BRIEFING ON NAME COLLISION RISK FOR NEW TLDS

1. BACKGROUND

ICANN's mission and core values call for ICANN to preserve and enhance the operational stability, reliability, security, and global interoperability of the Internet's system of unique identifiers (names, IP numbers and protocol parameters). In pursuing these goals and following the direction of its Board of Directors as well as taking into consideration the advice of the Security and Stability Advisory Committee, ICANN has been working on understanding and mitigating the issues related to name collisions in the DNS.

A name collision on new TLDs occurs when users unknowingly access a name that has been delegated in the public DNS when the user's intent was to access a resource identified by the same name in a private network. Circumstances like these, where the administrative boundaries of private and public namespaces overlap and name resolution yields unintended results, present concerns and should be avoided. However, the main concern is whether such collisions cause unexpected behavior or harm, the nature of the unexpected behavior or harm and the severity of consequence.

ICANN commissioned a study (http://www.icann.org/en/about/staff/security/ssr/name-collision-02aug13-en.pdf) on the potential security impacts of the applied-for new-gTLD strings (the "Study"). The Study considered whether name collisions might occur between applied-for new gTLD strings and domain names that may be in use in private namespaces ("non-delegated TLDs"). The Study also reviewed the possibility of name collision occurrences arising from the use of internal names for which X.509 digital certificates have been issued.

On 5 August 2013, ICANN published and made available the Study, which proposed categories of strings according to the occurrences of queries, as observed in root server log samples obtained from the "Day in the Life of the Internet" (DITL) initiative from DNS-OARC. The Study used as input: 1) samples of DNS requests transmitted to root servers (from the DITL initiative), complemented with 2) information from Certificate Authorities regarding the issuance of internal name certificates (e.g., TLS/SSL certificates for non-delegated names). A full description of the methodology of the Study can be found in section 3.4 of the Study.

Based on the Study, ICANN staff published a proposal to manage the risk of name collision for public comment from 5 August to 17 September 2013 (http://www.icann.org/en/about/staff/security/ssr/new-gtld-collision-mitigation-05aug13-en.pdf).

2. NEW GTLD COLLISION OCCURRENCE MANAGEMENT PLAN

On 7 October 2013, the Board New gTLD Program Committee adopted the New gTLD Collision Occurrence Management Plan (http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-07oct13-en.htm) (the "Plan"). The Plan is an updated version of the proposal that went for public comment on 5 August incorporating the input received.

The Plan identifies two strings, *home* and *corp*, that will likely cause problems if delegated (see section 6 of the Study), given their high frequency of occurrence in the 2012 and 2013 DITL data (an order of magnitude higher than the next most frequently occurring string). The Study identifies these strings as having a level of queries in the realm of heavily used TLDs. Both strings are also widely used in private namespaces within internal networks (for example, see Appendix G of RFC 6762, http://tools.ietf.org/html/rfc6762). Additionally, *corp* is identified as the string with the highest number of internal name certificates (see Appendix C of the Study).

Based on the analysis of frequency of occurrence and the perceived severity of impact, ICANN decided to defer delegating *home* and *corp* indefinitely, and agreed to collaborate with the technical and security community to continue to study the issues presented by these strings.

A core feature of the Plan includes undertaking additional study to develop a Name Collision Occurrence Management Framework (the "Framework") in cooperation with the community. The Framework is expected to include appropriate parameters and processes to assess both probability and severity of harm resulting from the occurrence of name collisions. The Framework will specify a set of collision occurrence assessments and corresponding mitigation measures (if any) that ICANN or TLD applicants may need to implement per second level domain name (SLD).

The Plan provides a new gTLD registry operator with the option to proceed to delegation prior to receiving its SLD collision occurrence assessment report (subject to established processes and procedures). If the registry operator chooses this *alternative path to delegation*, it must initially block *all* SLDs that appear in the DITL and other related datasets while the assessment is conducted.

An additional feature of the Plan includes a process to enable an affected party to report and request the blocking of a SLD that causes demonstrably severe harm as a consequence of name collision occurrences. This process is intended to mitigate the risk that collision occurrences not observed in the study dataset could have severe impact.

Lastly, the Plan describes an outreach campaign targeted to potentially affected parties to help them identify and manage the root cause of name collision occurrences in their networks, e.g., the use of name not rooted in the public DNS and/or the use of short unqualified names meant to be autocompleted by search lists. As part of the outreach campaign, ICANN is collaborating with other parties and members of the community that share the same interest in making progress in this issue.

3. CURRENT STATUS

ICANN has taken a number of steps over the past several months to continue to address name collisions. A mechanism to report name collision issues for affected parties has been implemented by ICANN (http://www.icann.org/en/help/name-collision/report-problems).

On 21 November 2013 the Board directed staff to develop a long-term plan to manage name collision at the root, and to work with the community to develop a long-term plan to retain and measure root-server data (http://www.icann.org/en/groups/board/documents/resolutions-21nov13-en.htm#2.d).

On 6 December 2013, ICANN published the "Guide to Name Collision Identification and Mitigation for IT Professionals" (http://www.icann.org/en/help/name-collision/mitigation). The Guide lists some of the risks related to name collision and specifies best practices for IT departments on how to manage the risks. The Guide is targeted to enterprise IT departments since they have the ability to effect the changes needed to fix the root cause of name collisions, i.e., the use of private namespaces that leak queries to the public DNS.

ICANN also launched an outreach campaign to raise awareness and help enterprises react, along with an information hub page (http://www.icann.org/namecollision). The informative materials have been translated and published in Arabic, Chinese, French, Spanish, Russian, and Portuguese.

Per the New gTLD Collision Occurrence Management Plan, a Name Collision Occurrence Management Framework is currently being developed as the long-term tool to address name collision risk for new gTLDs. Discussions with community are ongoing in a public mailing list (https://lists.dns-oarc.net/mailman/listinfo/collisions). A draft version of the Framework is expected in February 2014. The draft version will be published for public comment.

4. NEXT STEPS

Once the draft Framework undergoes public comment, and is updated to reflect input from the community; it is expected to be considered by the ICANN Board. The final Name Collision Occurrence Management Framework is expected to be applied to all new gTLDs that request delegation.

The issue of name collision is not unique of new gTLDs and could present in new ccTLDs too, both ASCII and IDN. ICANN is requesting the ccNSO to review the name collision issue and its implications for new ccTLDs. ICANN looks forward to collaborate with the ccNSO on the matter and is available to help and answer any questions that may arise.

Until advice is received from the ccNSO, ICANN plans to send each new ccTLD manager the same kind of interim report that new gTLDs received for the alternate path to delegation. It will remain the responsibility of the local Internet Community and the ccTLD manager to either: 1) proceed to delegation while temporarily blocking the SLDs identified in the report; 2) temporarily defer delegation until receipt of their full collision occurrence assessment and implementation of the measures described; or 3) some other course of action determined by the local Internet Community and the ccTLD manager.

ICANN's mission and core values call to preserve and enhance the operational stability, reliability, security, and global interoperability of the Internet's system of unique identifiers (names, IP numbers and protocol parameters). ICANN is fully committed to the delegation of new TLDs in accordance with its mission and core values. ICANN appreciates ccNSO consideration of this issue and further collaboration on the remaining work.