SSAC Report SAC009
Alternative TLD Name Systems and Roots: Conflict, Control and Consequences

SSAC
ICANN Security and Stability
Advisory Committee

A Report from the ICANN
Security and Stability
Advisory Committee
(SSAC)
March 2006

Executive Summary

In this report, SSAC considers conditions and factors that could accelerate fragmentation, destabilize root name service and alter the existing name system management framework to a much greater degree than pure for-profit initiatives. In the report, SSAC presents a rudimentary classification of alternative root name server systems and alternative TLD name system administrators. For each class, we attempt to identify the stated or implied incentives for operating an alternative root name service and managing alternative TLDs. We describe the operational model and the technical mechanisms each class of operators employs to provide name resolution and registration services. We then consider the impact on Internet users and service providers (ISPs), domain name registrants, and registries that operate under agreements with ICANN.

This report intentionally examines alternative root server systems and alternative TLD name system administrators *generically*, i.e., according to the characteristics SSAC associates with a class of operator rather than by the characteristics of individual operators. By elevating our examination to this level, we can focus on the common characteristics of each class of operator, and perhaps more accurately assess whether TLD name system administration and root name service operation of a given class create security and stability issues.

The Committee offers these findings and recommendations in the spirit of open review, comment and evaluation, with the expectation that they will be considered carefully before they result in action.

Finding (1): SSAC can find little evidence to support claims that alternative TLD name systems have or will attract a significant market share to fragment the root. Registrants who register names in alternative TLD name systems may encounter barriers to an estimated two trillion dollar ($ USD) e-commerce market, to global business-to-business collaboration, and to tourism, and other opportunities. Registrants who attempt to support global mobility for end users may be similarly affected when mobility solutions require universal resolvability.

Finding (2): A credible fragmentation threat is posed by sovereign nations and multi-national alliances that will not wait for ICANN to adopt a multilingual TLD policy and that choose to follow policy directions opposite to those arrived at using the ICANN collaborative policy development process. Many political reasons exist for countries to choose this course. ICANN cannot control how nations and alliances behave, but should (continue to) work with these parties towards a technically sound solution that is best for the Internet community.

Finding (3): At a technical level, multiple methods for supporting multilingualism in top level domains (Internationalized Domain Names) exist. ICANN has announced a time line for the development of a project for the technical test of internationalized TLD labels. SSAC believes that the technical test plan is essential. Technical alternatives must

be evaluated, a choice must be made, and trials must be conducted to assure that multilingualism at the root level of the DNS is ready for a production environment before a consensus policy might be reached.

Finding (4): ICANN will find it necessary to increase the number of TLDs to accommodate multilingualism and continued commercial interest. The root name server operations can accommodate a substantial increase in the size of the root zone. However, the technical aspects of name service are but one factor to consider. ICANN must review the existing TLD approval process as well as the processes whereby TLDs are introduced into the root zone (for subsequent ongoing administration) to ensure that all operations associated with adding TLDs can support the increase in TLDs.

On the basis of these findings, the Committee makes the following recommendations:

Recommendation (1): ICANN and the community at large should take appropriate measures to ensure that a thorough analysis of two candidate methods for encoding strings in TLD labels - DNAME Equivalence Mappings [15] and use of IDNA encodings [16] – is concluded quickly. Based on the conclusions and recommendations of parties responsible for this analysis, ICANN should adopt the preferred method.

Recommendation (2): ccTLD registries should actively participate in the ICANN IDN Experimental Testbed projects and provide their perspectives on the implementation of "internationalized" TLD labels in the root. SSAC recommends that ccTLD registries and national or regional linguistic organizations not implement standalone or alternate TLD schemes until the results of the IDN Experimental Testbed are evident.

Table of Contents

1 Introduction

The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for generic and country code Top-Level Domain name system management and root name server system management functions. ICANN coordinates the management of these elements of the DNS to ensure Internet users can predictably and reliably determine the public IP address associated with an ICANN-registered domain name, commonly known as *universal resolvability*.

The phrases *alternative roots* and *breakaway roots* refer to entities that operate independently from ICANN to provide root name service and to control TLD name system management functions, including TLD label approval and registry services for second level labels registered under TLDs they create. These entities provide alternative databases for domain name registration and operate alternative root name server systems so registrants and users can resolve alternative TLD names to public IP addresses. Alternative TLD labels are not recognized by ICANN and are not included in the authoritative name server information published by IANA. The 13 root name server systems that serve the "." zone published by IANA do not resolve domain names registered under these TLDs.

The subject of alternative root name server systems and alternative TLD name system administration are controversial and complex. From a technical perspective, the existence of multiple root name services undermines a fundamental design objective of the Domain Name System (DNS) [1, 2, 3]. The DNS is designed to provide predictable and reliable Internet communications using a globally unique public name space derived from a single, globally unique database called the root zone file. From a public service perspective, the alternative TLD name systems are not obliged to manage a unique root, operate in the public interest according to policies developed through community processes are destabilizing and problematic.

Much has already been published regarding alternative roots and competition in the oversight of TLD registries [4 - 9]. Prior articles and reports focus primarily on the technical impact to the authoritative root name service. These works spend less time investigating the motivations and conditions that encourage organizations to establish alternative TLD name system management functions. This was perhaps appropriate; until recently, organizations having commercial interests were the only entities perceived as being able to develop a constituency large enough to destabilize the root name service. Conditions have changed, and additional incentives must now be considered.

2 Classification of alternative root name services and TLD name system administrations

In this report, SSAC considers the following classes of alternative root name server and TLD name system operators:

- Private (intra-organizational, institutional, and enterprise) name systems
- Experimental roots and TLD name system administration
- Commercial (for profit) TLD name system administration and "inclusive" root name service
- Protest (democratic, community access) roots and TLD name system administration
- Politically motivated roots and TLD name system administration, including those established to support *multilingualism* (national and local character sets in top level domain labels).

We consider each of these in the sections that follow. Some of the classes identified in this taxonomy do not pose security and stability issues but are included for completeness.

2.1 Private name systems

Private name systems operate inside organizations, institutions and enterprise networks to provide internal name services for their users. Organizations use private roots to support a name schema and name service that has context inside the organization. A private registry name system administrator assigns labels under the second-level domain of the organization (`example.internal`) or under labels subordinate to the organization's second-level domain (`region1.example.internal`, `accounting.modesto.example.internal`).

Some organizations employ internal names often run a *split DNS*, where the domain names of the organizations' publicly accessible hosts (`www.example.com`) are universally resolvable but the names assigned to internal and "intranet" servers (`humanresources.example.com`) are isolated from the authoritative DNS and resolved only by name servers operated by the organization.

2.2 Experimental name systems and roots

Experimental root name services and name system administrations operate for many reasons, but primarily to research and analyze emerging technology. Recent experimental name services include test beds for extensions to the DNS protocol for internationalized domain names (IDNA). Experimental roots may be funded by research grants and (typically) do not operate for profit.

In certain cases, experimentation may result in changes to the authoritative root and name system realms. In cases such as DNSSEC and IPv6, for example, new resource record types were eventually introduced into the authoritative root zone file not only to test DNS operation, but to study the impact on name system administration and root zone publication processes.

2.3 Commercial TLD name systems and roots

Commercial TLD name system administrators establish root service operations, administer their own set of TLDs, and operate and franchise registries as opportunities present. They do so without establishing a relationship with ICANN through an individual Registry or Sponsorship Agreements. Such organizations have no obligation to comply with ICANN policies. They do not adhere to nor participate in the same processes as registries having agreements with ICANN. Such organizations administer TLDs and operate root name services separate from the authoritative root name service.

A number of different business models and target markets are nurtured for TLD labels and registry services.

Through **Vanity TLDs** individuals can register a full name, surname, nickname, or generally any name as a TLD. A local or global personality – for example, a rock musician, actor, model, or sports figure – establishes a surname or full name as a TLD for his or her web presence. Thus, instead of operating a vanity or personality web presence under `www.johnbossdaddyrockguy.name`, the (fictitious) rock musician John Boss Daddy could register the TLD `.johnbossdaddy` and offer SLDs publicly, possibly through franchise arrangements. Under this TLD, John Boss Daddy might also register SLDs for other personal and business purposes.

Through **Corporate TLDs**, organizations can establish their corporate name, product, or brand as a TLD. For example, rather than operating as `IBM.com`, International Business Machines could register the TLD, `.IBM.` To protect or promote a product, a parent company Example confectioners could register the product name as a TLD label; rather than using `whonkychocolates.exampleconfectioners.com` the company might register the TLD `.whonkychocolates`.

Some commercial operators run an **Open Market TLD name** system, offering any organization the opportunity to arbitrarily compose a top level label and operate a registry under that label. This is an unconstrained corollary to generic TLDs: pay for the TLD label you propose and it's yours, on a first-come, first-served basis. The TLD name system administrator may or may not require the TLD registrant to represent that the use of the label proposed does not infringe on the copyrights, trade or service marks, or other legal rights or claims of a third party.

Other commercial TLD name system operators offer **designated TLDs**, offering organizations the opportunity to register second level names under TLDs chosen by the TLD name system operator. The names such operators offer as TLD labels may be based on (perceived) market appeal and search engine relevance. For example, some TLD labels are popular search keywords (`.shop`, `.tech`, `.sport`, `.law`). Other TLD labels may offer contextual relevance to the registrant (`.family, .religion, .mp3`). Some TLD name system operators offer foreign language TLD labels. At present, these non-English language labels are composed using the "letter-digit-hyphen" subset of ASCII supported by DNS protocols without extensions to support non-Latin scripts. For example, a Spanish-speaking registrant might want to register the TLD `.empañada.` Support for tilde-n (Unicode U+00F1) is not available so the registrant might settle for `.empanada.` Similarly, a German-speaking registrant might want to register the TLD `.über`; again, support for umlaut-u (Unicode U+00FC) is not available so the registrant may choose `.uber` instead.

Commercial TLD name system administrators regard the creation of TLD labels as a lucrative business opportunity. They claim that ICANN's gTLD and sTLD approval processes and registry agreements impose business impediments that are unnecessarily constraining. Commercial TLD name system administrators justify their autonomy on one or more of the following bases:

- No limits should be imposed on the creation of generic TLDs.
- The approval process for would-be registry operators should be as simple as the process of creating a corporation.
- ICANN should not subject would-be registry operators to financial or business plan approval, nor should they be required to escrow funds for registry failover (name service continuity) but should be free to "start a business" as any entrepreneur might.
- The market will decide which TLDs succeed: as in dealing with any other businesses, registrants should understand that *caveat emptor* applies.

Advocates of commercial TLD name system administrations claim that the only checks and balances needed already exist in a market economy, and that competition provides an important check against what critics of ICANN claim is an unnecessary suppression of a market that has "hundreds of willing supplies and thousands, potentially millions of willing subscribers. [8].

2.4 Protest TLD name systems and roots

Some organizations have established TLD name systems in protest of ICANN's gTLD and sTLD approval processes and registry agreements, claiming that ICANN's policies are too restrictive and the process itself is too lengthy and costly. Protest TLD name system initiatives often have motivations other than profit. Organizations in this class may operate TLD name systems that:

1. Restrict membership. The TLD name system administrators might register one or more TLDs based on religious denomination (e.g., `.catholic, .lutheran, .judaism, .buddhism`), or based on political, environmental or social activism (e.g., `.liberaldemocrats, .cleanair, and .prochoice`).

2. Filter or censor content according to (stringent) policies asserted for that TLD. Such policies might aggressively filter to protect children from exposure to pornography

and other inappropriate content, or filter politically contradictory or inappropriate content (see also [12]).

3. Offer "democratic" TLD registration by setting very low admission criteria for membership and using a simple voting majority of members as the basis for adopting new TLD labels. This operating model is reminiscent of public access cable television in the United States. A community of interest chooses a TLD and proposes it to the community at large. If approved, the proposing community becomes a domain operator and provides such registry and support services as the community sees fit. It is entirely user-owned and operated, and has no apparent political agenda other than to remain so.

Some of the motivations in this classification may have political bases, but such cases represent only a subset of possible protest TLDs. The organizations in this classification are not sovereign nations or alliances of sovereign nations.

2.5 Politically motivated TLD name systems and roots

Some alliances and governments establish alternative TLD name systems and root services because they object to U.S. government involvement and do not agree with the operations and policies of current organizations that manage the authoritative TLD name system and service (the United States government, through its Department of Commerce, and ICANN). Reasons cited for such "breakaway" activities include:

Governance. Governance is an important matter for sovereign nations and multi-nation alliances. At issue is whether such governing bodies should be required to seek U.S. government approval of multi-national (e.g., .EU) TLD labels and TLD labels composed in national and local character sets. Governance also encompasses autonomy of operations. Some sovereign nations do not feel should they be entirely dependent upon U.S. government-funded and operated root name server systems. They may want to operate their own root servers to provide additional capacity and availability for their citizens. Political stature may also be a factor. A government may feel that economic or political influence entitles it to operate one of the existing authoritative root name server.

Trust. Organizations and governments may not feel comfortable with the USG and a USG-sanctioned private organization having control of and influence over TLD approval and root name server operation. They may worry that political conflicts or even disagreements with root operators could impact how their TLD information is administered in the root zone file.

Control. Some parties express concern that root name servers operate independently of (political) authority and would prefer to impose government oversight in their own country or region.

Reliability, availability, fair allocation of cost and resources. Some nations feel there are insufficient root servers in their region to provide adequate service at acceptable cost, especially in the event of political unrest, alienation and interference from the USG.

Multilingualism. Some alternate roots have been established to support multi-lingual (and non-ASCII character set) names in top level domain labels [13, 14], e.g., to support languages that use:

- extended Latin character sets and include characters with diacritical marks (upper and lower case letters with markings such as an acute, stroke, caron, cedilla, tilde, macron, diaeresis, ogonek, macron, thorn...),
- non-Latin alphabets, including Arabic, Cyrillic, Greek, Hebrew, Hindi
- logographic writing systems (ideograms), including Chinese, Classic Egyptian, Korean, and Japanese

Support for multilingualism in top level domain labels affects the operation of the domain name system at the root and affects the DNS protocols as well. Significant technical, political and administrative issues must be resolved by the community at large.

At the technical level, two methods for supporting multilingualism in top level domains have been proposed. One solution, colloquially referred to as `IDN.IDN`, applies the IETF IDNA standards in the composition of top level domain names [19]. IDNA (Internationalizing Domain Names in Applications) accommodates the use of Unicode-encoded characters in the composition of labels. It defines a method for encoding labels containing non-ASCII characters using only the “letter-digit-hyphen” subset of ASCII characters already allowed in the DNS for backward-compatibility so that “internationalized” domain names can be introduced with minimal changes to the existing infrastructure. A second solution [18] also recommends that local or national language equivalents of TLD labels be constucted as ASCII Compatible Encodings as specified in RFC 3492, *Punycode: A Bytestring encoding of Unicode for IDNA* [21], but that the DNAME construct defined in IETF RFC 2672, *Non-Terminal DNS Name Redirection* [20] be used to map such name spaces directly onto existing generic and country-code TLDs.

Evaluating technical modifications to the DNS, choosing a preferred alternative, assessing the operational changes required to implement the selected technique, and testing to assure that multilingualism at the root level of the DNS is ready for a production environment are critical tasks that must be completed before a consensus policy might be reached. Some countries have concluded that the need to support local and national languages for their people is immediate. These countries have elected not to wait for the international community to complete all these tasks, and have implemented internationalized domain names using their own technology, operations, and policies [15].

3 Issues

Having analyzed alternative TLD name systems and roots and categorizing them as we have in Section 1, we identify issues that are unique to individual categories, and identify several issues in common as well. The following sections examine the issues and possible consequences in some detail. This section concludes with a table summarizing and comparing issues versus class.

3.1 Private name systems

Such registries are by definition private. The name space is applicable to a closed community. Implemented correctly, private name services and registries do not pose threats to the authoritative root name service. When implemented incorrectly, the issue of unintentional disclosure of private names is more cause for concern for the organization operating the private registry than the community at large.

When domain name queries for names registered in a private registry “leak” out of the organization, they will (in most cases) not resolve. There have been cases where private registries have been implemented incorrectly, where the name space conflicted with delegations made by IANA. Such cases are a concern to ICANN and the community, but are not very common.

When a split DNS is implemented incorrectly, internal names that are unintentionally disclosed may reveal details about a company’s internal network topology (e.g., `research.trafalgar.london.example.com`) or network equipment (`catalyst5500.mainhub.reno.example.com`), or how and where the organization stores sensitive information (`patientrecords.office.example.com).`

3.2 Experimental name systems and roots

Experimentation and testing activities of this sort are commonly subjected to careful coordination and planning across the research community and the parties vested with the responsibilities associated with root zone publication (IANA, VeriSign, US Department of Commerce) so as not to interfere with the operation of the authoritative name service. Experimental roots and registries might cause a temporary disruption if implemented incorrectly but do not pose any long term issues to authoritative root name service and TLD name system management.

3.3 Commercial TLD name systems and roots

Operating under purely market checks and balances, commercial TLD name systems:

I-1 Regard dispute resolution as issues that fall under the jurisdiction of the Courts. In some cases, they claim that there is no need for any law in name dispute cases beyond corporate laws related to trade names, trademarks etc., and offer as corroborating evidence the fact that little legislation has been written specifically regarding domain names.

I-2 Are under no obligation to demonstrate they are able to underwrite the cost of registry operations, maintain a global, highly available root name service, and operate profitably.

I-3 Operate as privately held corporations, do not enter into formal agreements with ICANN, and cannot be held accountable to consensus policies established to assure fair name registration and transfer practices, dispute resolution, and WHOIS data accuracy.

I-4 Are under no obligation to assure uniqueness of TLDs with ICANN or any other TLD name systems.

I-5 Are under no obligation to submit their business cases to the external and community scrutiny and evaluation ICANN and the community at large conduct when entering into a gTLD agreement with a would-be registry operator.

I-6 Have no formal relationships with root name server operators and no obligation to assure uniform, universal name resolution with authoritative root name services and root name services that support competing commercial TLD name systems.

I-7 Are no obliged to make their root zone files available for download to parties other than affiliates.

I-8 Are under no obligation to submit their root server operations to review to assure that the number, location, and distribution of root name servers is sufficient to sustain acceptable levels of system performance, robustness, and reliability.

I-9 Are under no obligation to work with the community at large to assure that domains registered in their TLDs resolve to IPv4 and IPv6 addresses using conventional DNS client software and user configuration. As a result, users of these alternative TLDs could have names that do not resolve correctly, if at all.

I-10 Can intentionally or inadvertently modify the authoritative root zone data published by IANA if they choose to incorporate IANA's root zone data in their own root zone file (see *inclusive name service*, Section 3).

3.4 Protest TLD name systems and roots

Protest TLD name system administrators operate autonomously and could evolve to commercial enterprises. They share several characteristics with commercial TLD name system administrators and root operators. Additionally, I-11 Operate as a closed community and are not obliged to engage in community or consensus processes.

I-12 In situations where a simple voting majority of members is the only criteria for TLD label approval, the numbers of TLDs can grow at rates commensurate with SLDs registered in popular ICANN gTLDs.

I-13 Policies to protect organizations from name abuse and misrepresentation (e.g., an anti-Christian organization registering all Protestant denominations for purposes of slandering the Christian faith or doctrine) may not be asserted or enforced. No dispute mechanisms may be available to counter such infringements.

I-14 In the absence of membership fees or other means of financial support, it is unclear whether such registries can underwrite registry operating costs as well as the cost of a maintaining a global, highly available root name service.

3.5 Politically motivated TLD name systems and roots

Operating on behalf of a sovereign nation, treaty organization, or a political alliance, politically motivated TLD name system administrators share many characteristics with commercial administrators. Additionally, they can

I-15 Mandate that ISPs use only root name services operated by or on behalf of the sovereign entity.

I-16 Substitute their own root zone data for root zone data published by IANA to redirect users for the purposes of censorship, propaganda, or to enhance the commercial and economic interests of the sovereign body. (The effect might be compared to browser hijacking spyware).

I-17 Substitute domain names and addresses of sanctioned search engines and other Internet applications (messaging, collaboration, web services, etc.) to control user behavior and access to content.

I-18 Create names for gTLDs in local character sets without consultation or coordination with other organizations and/or nations that employ the same character sets (one effect of such actions would be that the same set of characters from a given local character set could represent a gTLD but that set of characters might resolve to different addresses depending on what country’s name servers the user contacted to resolve the domain name. Another effect is that several countries may choose different sets of characters from the same local character set and so the universality of the TLD is lost, as well as any reference to the registrant in the original gTLD character set.

3.6 *Summary of issues*

Several characteristics ascribed to one class of Alternative TLD name and root service administrators are shared by other classes.

Table 2-1 summarizes all the characteristics that are associated with each classification.

Issue	Private Name Systems	Experimental Registries	Commercial Name Systems	Protest Name Systems	Political Name Systems
I-1 Dispute resolution			X		
I-2 Solvency			X		
I-3 Accountability			X	X	
I-4 TLD uniqueness			X	X	X
I-5 Business case			X	X	
I-6 Root operator relationships			X	X	X
I-7 Root zone file availability			X	X	X
I-8 Root operations review			X	X	X
I-9 Universal Resolvability			X	X	X
I-10 Root zone modification			X	X	X
I-11 Closed community				X	X
I-12 TLD growth				X	
I-13Policy				X	
I-14 Solvency (2)				X	
I-15 Mandated use of root					X
I-16 Root zone substitution					X
I-17Behavior/content control					X
I-18 Character sets					X

Table 2-1.

4 Fragmentation of the root name service

In the general case, alternative TLD name system administrators operate their own root name services. These often mimic the root zone editing and publication process performed by IANA and VeriSign under US DoC oversight to varying degrees. Alternative TLD name system administrators commonly attempt to provide name resolution services for their own TLDs as well as the TLDs resolved via the authoritative root name service. Some offer *inclusive name resolution* by appending their own root zone file to the root zone file published by IANA. Others use referral and delegate name resolution to the authoritative name service for names in TLDs other than their own.

In cases examined by SSAC, the *inclusive* root zone files of alternative root name servers is only the union of the authoritative root zone created by IANA plus root zone data of the alternative TLD name system. No example of a root zone file that includes *all* TLDs of *all* alternative and authoritative TLD registries could be located. Given that there can be conflicting data (e.g., duplicate TLD labels), SSAC is skeptical that an all-inclusive root zone file could be created, maintained reliably, published in a timely and responsive manner, and be universally accepted.

In the current state, universal resolution of domains registered in TLDs administered by alternative TLD name system operators is not guaranteed. To be of any use whatsoever, users and DNS clients must be able to resolve names from both the authoritative DNS and each alternate root. This problem is addressed in several ways:

- Alternative TLD name system operators invite ISPs to partner or affiliate. Affiliates and partners are expected to replace the pre-stored IP addresses of the authoritative root name servers with those of their alternate root servers.
- Affiliate DNS operators are expected to install a special, “expanded” `named.root` or `hints` file created by the TLD name system operator.
- Internet users must configure the DNS settings on their client computers to use the IP addresses of the TLD name system operator’s DNS servers, or the IP addresses of an ISP affiliated with the TLD name system operator. In some cases, users must modify the Windows Registry.
- Internet users must install software extensions or a special client application that auto-configures the user’s DNS settings to point to the TLD name system operator’s name servers.

Coordination across all the alternative TLD name system operators does not exist today. Configurations and software extensions that work in individual cases are not sufficient to allow users to resolve names registered in TLDs across multiple TLD name systems. Some of the problems users will encounter if they try to resolve TLD labels registered in multiple TLD name systems are described below:

- When two TLD name system operators use the same client software extensions to auto-locate root servers, the root name servers installed will be different. Specifically, when there is no common root name service between name system operators A and B, it is not possible to resolve TLDs from both without reconfiguring a host.

- Some client software used for autoconfiguration are written as unsigned browser helper objects for Windows Internet Explorer. Many anti-spyware software identify the autoconfiguration software as spyware and either block or remove it.

- Client software is not available for all commercial operating systems.

- Client software is not compatible with all commercial and open source web browsers and Internet-enabled applications.

- Duplicate TLD labels will return different addresses depending on the name service queried.

Other issues arise when domain names are not universally resolvable. These can seriously affect registrants in several ways:

- Alternative TLD name systems create barriers to a estimated two trillian dollar (USD) e-commerce and business-to-business collaboration, tourism, commercial and other opportunities for registrants. The majority of Internet users do not use client software or special configurations simply so they can access alternative TLDs or internationalized TLDs. This is especially likely to be the case for users whose familiarity with TLDs other than .com, .net, and .org is limited.

- When registrants register domain names from commercial alternative TLD name systems, the information they publish and the services and products they offer are inaccessible to an estimated 972 million Internet users which places these registrants at a competitive disadvantage compared to registrants with domain names resolvable via the authoritative root. The same situation exists for registrants who choose to only register a domain name in a local or national character set from a politically motivated TLD name system.

- Registrants who register domain names from alternative TLD name systems may not be able to support a mobile workforce in situations where the mobile worker is unable to resolve the domain name of virtual private network (VPN) security gateways.

5 Findings and Recommendations

The Committee offers these findings and recommendations in the spirit of open review, comment and evaluation, with the expectation that they will be considered carefully before they result in action.

5.1 Findings

Finding (1): SSAC can find little evidence to support claims that alternative TLD name systems have or will attract a significant market share to fragment the root. Registrants who register names in alternative TLD name systems may encounter barriers to an estimated two trillion dollar ($ USD) e-commerce market, to global business-to-business collaboration, and to tourism, and other opportunities. Registrants who attempt to support global mobility for end users may be similarly affected when mobility solutions require universal resolvability.

Finding (2): A credible fragmentation threat is posed by sovereign nations and multi-national alliances that will not wait for ICANN to adopt a multilingual TLD policy and that choose to follow policy directions opposite to those arrived at using the ICANN collaborative policy development process. Many political reasons exist for countries to choose this course. ICANN cannot control how nations and alliances behave, but should (continue to) work with these parties towards a technically sound solution that is best for the Internet community.

Finding (3): At a technical level, multiple methods for supporting multilingualism in top level domains (Internationalized Domain Names) exist. ICANN has announced a time line for the development of a project for the technical test of internationalized TLD labels. SSAC believes that the technical test plan is essential. Technical alternatives must be evaluated, a choice must be made, and trials must be conducted to assure that multilingualism at the root level of the DNS is ready for a production environment before a consensus policy might be reached.

Finding (4): ICANN will find it necessary to increase the number of TLDs to accommodate multilingualism and continued commercial interest. The root name server operations can accommodate a substantial increase in the size of the root zone. However, the technical aspects of name service are but one factor to consider. ICANN must review the existing TLD approval process as well as the processes whereby TLDs are introduced into the root zone (for subsequent ongoing administration) to ensure that all operations associated with adding TLDs can support the increase in TLDs.

6 Recommendations

On the basis of these findings, the Committee makes the following recommendations:

Recommendation (1): ICANN and the community at large should take appropriate measures to ensure that a thorough analysis of two candidate methods for encoding strings in TLD labels - DNAME Equivalence Mappings [15] and use of IDNA encodings [16] – is concluded quickly. Based on the conclusions and recommendations of parties responsible for this analysis, ICANN should adopt the preferred method.

Recommendation (2): ccTLD registries should actively participate in the ICANN IDN Experimental Testbed projects and provide their perspectives on the implementation of "internationalized" TLD labels in the root. SSAC recommends that ccTLD registries and national or regional linguistic organizations not implement standalone or alternate TLD schemes until the results of the IDN Experimental Testbed are evident.

SSAC is aware that, as the Committee publishes this Report, the issues of TLD registry administration fragmentation and fragmented root name service operations have attracted considerable attention and concern. SSAC will continue to work with the community as the community attempts to resolve these issues. SSAC also notes that several recommendations, if accepted, will result in future work items for the Committee as well as various parties encouraged to take action.

7 Additional Sources and Reading

[1] ICP-3: A Unique, Authoritative Root for the DNS, http://www.icann.org/icp/icp-3.htm

[2] The Domain Name System: A Non-Technical Explanation:Why Universal Resolvability Is Important, http://www.internic.net/faqs/authoritative-dns.html

[3] RFC 2826, IAB Technical Comment on the Unique DNS Root, http://www.ietf.org/rfc/rfc2826.txt

[4] RFC 4367, What's in a Name: False Assumptions about DNS Names http://www.ietf.org/rfc/rfc4367.txt

[5] The Alternate Root, http://cbtollfree.com/Article.cfm?ArticleId=5297

[6] Alternate roots for domain names explained in IETF draft, http://seclists.org/lists/politech/2001/May/0083.html

[7] Alternate DNS Root, http://www.encyclopedia-online.info/Alternate_DNS_root

[8] Multipe DNS Roots, http://www.cs.utk.edu/~moore/opinions/multiple-dns-roots.html

[9] Competing DNS Roots, http://www.itu.int/osg/spu/seminars/mueller/tprc2001.pdf

[10] ISO 3166-1 "Country codes" and ISO 3166-2 "Country subdivision codes", http://www.iso.org/iso/en/prods-services/iso3166ma/05database/index.html

[11] ICANN Unsponsored TLD Agreement: Appendix K, Schedule of Reserved Names www.icann.org/tlds/agreements/unsponsored/registry-agmt-appk-26apr01.htm

[12] RFC 3675, .sex Considered Dangerous, http://www.ietf.org/rfc/rfc3675.txt

[13] Internationalized Domain Names (IDN) in .museum - Supported scripts and languages, http://www.about.museum/idn/language.html

[14] Browsing in Foreign Language and Non-Latin Scripts, http://www.pollycyber.com/howto/forlang.htm

[15] Internationalizing the DNS, http://www.icann.org/stockholm/draft-klensin-i18n-newclass-00.txt

[16] Signposts in Cyberspace:The Domain Name System and Internet Navigation, National Academies Press, http://www7.nationalacademies.org/cstb/pub_dns.html

[17] Generic Top Level Domain Names: Market Development and Allocation Issues http://www.oecd.org/dataoecd/56/34/32996948.pdf

[18] A Proposal for DNAME Equivalence Mapping for TLD Strings http://www.icann.org/announcements/proposal-dname-equivalence-mapping-tld-12dec05.pdf and http://www.icann.org/announcements/**dname**-white-paper-**verisign**-17nov05.pdf

[19] RFC 3490, Internationalizing Domain Names in Applications (IDNA), http://www.rfc-editor.org/rfc/rfc3490.txt

[20] RFC2672, Non-Terminal DNS Name Redirection (DNAME) http://www.rfc-editor.org/rfc/rfc2672.txt

[21] RFC 3492, Punycode: A Bytestring encoding of Unicode for IDNA http://www.rfc-editor.org/rfc/rfc3492.txt

Appendix A
Contributors

Alain Aina, Consultant

Jaap Akkerhuis, NLnet Labs

KC Claffy, CAIDA

Steve Crocker, Shinkuro (Chairman)

Johan Ihrén, Autonomica

Rodney Joffe, Centergate

Mark Kosters, Verisign

Allison Mankin, Consultant

Ram Mohan, Afilias

Russ Mundy, SPARTA, Inc

Frederico Neves, registro.br

Jon Peterson, NeuStar

David Piscitello, ICANN SSAC Fellow

Ray Plzak, ARIN

Mike St. Johns, Nominum

Doron Shikmoni, ForeScout, ISOC-IL

Bruce Tonkin, Melbourne IT; Chairman, Generic Names Supporting Organization

Paul Vixie, ISC

Suzanne Woolf, ISC