17 September, 2013

742 Ocean Club Place
Fernandina Beach, FL 32034

Mr. Cherine Chalaby
New gTLD Program Committee
Internet Corporation for Assigned Names and Numbers
Los Angeles, CA 90094

Re: Name Collision Public Comment, Response

Dear ICANN Board and Staff,

We are writing this in response to our own initial comment to the Name Collision Public Comment Period, submitted on August 26th. Since that time we have endeavored to obtain specific DITL information on .wiki, which was held back from contracting despite its priority at #181 due to its inclusion within the tail end of the 20% "Undetermined Risk" category. We were able to obtain information on .wiki query results thanks to our backend registry provider being a member of DNS-OARC, and while we will present and analyze this information and prove that .wiki is safe to delegate, we would also like to cover a number of other relevant topics within this discussion and how ICANN has framed it thus far. This includes halting contracting for the 20%; the financial onus unfairly placed on applicants by ICANN's current investigation and mitigation tactics; and the inefficient 120 day warning process between contracted applicants and the CA/Browser Forum.

Overall, the NGPC must plot a clear path forward, cognizant of the fact that there is currently no consensus as to: a.) What security and zone statistics demonstrate a legitimate security risk; b.) How and why these security risks are different than any other previously delegated TLDs; c.) If the current ICANN proposal of further research for 20% of applicants extrapolated from the 2013 DITL data reflects these risks and if not how this can be remedied; d.) What type of information needs to be researched in greater depth e.) How ICANN and applicants can facilitate any necessary research; f.) Why this process must or should take 3 - 6 months; g.) The process by which applicants will be removed from the current 20% freeze and allowed to continue with contracting and delegation.

We believe that the NTAG letters, submitted on August 15 and September 17, answer these questions and plot a way forward. NTAG frames the conversation well, noting that the query rates behind supposed risks are not nearly as pronounced as they were for recently delegated TLDs, which had no mitigation plans in place and experienced no publicized security issues. NTAG goes on to suggest mitigations that exceed what could be considered reasonable safety precautions, which demonstrate our collective interest in implementing new TLDs in a safe and timely manner. We strongly support the NTAG approach.

Halting the 20%

We were notified that .wiki would be halted in the contracting process some 7 hours before the close of the first public comment period on Name Collision. This is absolutely unacceptable. ICANN staff chose to create an arbitrary 20% of "Undetermined Risk" from the Interisle report, which was still being categorically refuted within the Public Comment Period as a group for concern, when ICANN staff then chose to halt contracting for these 20%. This is unacceptable because it shows a clear disregard for the multistakeholder process, especially when ICANN's Krista Papac instructed us during the joint RySG/NTAG call on August 28th that the Public Comment period was the only means of providing constructive feedback to move beyond the Name Collision issue. For ICANN Staff to claim that the Public Comments period is being listened to, and then to make a drastic processing decision related to their own initial reading of the Interisle report without even waiting for the public comment period to close, is wrong. It cannot be stressed enough that the 20% is an arbitrary category, and it is especially noteworthy that the 20% comes from the 2013 DITL data, not the 2012 or earlier. It has been recognized across the community, including by ICANN CSO Jeff Moss at a TLD Security Event in San Francisco held on August 22nd, that the 2013 DITL data may have been influenced by ICANN publishing the list of applied for strings on "Reveal Day." It remains unclear whether the query data was affected by individuals typing the new, publicized TLD extensions into their browsers and search engines to see if they were able to resolve yet.

.wiki is #181 in the ICANN implementation queue and as of writing #362 has signed a Registry Agreement with ICANN. Our priority number has been irrevocably disregarded due to the arbitrary creation of a 20% "Unknown Risk" category based off of potentially flawed 2013 DITL data and the subsequent staff approach of halting those 20% with no clear path to absolution. The halting of the 20% was an unnecessary step considering the fact that ICANN reserves the unilateral right to amend these contracts, so any repercussions from further investigation into Name Collision could, and still can be, provided for in individual registry agreements after the fact.

We ask ICANN's NGPC to immediately revoke the freeze of the 20% and to prioritize accordingly, in line with the original priority draw numbers. This can and should be handled holistically, with reconsideration of the entire 20% category, especially its reliance on the 2013 DITL information.

ICANN Creates Demand for Costly Zone Analysis

An important repercussion to note from ICANN's creation of the 20% "Undetermined Risk" category is that many applicants are now turning to Interisle and other firms to have their proposed TLD's zone file analyzed. While Interisle should be applauded for its quick work and neutral stance in the Name Collision report, it is troubling that many applicants now feel confined to pay tens of thousands of dollars to have Interisle or a similar firm provide them with TLD specific data. It is especially unfortunate that this is the case for applicants on the 20% list created from the 2013 DITL data, which we will continue to insist is potentially corrupted and should not be used for any further investigation or mitigation.

We appreciate the difficulty of the situation and all applicants' vested interests in bringing about secure TLD namespaces, however, ICANN has handled this haphazardly at best and it seems that following the ruling of the NGPC, applicants themselves may be financially responsible to prove the safety of their proposed namespaces. Given our distrust of the 2013 DITL data we reject any decision that acts on the 2013 data to create further cost burdens for applicants. Any costs related to name collision investigation and mitigation cannot be based off of potentially corrupted data.

Enhanced Outreach to CA/Browser Forum

We believe that ICANN's current plan of outreach to the CA/Browser forum is ineffective and could be made more efficient and result in cleaner timelines, to the benefit of all.

ICANN should disregard its suggested outreach strategy that relies on a separate 120 day waiting period for every TLD, as it is redundant. Instead, ICANN should *immediately* provide the CA/Browser Forum a comprehensive list of every TLD that has passed Initial Evaluation, and is therefore likely to delegate. A confirmation period can be facilitated whereby the newly contracted applicant communicates its launch schedule to the CA/Browser Forum, which according to ICANN rules, *must* include a 30 day sunrise warning and 30 day sunrise period; this 60 day period prior will see no delegation of any SLDs and it will be a sufficient timeframe for the CA/Browser Forum to note the confirmation of delegation and plan accordingly.

We note that the 120 day period was designed specifically with .corp in mind, which has been roundly recognized as a unique case, and as such, it should not be made the base for every TLD, which all have significantly fewer internal certificates issued.

Overview of Zone Analysis

While we are applicants for 9 TLDs, and we want to see any security risks quickly and thoroughly addressed for all TLDs, we will focus specifically on our own prospective .wiki. This is due to the aforementioned fact that .wiki, an uncontested TLD with the priority #181, was halted due to the freeze put on the entire 20% of “Undetermined Risk” strings.

This section explores a number of specific remedies for .wiki; we submit this specific case as further corroboration that the NTAG’s mitigation plan will work, and as a commitment that we are ready to go above and beyond for our specific TLD. However, while we are prepared to go above and beyond via these mitigation tactics, the extent to which the supposed security risks are being over dramatized must be revisited. The NTAG correctly notes in its August 15th Public Comment that ALL applied for new TLDs, other than .home and .corp, represent a combined 0.016% of the total query rate in the 2012 DITL data provided by Interisle. This figure and the potential reasons that these queries are taking place simply do not warrant mitigation through a 3 - 6 month delay. We note the NTAG letter clearly demonstrates that .sx was delegated in 2012 with a higher NXDOMAIN query rate than all but five of the currently applied for TLDs. There is simply no precedent nor valid rationale for this type of widespread delay and we implore the NGPC to thoroughly consider the NTAG’s guidance when they define the outstanding questions surrounding what constitutes a security risk and why; what must be analyzed in greater depth and how; and how applicants can proceed beyond these issues.

.wiki Zone Analysis

We have attached, “Wiki Collision Analysis.pdf,” to the Public Forum post, which specifies the exact SLD that is being queried at the root that could cause the potential for name collision and the total number of queries. CentralNic extracted this data from the 2012 “Day In the Life” data provided by DNS-OARC.[1] We have grouped the query types into four main groups: 1 or 2 character names (24.53% of total); Blocked Names (24.51%); Random Noise (22.02%); and Invalid Names (2.15%). The remaining 26.79% of queries are spread across individual SLDs, the highest-queried being “rdr” at 771 queries.

1 or 2 Character Names (24.53%)

We can first note that 1 or 2 character names are automatically withheld and their release is dependent on petitioning ICANN. We note that without ICANN approval they will remain blocked and not resolve as SLDs. While we reserve the right to petition ICANN to release these domains, we assume doing so will involve further security checks at that time.

Blocked Names (24.51%)

Our self-imposed Blocked Names group is made up of 10 SLDs that make up nearly a quarter of the queries analyzed. We propose to block and further study all 10 of these SLDs. We note that “example” is already blocked under ICANN rules and that “com”, “org” and “wpad” are all suggested for blocking as per the NTAG’s September 17 letter. The remaining 6 SLDs are internal additions to the process suggested by NTAG, whereby delegation of the SLD in question would need to follow a RSEP process. The 10 SLDs are:

1. example
2. www
3. org
4. com
5. wpad
6. localhost

[1] While DNS-OARC provided the raw data, the analysis was carried out by CentralNic and DNS-OARC takes no position with respect to the results of this analysis.

7. net
8. local
9. wwww
10. dev

Random Noise (22.02%)

Most TLD operators see periodic spikes of DNS queries (mainly MX queries) for seemingly randomly-generated domain names. The best guess of the source of these names is that they are a side-effect of a widely deployed "spam fighting" program which attempts to pollute the databases of email addresses used by spammers, by generating web pages containing million of random email addresses. These addresses are then harvested by web spiders and added to databases of email addresses.

However, the economics of spam are such that spammers simply ignore this pollution rather than clean their databases, so when a spammer sends out an email (typically using a botnet), the affected TLD operators see large volumes of unique queries (i.e., each name only receives a single query). This pattern was observed in the DITL dataset, and presuming that the above theory holds true for the queries seen in the dataset, these can be discounted as a security and stability risk.

Names were assigned into this category by means of an n-gram analysis.[2] The implementation used provided a confidence level associated with any language detected: any string with a confidence level below 12.5% was added to this category. This is a conservative threshold chosen to eliminate false positives and ensure that human-meaningful names were not incorrectly categorized as noise.

Invalid Names (2.15%)

[2] see, http://en.wikipedia.org/wiki/N-gram

These are names that contravene RFC 1035, section 2.3.1. For the most part, these are names with underscores that are used for service discovery (i.e., SRV records). As these names will never resolve once .wiki is delegated, they also represent no risk.

Remaining Names (26.79%)

All remaining SLD queries do not represent a significant query rate where Name Collision can be considered to be a widespread risk to the TLD as a whole. As noted, the most queried of these names only resulted in 771 total queries.

Moving Forward

We are aware of the mitigations presented in the NTAG's Second Public Comment on this issue, submitted on September 17th. We believe that their path forward is the most comprehensive, and you'll note that our suggested mitigations, including the blocking of 10 SLDs that resulted in 26.79% of the total query volume, go above and beyond the precedent that the NTAG has set.

We expect the NGPC to quickly and judiciously plot a way forward for the applicants that have been held from contracting processes due to inclusion in the "Undetermined Risk" category. It is fair to say that we now have determined the risk, which is limited to nonexistent.

Respectfully Yours,

/s/

Andrew Merriam
Business Development Coordinator
Top Level Design, LLC
andrew@tldesign.co
505.238.9166