ICANN

The Internet Corporation for Assigned Names and Numbers

9 October 2013

Heather Dryden
Chair, Governmental Advisory Committee

Re: Written Briefing on Dotless Domains and Internal Names Certificates

Dear Heather,

The purpose of this letter is to follow up on the commitment made by the New gTLD Program Committee to provide a written briefing to the GAC regarding SSAC's advice on Dotless Domains and Internal Names Certificates.

Background

In the Durban Communiqué, the GAC stated:

a. The GAC shares the security and stability concerns expressed by the SSAC regarding Internal Name Certificates and Dotless Domains. The GAC requests the ICANN Board to provide a written briefing about:
    i. how ICANN considers this SSAC advice with a view to implementation as soon as possible. The GAC believes that all such stability and security analysis should be made publicly available prior to the delegation of new gTLDS.
    ii. **The GAC Advises the ICANN Board to:**
        a. As a matter of urgency consider the recommendations contained in the SSAC Report on Dotless Domains (SAC053) and Internal Name Certificates (SAC057).

In its initial response of 10 September 2013, the NGPC indicated:

> The NGPC will provide a written briefing regarding how ICANN considers this SSAC advice with a view to implementation as soon as possible. The NGPC agrees with the GAC that all such stability and security analysis should be made publicly available prior to the delegation of new gTLDS. The NGPC notes the publication of the "Name Collision in The DNS" Study" and the "Dotless Domain Name Security and Stability Study Report."

The following is intended to respond to the GAC's request for a written briefing on Dotless Domains and Internal Name Certificates. We also describe ICANN's plans to implement the SSAC's advice on these subjects.

Dotless Domains

At its meeting on 13 August 2013, the ICANN Board New gTLD Program Committee (NGPC) adopted a resolution affirming that "dotless domain names" are prohibited. Dotless domain names are those that consist of a single label (e.g., http://***example***, or mail@***example*)**. Dotless names would require the inclusion of, for example, an A, AAAA, or MX, record in the apex of a TLD zone in the DNS (i.e., the record relates to the TLD-string itself).
In addition to public comments on dotless domain names, the NGPC considered the security and stability risks associated with dotless domain names highlighted in the following papers:

- On 23 February 2012, the ICANN Security and Stability Advisory Committee (SSAC) published SAC 053: SSAC Report on Dotless Domains. In this report, the SSAC stated that dotless domains would not be universally reachable and recommended strongly against their use. As a result, the SSAC recommended that the use of DNS resource records such as A, AAAA, and MX in the apex of a Top-Level Domain (TLD) should be contractually prohibited where appropriate, and strongly discouraged in all cases.

- On 10 July 2013 the Internet Architecture Board (IAB) released a statement on dotless domain names, recommending against the use of dotless domain names for TLDs.

- On 29 July 2013 Carve Systems delivered a report on dotless domain names, which was commissioned by ICANN. Consistent with the SSAC report, Carve's report on dotless domain names identifies security and stability issues.

When adopting its resolution, the NGPC considered the security and stability risks identified in these papers, as well as the impracticality of mitigating these risks. Based on the NGPC resolution, ICANN does not plan to pursue any additional studies on the subject.

Internal Names Certificates and Name Collisions

A name collision occurs when Internet users unknowingly access a name that has been delegated in the public DNS when the user's intent was to access a resource 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 if possible. However, the collision itself is not the concern but whether such collision occurrences cause unexpected behavior or harm, the nature of the unexpected behavior or harm and the severity of consequence.

In November 2012, the ICANN Security and Stability Advisory Committee (SSAC) became aware of an issue regarding the handling of non-delegated TLDs in X.509 digital certificates (e.g., those used for SSL/TLS) by Certificate Authorities (CAs) who issue them. On 15 March 2013, the SSAC published SAC 057: SSAC Advisory on Internal Name Certificates, which advised the ICANN Board to take immediate steps to mitigate the risks associated with the handling of non-delegated TLDs in X.509 digital certificates, and noted that this could impact the new gTLD Program.
At its 18 May 2013 meeting, the ICANN Board adopted a resolution directing the President and CEO, in consultation with the SSAC, to commission a study to identify the level of potential impact posed by each applied-for new gTLD string with respect to the 120-day certificate vulnerability window and the general concern regarding the use of non-delegated TLDs. (http://www.icann.org/en/groups/board/documents/resolutions-18may13-en.htm#2.a).

The study, "Name Collision in the DNS," together with a proposal to manage the risks identified in the Study was published for public comment from 5 August to 17 September. During the public comment period, 75 comments were received, and based on the public comments, staff updated the proposal to manage the risks identified in the Study.

The following describes the plan to manage the collision occurrences between new gTLDs and existing private uses of the same strings. It has been updated in response to community feedback during the public comment forum. A core feature of the updated plan includes undertaking additional study to develop a name collision occurrence management framework. The framework will include appropriate parameters and processes to assess both probability and severity of harm resulting from the occurrence of name collisions.
Examples of the parameters might include number of DNS requests, type of DNS requests, type of queries, diversity of query source and appearances in internal name certificates. 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) seen in the "day in the life of the Internet" (DITL) dataset.

The plan provides a 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 dataset while the assessment is conducted.
An additional feature of the Proposal recommends a process to enable an affected party(ies) 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.

The plan includes a targeted outreach campaign to potentially affected parties to help them identify and manage the origins (causes) of name collision occurrences in their networks. As part of the outreach campaign, ICANN will invite and collaborate with other parties and members of the community that share the same interest in making progress in this issue.

Finally, at its 7 October 2013 meeting, the NGPC made a series of recommendations to the ICANN Board concerning name collisions. The NGPC recommended that the ICANN Board: (1) request that the ICANN Board Risk Committee expressly reviews this matter and reports back to the Board, and continues to review and report at regular intervals; (2) direct the ICANN President and CEO to develop a long-term plan to manage name collision at the root; and (3) direct the ICANN President and CEO to work with the community to develop a long-term plan to retain and measure root-server data.

The full details of the plan are available here and the NGPC's resolution is available here.

I hope that you find the above responsive to the GAC's request for a written briefing on dotless domains and internal name certificates and that it addresses the GAC's advice on these subjects.

Best regards,

Stephen D. Crocker
Chair, ICANN Board of Directors