Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

December 15, 2008

VIA EMAIL

Mr. Peter Dengate Thrush
Chairman of the Board of Directors
Dr. Paul Twomey
President and CEO
ICANN
4676 Admiralty Way, Suite 330
Marina del Ray, CA 90292

Re: Comments of Microsoft Corporation on Technical Considerations Related to the Introduction of new gTLDs

Dear Mr. Dengate Thrush and Dr. Twomey:

Microsoft Corporation ("Microsoft") wishes to take the opportunity of public comment on the new gTLD Draft Application Guidebook ("DAG") to provide to ICANN its comments on the technical considerations related to the introduction of new gTLDs. Microsoft has submitted separate comments to ICANN on the DAG.

Microsoft is a worldwide leader in the IT industry, with a mission to enable people and businesses throughout the world to realize their full potential. Since the company was founded in 1975, it has worked to achieve this mission by creating technology that transforms the way people work, play, and communicate. Microsoft is also an owner and champion of intellectual property rights. It maintains sizable trademark and domain name portfolios and takes pride in the worldwide recognition of multiple of its trademarks. Further, Microsoft's businesses rely heavily on the Internet and the current system of top level domains, and Microsoft is an ICANN-accredited registrar. As such, Microsoft is well positioned to provide meaningful comments to ICANN on the technical considerations related to the introduction of new gTLDs.

The comments below identify several areas in which deployment of new gTLDs seem likely to result in technical issues.

User Experience with Flat Names (often called single label names).

Organizations frequently have multiple name services in operation on their computer networks. In home networks it is interesting to note that the global DNS is frequently used for resources outside the home network, but the resources on the home network are commonly not named in the DNS. It is common that the namespace for intra-organizational resources (e.g. personal computers, servers, printers, fileservers, etc.) are named with flat label names such as "LaserPrinter", "FileServer1", etc. Microsoft has used NetBIOS (RFC 1001, RFC 1002) as a flat namespace for a long time, but it should be noted that in the most recent releases of the Windows OS it is not necessary to use NetBIOS naming. However, NetBIOS is broadly deployed and used in Business and Home networks since earlier versions of Microsoft systems uses NetBIOS. Since NetBIOS is well documented and understood, it is also used by a wide number of non-Microsoft systems such as Apple, Samba, small Network Attached Storage devices from Buffalo, Linksys, D-Link, most network-capable printers, etc. As systems and applications started to incorporate the DNS in the 1990s, developers merged the use of flat names like NetBIOS and the DNS to allow for interoperation of old and new systems. As an example of this merging, in a web browser like Internet Explorer one can enter http://www.icann.org to reference an Internet resource, OR one can enter http://Finance to access and view an Intranet web server. In these examples the name "www.icann.org" is resolved by using the DNS, whereas the name "Finance" is resolved by using the NetBIOS name service. As part of simultaneous use of multiple namespaces it is common that heuristics were built into applications and systems to determine which name service should be used.

For example, some networked applications and systems look for BNF style patterns in names such as:

<hostname label>.<3 letter label> (e.g. example.com) or

<hostname label>.<2 or 3 letter label>.<2 letter label> (e.g. example.co.jp)

to find DNS names, and make decisions on how to use these names. Single label names are routinely considered to be "Intranet" and may be handled in a separate manner from an Internet experience. Names that are not matched by the Internet patterns can be interpreted as non-Internet in nature.

Given the public discussion of new gTLDs, Microsoft has heard from some customers that are concerned that they will get a gTLD for their company_name, yet http://company_name will not get handled in the same ways as http://company_name.COM, or http://company_name.co.<country code> . Large scale deployment of new gTLDs runs the risk of significant confusion in the existing user base and unmet expectations in organizations that acquire new gTLDs.

A second concern is the changing of routing of web requests: today http://somename will in general be routed so as to be kept internal to an organization's network. If "somenameX" were to become a gTLD and if an intranet user mistyped http://somename as

http://somenameX then a new form of decision will need to made about routing the web request, potentially leading to information disclosure. Any potential changes to related software, services and deployments should be evaluated against the issues called out in this section.

Hosting Services in new gTLDs.

In http://www.icann.org/en/topics/new-gtlds/reserved-names-24oct08-en.pdf ICANN is requiring second level reservations for WWW, NIC, WHOIS. We recommend that ICANN be more strict and require that ALL second level names in a new gTLD should be limited to namespace delegations, and that common Internet service names should be reserved and not delegated. This would be in keeping with existing gTLDs. Following the existing common pattern in the Internet increases the likelihood that existing software and services will operate as expected. Over time the Internet should develop a canonical naming for so that the use of www.example.com can be augmented with www.<canonical label>.example (e.g. www.info.example, where info is the canonical label).

DNS Heuristics in Web Based Sub-Systems

Web based sub-systems using DNS heuristics may fail to operate well with new gTLDs. Much like user experience code for namespace handling detailed above, there are non-UX subsystems that use DNS names that may not adequately handle several forms of new gTLDs. It appears there are several systems that handle http cookies in a manner that depend on the current patterns of DNS namespace structure and do similar matching for the existing pattern for current gTLDs. At this stage Microsoft hasn't completed the evaluation on the extent of these issues or the resulting impact(s), but it is possible that the extent of these issues is beyond what is documented here.

Intranet certificates.

Several networks incrementally secure their intranet websites using "intranet certificates". A website on the Internet has a common name in the certificate (CN) that is the fully qualified DNS name (FQDN) (e.g. CN=www.example.com). For intranet websites the market has developed intranet certificates sold by the same certificate authorities that are in browsers' trust stores. The CN in an intranet cert is usually a single label, such as CN=myEXAMPLE. This allows a browser accessing the website https://myEXAMPLE to authenticate with SSL that the website is indeed https://myEXAMPLE. If myEXAMPLE becomes a gTLD, then there is the possibility that a trust chain for https://myEXAMPLE can be established that runs through an intranet cert instead of an Internet cert owned by the owners of the gTLD myEXAMPLE. Intranet certs have been around and sold by top level certificate authorities for over 5 years. (e.g. https://secure.instantssl.com/products/SSLIdASignup1a). It is interesting to note that the same single label (e.g. "myEXAMPLE") can be used by multiple organizations and thus there can be multiple intranet certificates with the same CN, each cert with a separate serial number and ownership fields in the cert.

Discussion

It can be observed that many of these issues stem from the externalities, yet realities, of using flat names (e.g. example) instead of fully qualified DNS names (e.g. user@mail.example.com, www.example.com, etc.). Unfortunately, new DNS gTLDs are a substantial change to the system, and to some extent a lot of software is "gated" in its use by the existing shape of gTLDs in the DNS that have not changed for years. In some cases this is not due to gTLDs specifically, it is due to the desire of many organizations and consumers to come up with "short cut naming for commonly accesses resources: e.g. move from using http://www.example.branch.corp.organization.com to http://www.example. What this illustrates is that the canonical form of names may change, and as a result the existing methods for handling DNS names may not work as expected.

ICANN should consider a staged and incremental deployment of new non-CC gTLDs, where staging would take an extensive period of time (not less than a year). The purpose of a slow and incremental deployment is to get adequate testing and experience, and to allow for ALL stakeholders of the Internet and DNS to adjust. We expect some network administrators will need to make changes to their firewalls and proxies, DNS servers, email servers, perhaps email clients, and other infrastructure that is active in using DNS. In some cases, new software may have to be developed or newer versions of existing software deployed. To get adequate testing coverage an early deployment of several gTLDs for names that are already in common use on the Internet would prove very valuable. That way millions, potentially tens of millions, of users would test them prior to broad deployment of a large number of new forms of DNS names rooted in new gTLDs. For example, "ietf", "icann", "isoc", "itu" , or perhaps the names of some large well known and heavily trafficked organizations (e.g. "icq", "bbc") would be appropriate to validate the interaction with a broad set of software and systems. The expansion of the DNS from what it has been for decades should be taken with extensive real operational testing prior to going fully online with substantial numbers of new gTLDs.

* * *

In conclusion, Microsoft urges ICANN to consider and test fully the technical considerations related to the introduction of new gTLDs. ICANN's failure to do so runs the risk of user confusion and inconsistent system operation.

Microsoft staff is available for further discussion of these issues with ICANN.

Thank you for your consideration. If you have questions or wish to discuss any of the points raised herein, please contact Anoop Gupta (anoop@microsoft.com) or Peter Ford (peterf@microsoft.com).

Respectfully submitted,

Microsoft Corporation

Anoop Gupta
Corporate Vice President

Peter Ford
Lead Architect, Networking

cc: Dr. Steve Crocker, Chair
ICANN Security and Stability Advisory Committee