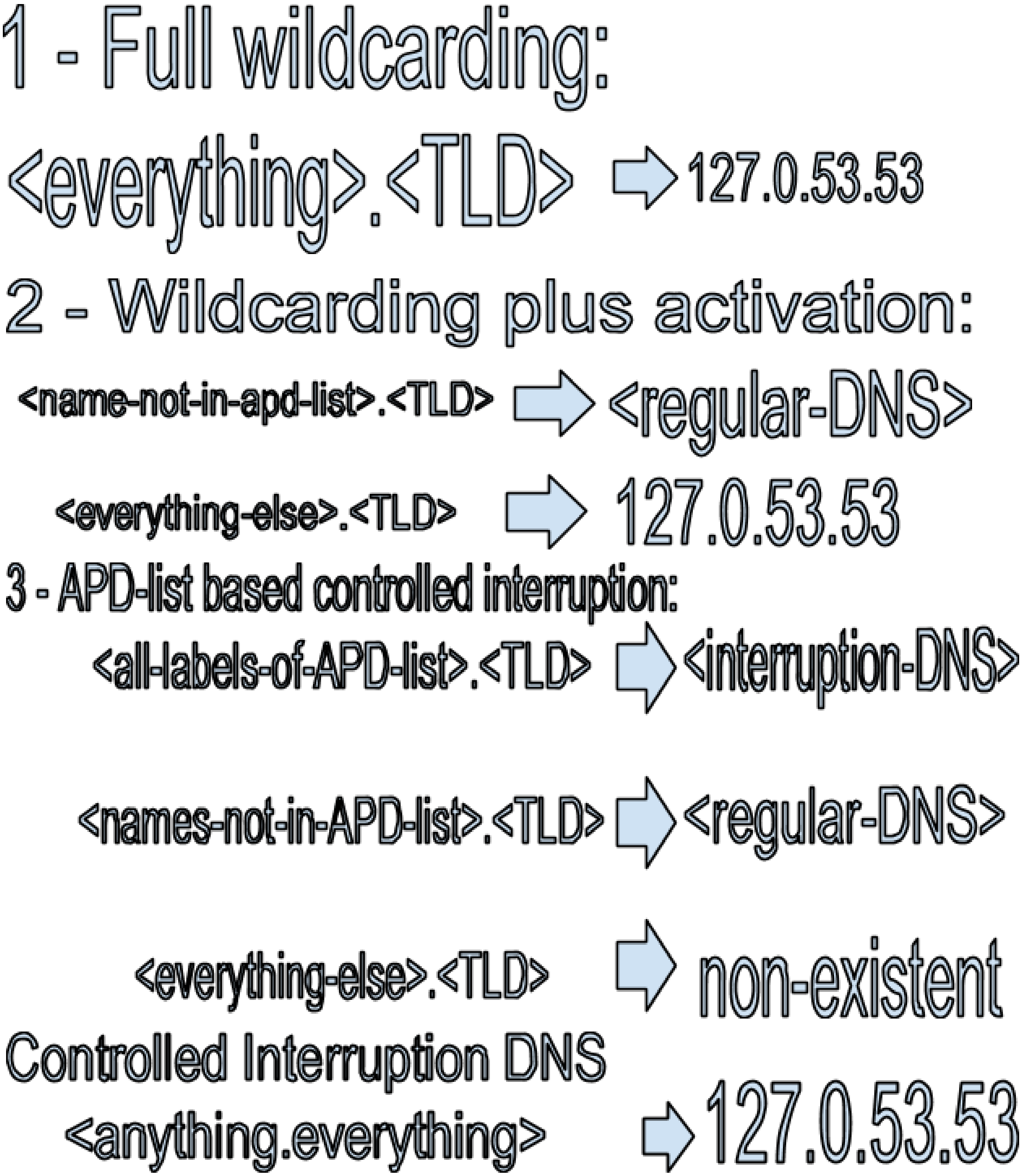
Member support level: This comment has received thorough support and input from across the NTAG; none of the 99 NTAG members have opposed this comment.

[1] created following NGPC decision of October 8th 2013, see https://www.icann.org/en/news/announcements/announcement-08oct13-en.htm

[2] Delegated registries are not being ordered to add wildcards or remove currently delegated DNS labels.

[3] See, in particular, RFCs 2606 and 6761, both of which identify TLDs reserved for specific purposes.

Annex I: Three ways of implementing controlled-interruption



1 - Full wildcarding:

<everything>.<TLD> → 127.0.53.53

2 - Wildcarding plus activation:

<name-not-in-apd-list>.<TLD> → <regular-DNS>

<everything-else>.<TLD> → 127.0.53.53

3 - APD-list based controlled interruption:

<all-labels-of-APD-list>.<TLD> → <interruption-DNS>

<names-not-in-APD-list>.<TLD> → <regular-DNS>

<everything-else>.<TLD> → non-existent

Controlled Interruption DNS

<anything.everything> → 127.0.53.53