Building Towards a Comprehensive gTLD Registry Failover Plan
1 June 2007

Table of Contents

1. Executive Summary

The 2006-2007 ICANN Operating Plan (http://www.icann.org/announcements/operating-plan-22jun06.htm) describes the series of projects and deliverables based on the ICANN Strategic Plan (http://www.icann.org/announcements/strategic-plan-22jun06.htm). According to the Operating Plan, ICANN is to "establish a comprehensive plan to be followed in the event of financial, technical or business failure of a registry operator, including full compliance with data escrow requirements and recovery testing" (see Section 1.1.2).

This report is being prepared as part of the registry failover project to provide guidance to ICANN and the Internet community in the event of a registry failure. This is not intended to be a policy document. The registry failover project poses a complex set of issues that involve ICANN's mission in both ensuring DNS stability and promoting competition. Following the 29th ICANN International Public Meeting in San Juan, Puerto Rico, ICANN will synthesize a best practices document describing registry failover mechanisms. These mechanisms will also provide guidance or be incorporated into ICANN's new gTLD process potentially as a best practices contractual requirement.

The failover mechanisms will, in the event of registry failure:

- Provide recovery and escrow of domain name registration information and registrant account information
- Provide a period of ongoing operations where a replacement entity may be engaged, or
- Provide a period of notice to registrants of impending closure so that registrants may take their own remedial measures.

The mechanisms are being considered in light of the following questions:

- What is ICANN's duty to registrants in the event of a failure of a gTLD registry?
- What would trigger ICANN involvement in a potential registry failure?
- Should a registry be required to designate a back-up registry operator that would step in to maintain the registry in the event of a long-term failure?
- Could ICANN designate a replacement registry, and if so, how would that occur?

ICANN has conducted a review of the critical functions of a registry, examined transition of a registry from one operator to another, and examined potential failure scenarios. This report finds that the identification of critical functions, along with establishment of best practices by registries will assist ICANN in the event that a registry failure occurs. ICANN has identified a number of scenarios that require further examination and discussion before a registry failover plan can be adopted. This report provides the elements of the registry failover plan and initial recommendations based on current registry practices. These elements include best efforts at geographic diversity of name servers, the creation and testing of registry contingency plans, the establishment of a clear communications plan and identification of a failure as a temporary or long-term condition.

2. Background

2.1 Consultations

Since the commencement of the registry failover project in early 2006, ICANN staff has conducted extensive research to advance work on registry failover, and has consulted widely with gTLD representatives, ccTLD managers and the ccNSO, external experts, data escrow providers and the ICANN Board. Staff has conducted outreach with SSAC, ALAC and the ICANN community for additional feedback on aspects of the registry failover project. SSAC provided extensive comments and suggestions during the drafting of this report.

The topic of registry failover and contingency planning was discussed by the Registry Constituency in June 2001. The Constituency created a Registry Failure Task Force to research and develop procedures in the event of registry failure. The Task Force examined registry security best practices in order to understand the functions, activities, costs and performance criteria that apply to a sound TLD registry.

ICANN devoted its November 2001 Annual Meeting to the topic of DNS Security, and during that meeting the Registry Constituency provided an update on the work of the Task Force.[1] A summary of that report was included in SSAC DNS Security Update #1, published 4 January 2002.

[1] Registry Constituency presentation, 14 November 2001, http://www.gtldregistries.org/responses/gTLD_RC_SecurityBestPractices.ppt.

Between 2002-2006, registry failover was incorporated as a contractual requirement in new gTLD registry agreements (.JOBS, .MOBI, .TRAVEL, .ASIA. Registry failover was also discussed in the context of the sponsored TLD round of 2003.

The present registry failover project was described during the ICANN Operational Planning Workshop in Wellington, New Zealand (28 March 2006) and was later incorporated into the budget that was approved by the Board. To collect information for this project, in May 2006, ICANN's gTLD registry team initiated a review of gTLD failure scenarios and ICANN's data escrow requirements. In accordance with the project plan, ICANN's gTLD registry team conducted working sessions with gTLD representatives during the ICANN Meeting in Marrakech, Morocco (24-30 June 2006), with ccTLD managers and the gTLD Registry Constituency in Sao Paulo, Brazil (2-8 December 2006), and most recently presented to the ccNSO and gTLD Registry Constituency in Lisbon, Portugal (24-30 March 2007).

Staff provided an update on the registry failover project to the ICANN Board on 13 March 2007 (http://www.icann.org/minutes/minutes-13mar07.htm). An update on the project was provided to the ccNSO Members in Lisbon on 27 March 2007 (transcript available at http://www.icann.org/meetings/lisbon/transcript-ccnso-members-27mar07.htm), and the ccNSO cited the project an update to the Board during the ICANN Public Forum on 29 March 2007 (transcript available at http://www.icann.org/meetings/lisbon/transcript-public-forum-29mar07.htm).

In Lisbon, the Government Advisory Committee released its GAC Principles on New gTLDs (http://gac.icann.org/web/communiques/gac27com.pdf). The Principles contain two recommendations on registry failover:

> 2.10 A new gTLD operator/registry should undertake to implement practices that ensure an appropriate level of security and stability both for the TLD itself and for the DNS as a whole, including the development of best practices to ensure the accuracy, integrity and validity of registry information.
>
> 2.11 ICANN and a new gTLD operator/registry should establish clear continuity plans for maintaining the resolution of names in the DNS in the event of registry failure. These plans should be established in coordination with any contingency measures adopted for ICANN as a whole.

This report represents the inputs received from members of the Registry Constituency, ccTLD managers, ALAC members and other stakeholders to date. Following sufficient public comment, ICANN intends to provide a comprehensive registry failover plan to the ICANN Board for consideration during the ICANN 29th International Public Meeting in San Juan, Puerto Rico (25-29 June 2007).

2.2 Glossary

2.2.1 DNS

The Domain Name System (DNS) is a distributed database that translates domain names (computer hostnames) to IP addresses. Domain names are defined in RFC 1034 (ftp://ftp.rfc-editor.org/in-notes/rfc1034.txt). RFC 1035 describes the domain system and protocol (published in November 1987 and recognized as an Internet Standard, ftp://ftp.rfc-editor.org/in-notes/rfc1035.txt). As stated in RFC 1035, “The goal of domain names is to provide a mechanism for naming resources in such a way that the names are usable in different hosts, networks, protocol families, internets, and administrative organizations.” The DNS consists of a hierarchical set of DNS servers. Each domain or subdomain has one or more authoritative DNS servers that publish information about that domain and the nameservers of any domains below it.

- The DNS consists of resource records, zones, nameservers, and resolvers. Programs such as BIND, that respond to queries about the domain namespace via the DNS protocol, are called nameservers.[2]

- The data associated with domain names are contained in resource records. There are several types of resource records, corresponding to the varieties of data that may be stored in the domain namespace, including Start of Authority records, NS (nameserver) records, Address records, and PTR (pointer) records.[3]

- A zone is an autonomously administered piece of the name space.

- Nameservers load data from zone datafiles. These files contain resource records that describe the information within a particular zone. Resource records describe the hosts within the zone and delegation of subdomains.[4]

- Resolvers are the clients that access nameservers, and handle queries and responses.

2.2.2 Registry

A registry is an organization responsible for maintaining the zone files of a top-level domain (TLD). “Under the current structure of the Internet, a given top-level domain can have no more than one registry.”[5]

2.2.3 Registrar

A registrar acts as an interface between registrants and registries, providing registration and other value-added services. The registration process occurs when a customer provides contact and perhaps billing information to a registrar (or in some cases, a registry) in exchange for delegation of a domain name.[6]

2.3 Related Documents

RFCs. “The Requests for Comment (RFC) documents form a series of notes started in 1969 by the research community that designed and built the ARPAnet. The RFCs series forms an archive of technical proposals, standards, and ideas about packet-switched networks.”[7] RFCs are maintained by the Internet Engineering Task Force (IETF) and published at http://www.rfc-editor.org/.

[2] Liu & Albitz, DNS & BIND, 5th Ed. (May 2006), page 22.
[3] Id., page 16, 55-61.
[4] Id., page 26.
[5] Id., page 41.
[6] Id., page 41.
[7] http://www.rfc-editor.org/rfc-online.html.

RFC 1033, Domain Administrators Operations Guide, provides guidelines for domain administrators in operating a domain server and maintaining their portion of the hierarchical database (ftp://ftp.rfc-editor.org/in-notes/rfc1033.txt).

RFC 1034, Domain Names - Concepts and Facilities, provides extensive background information on the DNS. The DNS has three major components: resource records, name servers and resolvers (ftp://ftp.rfc-editor.org/in-notes/pdfrfc/rfc1034.txt.pdf).

RFC 1035, Domain Implementation and Specification, is cited above.

RFC 1101, DNS Encoding of Network Names and Other Types, describes a method for mapping between network names and addresses (ftp://ftp.rfc-editor.org/in-notes/rfc1101.txt.pdf).

RFC 1591, Domain Name System Structure and Delegation, provides information on the structure of names in TLDs and the administration of domains (ftp://ftp.rfc-editor.org/in-notes/pdfrfc/rfc1591.txt.pdf). This RFC is particularly useful in describing the role of the designated manager of a TLD:

> "A new top-level domain is usually created and its management delegated to a 'designated manager' all at once…The major concern in selecting a designated manager for a domain is that it be able to carry out the necessary responsibilities, and have the ability to do a equitable, just, honest, and competent job" (see RFC 1591, page 3).

RFC 1591 identified several principles for a designated manager of a TLD and identified critical functions of a registry:

- There should be a designated manager for a TLD. "The manager must, of course, be on the Internet. There must be Internet Protocol (IP) connectivity to the nameservers and email connectivity to the management and staff of the manager."[8]

- "The designated authorities are trustees for the delegated domain, and have a duty to serve the community."

- "The actual management of the assigning of domain names, delegating subdomains and operating nameservers must be done with technical competence…and operating the database with accuracy, robustness and resilience."[9]

RFC 2181, Clarifications to the DNS Specification, provides an update to the DNS specification (ftp://ftp.rfc-editor.org/in-notes/rfc2181.txt).

RFC 2182, Selection and Operation of Secondary DNS Servers, is a best current practice for the selecting and operating secondary DNS Servers (ftp://ftp.rfc-editor.org/in-notes/rfc2182.txt)

RFC 3467, Role of the Domain Name System, provides useful information on the original function and purpose of the domain name system (ftp://ftp.rfc-editor.org/in-notes/rfc3467.txt).

[8] RFC 1591, J.Postel, page 4 (March 1994), ftp://ftp.rfc-editor.org/in-notes/pdfrfc/rfc1591.txt.pdf.
[9] Id., page 6.

BCP 126, Operation of Anycast Services, specifies the best current practices for using Anycast to add redundancy to DNS servers (ftp://ftp.rfc-editor.org/in-notes/bcp/bcp126.txt).

Internet draft on ccTLD Best Current Practices (http://ws.edu.isoc.org/workshops/2006/PacNOG2/track1/day3/draft-wenzel-cctld-bcp-02.txt). This is a draft document on best current practices within the ccTLD community. As an Internet-draft, this document is not a standard and is considered a work-in-progress.

Proposed Rule on the technical management of Internet Names and Addresses (20 February 1998), the US Department of Commerce, National Telecommunication and Information Administration (NTIA) (http://www.ntia.doc.gov/ntiahome/domainname/022098fedreg.htm). The document defined registry requirements as:

1. An independently-tested, functioning Database and Communications System that:

    a) Allows multiple competing registrars to have secure access (with encryption and authentication) to the database on an equal (first-come, first-served) basis

    b) Is both robust (24 hours per day, 365 days per year) and scalable (i.e., capable of handling high volumes of entries and inquiries).

    c) Has multiple high-throughput (i.e., at least T1) connections to the Internet via at least two separate Internet Service Providers.

    d) Includes a daily data backup and archiving system.

    e) Incorporates a record management system that maintains copies of all transactions, correspondence, and communications with registrars for at least the length of a registration contract.

    f) Features a searchable, on-line database meeting the requirements of Appendix 2.

    g) Provides free access to the software and customer interface that a registrar would need to register new second-level domain names.

    h) An adequate number (perhaps two or three) of globally-positioned zone-file servers connected to the Internet for each TLD.

2. Independently-reviewed Management Policies, Procedures, and Personnel including:

    a) Alternate (i.e., non-litigation) dispute resolution providing a timely and inexpensive forum for trademark-related complaints. (These procedures should be consistent with applicable national laws and compatible with any available judicial or administrative remedies.)

    b) A plan to ensure that the registry's obligations to its customers will be fulfilled in the event that the registry goes out of business. This plan must indicate how the registry would ensure that domain name holders will continue to have use of their domain name and that operation of the Internet will not be adversely affected.

c) Procedures for assuring and maintaining the expertise and experience of technical staff.

d) Commonly-accepted procedures for information systems security to prevent malicious hackers and others from disrupting operations of the registry.

3. Independently inspected Physical Sites that feature:

a. A backup power system including a multi-day power source.

b. A high level of security due to twenty-four-hour guards and appropriate physical safeguards against intruders.

c. A remotely-located, fully redundant and staffed twin facility with ``hot switchover'' capability in the event of a main facility failure caused by either a natural disaster (e.g., earthquake or tornado) or an accidental (fire, burst pipe) or deliberate (arson, bomb) man-made event. (This might be provided at, or jointly supported with, another registry, which would encourage compatibility of hardware and commonality of interfaces.)

There have been significant improvements in technology, operations and internationalization since the NTIA rule was published nearly 10 years ago. A proposed revision to the rule if required in order to stay current with best current practices may be undertaken in a separate effort.

3. Critical Functions of a Registry

Prior to the development of a comprehensive registry failover plan, it is necessary to describe those functions that are deemed to be critical in order to operate a gTLD registry. This report is not intended to be exhaustive of all registry functions, but highlight those functions that are necessary in order to maintain the operation of a registry in the event of failure.

3.1 Critical Functions in ICANN’s gTLD Registry Agreements

ICANN’s current gTLD registry agreements require that registry operators comply with RFCs 1034, 1035, 1101, 2181 and 2182 for nameserver operations.[10]

As an example of registry functions defined in ICANN’s current gTLD registry agreements, section 3.1(d)(iii) defines Registry Services as:

> (a) those services that are both (i) operations of the registry critical to the following tasks: the receipt of data from registrars concerning registrations of domain names and name servers; provision to registrars of status information relating to the zone servers for the TLD; dissemination of TLD zone files; operation of the registry zone servers; and dissemination of contact and other information concerning domain name server registrations in the TLD as required by this Agreement; and (ii) provided by the Registry Operator for the .com registry as of the Effective Date; (b) other products or services that the Registry Operator is required to provide because of the establishment of a

[10] As an example, see Appendix 7 (Functional and Performance Specifications) from the .ASIA Registry Agreement (http://www.icann.org/tlds/agreements/asia/appendix-7-06dec06.htm).

Consensus Policy (as defined in Section 3.1(b) above); (c) any other products or services that only a registry operator is capable of providing, by reason of its designation as the registry operator; and (d) material changes to any Registry Service within the scope of (a), (b) or (c) above.[11]

The gTLD registry agreements also provide that registries "shall make access to Registry Services, including the shared registration system, available to all ICANN-accredited registrars."[12]

On a monthly basis, based on the format specified in the registry or sponsorship agreement, gTLD registries and sponsors provide a report to ICANN containing information on the following categories:

- The number of accredited registrars for the TLD
- Service level agreement performance
- TLD zone file access activity
- Whois service availability
- Total number of transactions by subcategories (adds, deletes, modifies, checks, renewals, transfers and restores)
- Daily transaction range
- Per-registrar activity report[13]

Although the monthly reports are not definitive of critical functions of a registry, the reports do provide useful information on registry performance in areas that may be considered critical.

The gTLD registry agreements also include provisions on functional and performance specifications. These provisions are typically found in Appendix 7 of ICANN's gTLD registry agreements. As an example, see Appendix 7 of the .ASIA Registry Agreement, http://www.icann.org/tlds/agreements/asia/appendix-7-06dec06.htm. This appendix includes requirements for the operation of nameservers, registry systems, Whois, data escrow, reporting requirements, DNS service availability, performance levels, location of data centers and, in some registry agreements, fail over practice requirements and use of EPP (Extensible Provisioning Protocol).

The .JOBS Registry Agreement states that "Fail over from one data center to another will be practiced at least once every two years as part of the registry's robust disaster recovery plan. Any such fail over practice will be planned in advance, and the registrars will be given advance notification." See http://www.icann.org/tlds/agreements/jobs/appendix-7-05may05.htm.

3.2 DNS data, zone file and nameserver maintenance

The maintenance of nameservers and DNS for domains is probably the most critical function of a registry. The DNS enables domain names that are registered to resolve on the Internet.

[11] This provision appears in the .ASIA, .BIZ, .CAT, .COM, .INFO, .JOBS, .MOBI, .NET, .ORG, .TEL, .TRAVEL registry agreements.

[12] This provision appears in the .ASIA, .BIZ, .CAT, .COM, .INFO, .JOBS, .MOBI, .NET, .ORG, .TEL and .TRAVEL registry agreements, Section 7.1(a).

[13] Categories derived from Appendix 4 of the .COM Registry Agreement, http://www.icann.org/tlds/agreements/verisign/appendix-04-01mar06.htm. As an example, see the January 2007 .ORG Monthly Report, http://www.icann.org/tlds/monthly-reports/org/pir-200701.pdf.

A TLD zone file contains Start of Authority (SOA) records, Nameserver (NS) records for each name server of each domain (such as NS.ICANN.ORG), Time to Live (TTL) records (the amount of time DNS resource records are to be cached), and Address (A and AAAA) records (IP addresses) for the nameservers. These records must be maintained by a registry operator according to recognized best practices.

"The DNS was designed to identify network resources…with the flexibility to accommodate new data types and structures." RFC 3467 (ftp://ftp.rfc-editor.org/in-notes/pdfrfc/rfc3467.txt.pdf).

ICANN's Security and Stability Advisory Committee released a DNS Infrastructure recommendation on 1 November 2003 (see http://www.icann.org/committees/security/dns-recommendation-01nov03.htm) to address stability of DNS infrastructure. The paper provides two recommendations on the delegation of zones in the DNS:

> 1. Zone administrators should adopt a policy that ensures that referral information for their sub-zones is updated upon request and in a timely fashion.
> 2. Zone administrators should adopt a policy that requires multiple independent servers for their zone when it delegates sub-zones to more than one responsible party.

At a minimum, registries should implement geographic diversity of DNS services. Geographic diversity serves two purposes: 1) increases the security and stability of a TLD, 2) locates name servers closer to local communities, helping users resolve domain names more quickly.[14] As an example, Packet Clearing House (see www.pch.net) provides secondary DNS service to registries (both ccTLDs and gTLDs), allowing registries to distribute their DNS services across multiple regions and exchange points.

If costs permit, registries should consider implementation of Anycast services (see, BCP 126, ftp://ftp.rfc-editor.org/in-notes/bcp/bcp126.txt) to increase the availability and improve response times for queries of records in their TLD zones. Anycast is a service that increases the redundancy of DNS servers through multiple, discrete, autonomous locations. If a registry can afford multiple locations, the incremental cost of implementing Anycast is not onerous. A recent article in the Internet Protocol Journal (Vol 10, No. 1), provides useful information on the issues of geographic diversity of DNS infrastructure distribution (see http://cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-1/101_dns-infrastructure.html).

While specifically for root server operators, BCP 40, RFC 2870, (ftp://ftp.rfc-editor.org/in-notes/rfc2870.txt), provides best current practices on Root Name Server Operational Requirements. This document may be useful for registry operators in the operation of DNS servers and TLD zone files.

3.3 Shared Registration System

The Shared Registration System (SRS) is the software (clients and servers) provided by a registry to facilitate the registration of domain names, updates to nameservers, contact information and overall management of a registry. The SRS is used by registrars to connect to

[14] VeriSign DNS Management Best Practices data sheet, http://www.verisign.com/static/002104.pdf.

the registry, and "its purpose is to create an environment conducive to the development of robust competition among domain name registrars."[15]

The SRS refers to the ability of Registrars to add, modify, and delete information associated with domain names, nameserver, contacts, and Registrar profile information. This service is provided by systems and software maintained in coactive redundant data centers. The service is available to approved Registrars via an Internet connection, and may include a web-based interface for registrars.

3.4 Whois Service

Whois service consists of Port 43 Whois protocol interface and a web-based user interface to all publicly accessible domain name registration records. The Whois service contains registrant, administrative, billing and technical contact information provided by registrars for domain name registrations. A registry may operate as either a "thick" or "thin" registry. A "thick" registry is one that displays in Whois authoritative information for a domain name received from a registrar. A "thin" registry will only display the information showing the registrar of record, creation date, and nameservers.

With the 'thin' model, only the operational data about each domain is stored in the central registry database while contact data and billing information is maintained by the registrar sponsoring the domain name. The registry only knows the mapping from a domain name to a registrar, and the associated name servers. Whois services operated by the registry publish that mapping; the registrant's identity is then published by the registrar.

In a "thick" registry model, registrant data is retained by the registry in its centralized database. This is useful in the event of registrar failure as the registry would have a copy of relevant registrant data in its "thick" Whois service.

3.5 Registrar Billing and Accounting Information

Registrar billing and accounting information is maintained by a registry for the registration of domain names, provisioning of services, refunds for necessary grace period deletions, transfers. Billing information includes accounts for each registrar accredited to operate with the registry, account balance information, present book entries, billing events associated with particular domains, registrar wire information or letters of credit. Registries only have the billing data in regard to their registrars and registrar accounts, and do not have any private customer billing data.

3.6 Data Security and Data Escrow

ICANN requires gTLD registries under contract with ICANN to escrow registry data. Registry data escrow helps to ensure continuity of service for registrants in the event of a registry failure. For the purposes of this report, registry data escrow is included with other measures employed by the registry to provide security and stability for the TLD. For more information on ICANN's gTLD registry data escrow requirements, see http://www.icann.org/announcements/announcement-05mar07.htm.

[15] Melbourne IT Help Centre, definition of SRS, http://www.melbourneit.com.au/help/index.php?questionid=53.

A registry should implement measures to mitigate “the unauthorized disclosure, alteration, insertion or destruction of Registry Data”, that is not compliant with applicable relevant standards published by the IETF, or that “creates a condition that adversely affects the throughput, response time, consistency or coherence of responses to Internet servers or end systems, operating in accordance with applicable relevant standards.”[16]

In response to the registry data escrow report and the draft Registrar Data Escrow specifications[17] published on 17 May 2007, SSAC, data escrow providers and gTLD registries suggested improvements to the escrow requirements and recommended best practices such as:

- Escrow of all information that would be required to recreate the registration and restore service to registrants
- Escrow of all data fields specified in EPP 1.0 (Extensible Provisioning Protocol, see RFC 4930)[18]
- Status of the name registration
- Any registration “features” (locks, domain proxy, etc.)
- Transactional data
- Use of a standard, non-proprietary electronic file format, such as XML
- Stored data encryption and data transmission encrypted
- Data signing
- Digitally signed deposits
- Verification of incoming data deposits
- Escrow agent certification and annual certification test
- A requirement in the data escrow agreement that escrow agent notify the registry (and registry services provider, if applicable) if an escrow deposit is not received
- Data placed in escrow should be tested to ensure that the data can be used to restore registry operations

ICANN will be issuing an update on the data escrow report as part of this project describing potential improvements to the data escrow requirements.

3.7 IDN Tables

ICANN has made a commitment to Internationalized Domain Names (IDNs). ICANN’s Affirmation of Responsibilities[19] states that “ICANN shall maintain and build on processes to ensure that competition, consumer interests, and Internet DNS stability and security issues are identified and considered in TLD management decisions, including the consideration and implementation of new TLDs and the introduction of IDNs.”

For registries that allow for the registration of IDNs, it is important that these registries also ensure that the IDN tables and languages supported are also protected as a registry resource. gTLD registries that observe the IDN guidelines will make definitions of what constitutes an IDN

[16] From the definitions of security and stability, .ORG Registry Agreement, Section 3.1(d)(iv)(G), http://www.icann.org/tlds/agreements/org/registry-agmt-08dec06.htm#3.1.d.iv.

[17] http://www.icann.org/announcements/rfp-registrar-data-escrow-svs-17may07.pdf.

[18] RFC 4930, ftp://ftp.rfc-editor.org/in-notes/rfc4930.txt.

[19] Affirmation of Responsibilities, http://www.icann.org/announcements/responsibilities-affirmation-28sep06.htm (approved by the ICANN Board on 25 September 2006 and incorporated as Annex A in the Joint Project Agreement between the U.S. Department of Commerce and ICANN, http://www.icann.org/general/JPA-29sep06.pdf).

registration and the associated registration rules available to the IANA Repository for IDN Tables (http://www.iana.org/assignments/idn/index.html). In the event that a registry is transitioned to another operator, this will assist the caretaker or acquiring operator with the maintenance of the existing registrations and the operation of the registry going forward.

The protection of IDN tables should be a priority for registries that accommodate IDNs today, and the tables as well as any other IDN-related data and registry processes should be considered in defining registry failover.

3.8 DNSSEC Keys

The DNS Security Extensions (DNSSEC) enable DNS administrators and registry operators to digitally sign their zone data using public-key cryptography. This provides a layer of security to the zone and is designed to provide "origin authentication of DNS data, data integrity and authenticated denial of existence."[20] For registry operators that adopt DNSSEC and sign their zones, it is expected that those registries will follow the DNSSEC Operational Practices to secure the zone keys for their TLD. RFC 4641 is the most current draft of the DNSSEC Operational Practices (see ftp://ftp.rfc-editor.org/in-notes/pdfrfc/rfc4641.txt.pdf). This is an area for further work and study.

Registry failover issues for registries that have signed their zone with DNSSEC will be addressed in a separate document.

4. TLD Transition

4.1 Historical provisions in ICANN Agreements

Since ICANN's inception, all gTLD registry agreements have contained language on transition following termination of TLD registry operations. Amendment 19 to the Cooperative Agreement between NSI and the US Department of Commerce (http://www.icann.org/nsi/coopagmt-amend19-04nov99.htm) provided for transition of the .COM, .NET and .ORG TLDs to a successor registry (see http://www.icann.org/nsi/nsi-registry-agreement-04nov99.htm#22 and http://www.icann.org/nsi/coopagmt-amend19-04nov99.htm#IB8).

4.2 Current transition provisions in gTLD registry agreements

ICANN's current registry agreements provide mechanisms for transition of a TLD from one operator to another in the event of termination of the registry agreement. This is an area for further study. A number of registry agreements enable TLD transition in the event of 1) termination of the registry agreement by ICANN, 2) bankruptcy, 3) transition of registry upon termination of agreement, 4) breach of the agreement, or 5) failure to perform in good faith. This provision is reflected in all of the new gTLD agreements signed since 2005.

The .MUSEUM sponsorship agreement also contains additional language on termination (see section 5.4, http://www.icann.org/tlds/agreements/sponsored/sponsorship-agmt-16oct01.htm), e.g., in the event that the sponsor is convicted in court of a felony or other serious offense related to financial activities, is disciplined by the government of its domicile for conduct involving dishonesty or misuse of funds of others, or "Sponsor acts or continues acting in a

[20] Explanation from DNSSEC.net; further information on DNSSEC is available in RFCs 4033, 4034, 4035, 4310, 4398, 4471 and 4641.

manner that ICANN has reasonably determined endangers the stability or operational integrity of Registry Services, the DNS, or the Internet after receiving three days notice of that determination." This provision states that ICANN can terminate the relationship, but does not explain how it will ensure that registrations and name service will persist.

The current .AERO sponsorship agreement states that upon the conclusion of the sponsorship agreement, "Sponsor shall make (and shall require Registry Operator to make) all commercially reasonable efforts to cooperate with ICANN, and with any party designated by ICANN to succeed Sponsor, to facilitate prompt and smooth transition of the sponsorship and operation of the Sponsored TLD."[21]

The .MOBI Registry Agreement contains a provision for termination by the registry operator in Section 6.1(b): "Registry Operator may terminate this Agreement and its designation as Registry Operator for the TLD pursuant to 120 days prior notice in writing to ICANN, and subject to compliance with Section 6.4 hereof." See http://www.icann.org/tlds/agreements/mobi/registry-agmt-mobi-01jan07.htm.

The .NAME and .PRO registry agreements also contain a provision limiting merger, consolidation or reorganization.[22]

> During the Term of this Agreement, Registry Operator shall not: (1) merge, consolidate or otherwise reorganize into or with a Registry Operator for a TLD that has more than 10,000,000 Registered Names under management, or any of its affiliates; or (2) sell or otherwise transfer all of its assets or stock to a Registry Operator for a TLD that has more than 10,000,000 Registered Names under management, or any of its affiliates. Registry Operator may merge, consolidate or otherwise reorganize into or with a (1) Registry Operator that has less than 10,000,000 Registered Names under management, or (2) a domain name registrar, only upon the express written consent of ICANN, which consent may not be unreasonably withheld or delayed. In considering whether to give consent, ICANN may consider Concepts 3, 5 and 6 in Appendix U to this Agreement.

The provisions on termination do not specify how ICANN would transition a registry in the event that termination is invoked. This is an area for further study.

4.3 Examples of Transition from gTLDs

4.3.1 Transition of .ORG from VeriSign to Public Interest Registry

The experience in transition of the .ORG TLD from VeriSign to Public Interest Registry (PIR) in 2002-2003 may be helpful in identifying issues involved in moving operation of a TLD from one entity to another. In the case of .ORG, PIR was selected to operate the registry as the result of an open submission process, and the transition was effected with cooperation from all parties. At the time of the transition, there were approximately 2.6 million domain names registered in .ORG. A broad summary of the steps used in this transition is included below. The complete transition plan is detailed in Appendix J to the .ORG Registry Agreement (see http://www.icann.org/tlds/agreements/org/registry-agmt-appj-24oct02.htm).

[21] Section 5.1.3, .AERO Sponsorship Agreement (17 December 2001), http://www.icann.org/tlds/agreements/sponsored/sponsorship-agmt-05nov04.htm.

[22] .PRO Registry Agreement, Appendix W.2 (4 March 2002), http://www.icann.org/tlds/agreements/pro/registry-agmt-appw-04mar02.htm.

The transition plan used for the .ORG TLD provides a baseline for transition scenarios. Further study of TLD transition should examine scenarios and issues such as:

- Lack of cooperation between the current registry operator and the designated successor
- Data is lost or integrity of the data is in question
- The continuing and overlapping name service arrangements, and the duration of those arrangements

All pre-existing .ORG registrars wishing to continue to operate in .ORG were required to enter into a Registry-Registrar Agreement (RRA) with PIR. While the majority of registrars completed this step in a timely manner, a small number were unresponsive or stated they did not wish to enter into an agreement with PIR and did not wish to continue selling .ORG names. Further study of TLD transition should examine whether there are lessons that can be learned from the way PIR and VeriSign handled the .ORG transition.

For the first 25 days of the transition period, VeriSign continued to operate the .ORG registry as a subcontractor to PIR. Registry data was provided to PIR according to the specifications laid out in the agreement, so that internal testing could take place. A test environment was also available for registrars to complete Operational Test and Evaluation (OT&E) prior to the cutover. On 25 January 2003, the operation was shifted from VeriSign to Afilias (PIR's back-end provider). There was an outage of approximately 7 hours on this date, during which registrars were not able to send changes to the registry. Once the shift was completed, registrars then completed testing and began once again to send change requests via the Registry-Registrar Protocol (RRP).

PIR then began the migration from RRP to EPP (Extensible Provisioning Protocol, see RFC 4930), over the course of 2003. PIR handled the transition through a project plan by dividing the registrars into groups so they could go through the OT&E and do any troubleshooting on a group-by-group basis. There were delays resulting from registrars making the transition from RRP to EPP. Registrars generally viewed this transition as an investment of resources that did not provide any additional benefit for them or their customers.

PIR was contractually required to discontinue RRP on 1 January 2004. The final group to make the transition at the end of 2003 consisted of registrars who had previously been unresponsive to multiple notices from the registry. ICANN staff assisted in this matter on an ad hoc basis by personally contacting these registrars to inform them of the necessity of completing this migration to avoid cut-off of their access to the registry. Future transitions would benefit from a clearly documented process that provides instructions and notices to registrars.

Once all registrars were accessing the registry via EPP, registrars went in and updated the Whois records on all .ORG domain names to include the thick data.

Through the overall process, two existing registrars having current .ORG registrations elected not to sign a new RRA with PIR. These registrars made arrangements with other accredited registrars willing to sponsor the names. The registrars then submitted a bulk transfer request which was approved by ICANN and implemented by the registry.

In the overall process, six registrars had not made the transition from RRP to EPP by the time RRP was shut off (with approximately existing 1500 domain names belonging to these registrars). This was handled by PIR/Afilias developing a web-interface tool that would allow registrars to connect to the registry using EPP even if they had not yet migrated from RRP.

The transition plan included contingency plans in the event of failure at any phase of the cutover. Additionally, VeriSign had a contractual obligation to provide backup services and facilities to the successor Registry Operator (PIR) until the end of 2003. VeriSign continued to provide nameservice for the .ORG TLD until August 2003. VeriSign also continued to perform backup of the .ORG zone files until December 2003.

4.3.2 Change of backend registry operator - .AERO

When .AERO was launched in 2002, SITA, the sponsoring organization for .AERO, appointed SITA INC BV to serve as the registry operator. SITA INC BV outsourced the operation of certain registry functions to CORE. Under the terms of its sponsorship agreement, SITA was obligated to locate a new registry operator within four years of being awarded the sponsorship of .AERO. SITA issued an RFP to select a new registry operator on 6 July 2005 (http://www.information.aero/news/2005-07-05-01).

In January 2006, SITA announced the selection of Afilias to be its new backend registry operator. Public announcement of the result is available at http://www.information.aero/news/2006-01-11-01. The lesson to be learned from this transition is that it was a change of operator where no staff were transferred along with the registry.

4.3.3 Change of backend registry operator - .COOP

The .coop gTLD Registry Operator was originally Poptel Ltd, a worker's cooperative in the UK. After the initial launch period, Poptel ownership was transferred and management became investor-owned. According to the Sponsoring Organization, although the investor was fully in support of the .coop TLD, the investor wanted to change the focus of the business, so the investor sought new owners for the registry operator and registrar businesses. Eventually the businesses were purchased by the Oxford, Swindon and Gloucester Co-operative Society, LTD. in the UK.

According to Carolyn Hoover at DotCooperation, “All staff were initially transitioned to the new owner although turnover to existing staff within OS&G started almost immediately. All hardware and software were conveyed intact to OS&G including transitioning of support contracts with existing vendors for various outsourced facilities required to support the registry functions. OS&G also signed new agreements with all .coop registrars to ensure the recognition of the transfer from those business partners.” The sale was commenced on September 1, 2004 and the transition to new systems and staff was completed by April, 2005. There was no disruption during the transfer to registrants or registrars.

In September 2006, OS&G merged with another co-op in the UK to form Midcounties Co-operative Society. There was no specific change to the registery operator system or staff related to that merger although a specific entity, Midcounties Co-operative Domains was created to specifically run the registry operator business as opposed to other software systems supported by the co-op. The lesson to be learned from this transition is that it involved a business unit divestiture by Poptel and acquisition by OS&G. Operations and staff changed ownership but did not change how the registry was operated.

4.4 Examples of Transition from ccTLDs

On 26 April 2006, Afilias completed the transition of registry services from VeriSign for Belize's .BZ ccTLD (see http://domaintimes.net/newseng.php?mhnews_id=306&mhnews_newsid=8678&mhnews_page=1). Afilias transitioned 35,000 domain names and assumed responsibility for all backend registry services. The lesson to be learned from this transition is that it was the transition from one experienced registry operator to another.

Other ccTLD transition examples include the transition of .US from VeriSign to NeuStar in 2001[23], and the transition of .AU from auDA to AusRegistry in 2001 (see http://www.ausregistry.com.au/news/news84.php).

JPRS has a plan in place for the transition of the .JP ccTLD from JPNIC. The plan originates from the JPRS-JPNIC Memorandum of 9 November 2001 (see http://www.iana.org/cctld/jp/jprs-jpnic-memorandum-09nov01.htm) and the ccTLD Sponsorship Agreement of 27 February 2002 (http://www.icann.org/cctlds/jp/sponsorship-agmt-27feb02.htm).

Some ccTLDs outsource their backend operations to third party providers. Many of these providers maintain backend registry operations for several TLDs. This is an important model to explore because of the potential for the simultaneous failure of multiple registries having a common operator.

ICANN is interested in collecting more information on the experiences of ccTLD managers in the transition of ccTLDs from one operator to another. The IANA redelegation reports, posted at http://www.iana.org/reports/cctld-reports.htm, provide information on redelegation of ccTLDs from one manager to another, but may not necessarily capture examples of transition of registry operations from one operator to another. ICANN welcomes input from ccTLD managers in this area.

5. Failure Scenarios

A number of recent events demonstrate the need for the development by ICANN of a comprehensive registry failover plan. The plan will also be important in the launch of new gTLDs. The GAC Principles on New gTLDs recommend that ICANN establish clear continuity plans for maintaining the resolution of names in the DNS in the event of registry failure.

This report is only intended to examine potential registry failure scenarios, and is not intended to address issues related to potential registrar failure. Registrar examples are only included to demonstrate potential failures.

Any scenarios not included in the report should be submitted for discussion in the comprehensive plan.

- Temporary Failures
- Long Term Failures

- Business/Financial Failures
- Technical Failures
- Other Failures as described below

[23] NeuStar's transition plan for .US was included in its proposal to NTIA in 2001. See http://www.ntia.doc.gov/ntiahome/domainname/usca/cafiles/SectionT.pdf.

Failure scenarios can be divided into temporary and long-term failures. A temporary failure is defined as a registry failure where there is certainty of recovery in a reasonable period of time. As mentioned previously, there was a seven hour loss of service in January 2003 when VeriSign and Afilias transitioned the .ORG TLD. This was a scheduled outage. An example of an unscheduled temporary failure occurred in mid April 2007, when a software update to the servers that maintain the network for Blackberry email service failed, preventing millions of subscribers from accessing email through Research in Motion (RIM)'s Blackberry service for at least nine hours (see http://news.bbc.co.uk/2/hi/business/6574767.stm). According to the statement released by RIM, the failover plan for responding to the software outage "did not perform to expectations" (see http://www.latimes.com/business/la-fi-blackberry21apr21,1,4979713.story?ctrack=1&cset=true).

An example of a temporary failure at a registry occurred on 29 August 2006. ESNIC, the manager of Spain's .ES ccTLD, reported a two-hour software outage that took the .ES registry offline (see https://www.nic.es/noticias/notas/nota_desarrollada.html). As many as 400,000 were offline as Internet users were unable to access domain names ending in .es (see http://news.netcraft.com/archives/2006/08/30/thousands_of_spanish_web_sites_knocked_offline_by_software_error.html).

Failures may also be further divided into business/financial failures and technical failures. The category of Other Failures has been included as to cover those failures that do not fit in the business/financial and technical categories.

5.1 Business/Financial Failures

As with any business, registry operators must properly manage financial assets, funding and cash flow or face potential financial failure. Businesses and entities interested in entering the registry market should study the examples set by current registry operators in order to understand the business of domain names. Business failure examples include bankruptcy, buy-out, loss of funding, liquidation, management failure, marketing failure, litigation-related or induced failure or termination of payment processing capability.

The ICANN Board discussed business failure of gTLD registries during the public forum of the ICANN meeting in Luxembourg, 14 July 2005 (see http://www.icann.org/meetings/luxembourg/captioning-pf2-14jul05.htm). One public comment asked "what happens if one [of these] new TLD[s] goes bankrupt?" The response was that registry failure should be considered in the process for new gTLDs, and that as a topic, it has received "very specific and direct attention."[24]

Former ICANN Board member Michael Palage released a White Paper addressing the subject of registry business/financial failure in August 2005 (see http://forum.icann.org/lists/new-gtld-questions/msg00006.html). A partial list of his recommendations includes:

- All registry operators be required to operate on the current EPP standard
- ICANN listed as direct beneficiary of data escrow agreement, with active script verification and periodic download
- ICANN access to zone files
- Education on existence and function of Auth Codes

[24] Response to question made by Steve Crocker, see bottom of transcription, http://www.icann.org/meetings/luxembourg/captioning-pf2-14jul05.htm.

- Bonding requirement
- Discussion of “thick” vs “thin” registries

The Palage paper identified two main failure scenarios, business failure of registry requiring transition to a new operator (requiring selection of a caretaker and eventual selection of successor registry) and failure of registry operator with wind down of operations (where no registry successor can be found).

Examples of business/financial failure include:

- Marketing Failure
- Litigation-related Failure
- Termination of payment processing capability
- General Business Failure

5.2 Technical Failures

This section describes potential technical registry failure scenarios, both temporary and permanent. Natural disasters and human acts (operator error and malicious activities) could cause a technical failure to a registry. As new gTLDs are added in more diverse locations worldwide, as part of the application process, registries should provide detail on planned responses to technical failures that may be common to their base of operations.

As an example, Appendix 7 of the .COM Registry Agreement (http://www.icann.org/tlds/agreements/verisign/appendix-07-01mar06.htm) defines a “Core Internet Service Failure” as “extraordinary and identifiable events beyond the control of Registry Operator affecting the Internet services to be measured pursuant to this section, including but not limited, to congestion collapse, partitioning, power grid failures, and routing failures; DNS Name Server unavailability shall mean less than four (4) sites on the Registry Operator’s constellation are returning answers to queries with less than 2% packet loss averaged over a Monthly Timeframe”.

5.2.1 Natural Disasters

A natural disaster may have a devastating financial impact on a registry, even if it has a well-developed registry failover plan. This is particularly in the case where a nation is unable to cover the costs of rebuilding key infrastructure needed to maintain registry operations. Examples follow.

5.2.1.1 Earthquakes

The 26 December 2006 earthquake off the coast of Taiwan cut undersea cable connecting Taiwan and mainland China. The earthquake cut off Internet access to millions. TWNIC (the registry operator for Taiwan’s .TW ccTLD) did not lose DNS services, and had just tested their registry failover procedures in November 2006. JPRS in Japan did not lose connectivity.

A strong earthquake could cause a temporary failure for a registry. A registry located in an earthquake-prone location should have contingency plans in place to ensure continuity of operations.

5.2.1.2 Hurricanes

Hurricane Katrina (23-31 August 2005) is estimated to be responsible for over $75 billion USD in damages. When Hurricane Katrina hit New Orleans 27-30 August 2005, it caused a temporary failure to ICANN-accredited registrar Intercosmos Media Group. Intercosmos was able to avoid a prolonged outage because it had a plan for the backup of critical registrar resources. Although Intercosmos is a registrar, it may serve as an example for registries facing potential disaster scenarios.

5.2.1.3 Tsunami

While no registries are currently located in a tsunami-danger zone, future registry operators in tsunami-prone areas should have contingency plans in place to ensure the stability of registry operations.

5.2.1.4 Blackout/Energy Failure

On 14 August 2003, the largest blackout in North American history affected over 10 million people in Ontario, Canada and over 40 million people in eight states from Ohio to New York. On 28 September 2003, a blackout hit all of Italy except for Sardinia for 9 hours and part of Switzerland near Geneva for 3 hours, knocking out power for 56 million people. In particular, blackouts and power failures were noted in the technical Evaluation Team's comments during the sTLD round (see report http://www.icann.org/tlds/stld-apps-19mar04/PostAppD.pdf, page 5).

In the future, a similar large-scale power outage could impact registry operators that have not implemented protections against localized outages at registry operations centers.

5.2.1.5 Other Potential Natural Disasters

Other potential natural disasters that may cause a technical failure include: tornadoes, fire, and snowstorm/blizzard related power outages.

5.2.2 Human Acts

Registries are vulnerable to many forms of human acts ranging from internet-based attacks against their registration and name service infrastructures to operator and configuration errors. Both temporary and permanent failures may result from such acts. Examples follow.

5.2.2.1 Malicious acts

On 6 February 2007, a distributed denial of service attack affected six of the thirteen root servers that form the foundation of the Internet. A factsheet on the attack is available at http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf. The use of Anycast (http://en.wikipedia.org/wiki/Anycast) by root server operators helped prevent a major disruption to Internet operations.

In March 2006, a distributed denial of service attack was launched on a number of root servers, registrars and registry operators. The attacks temporarily impacted accredited registrars in Germany and in the United States.
http://www.macworld.com/news/2006/04/04/network/index.php and
http://www.pcworld.com/article/id,125554-page,1-c,applicationbugs/article.html. Combined, the

registrars had approximately 8,000,000 domain names under management (approximately 11.5% of active domain name registrations as of 11 May 2006).

On 31 March 2006, ICANN’s SSAC released an advisory on DNS Distributed Denial of Service Attacks (see http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf). The advisory made a number of recommendations for Root and TLD Name Server Operators. These recommendations could also be employed by the registry operators.

Afilias informed ICANN that in the first quarter of 2004, surges of abusive transaction requests to its SRS servers for .INFO and .ORG caused extended transaction times beyond stated service level agreement requirements. These delays were caused by contention for released domain names (deleted domain names) in .INFO and .ORG.

In response, Afilias formed an emergency task force to examine traffic patterns, identify specific load points and developed software upgrades and hardware recommendations. Afilias also conducted meetings with its registrars and consulted with its rate-limiting equipment vendor

On 17 October 2002, SSAC released a document titled “Securing the Edge” (http://www.icann.org/committees/security/sac004.htm), which described security problems “at the edge” of the Internet and included recommendations for improvement.

There is a concern that terrorist attacks could be planned against critical infrastructure resources worldwide. A targeted attack on a registry, network operations center or power center could cause a technical failure of a registry operator.

gTLD registries and technical staff identified other categories of Internet-based attacks may include malicious code, asset-driven criminal attacks, spam, phishing, adware and spyware, and browser flaws.

5.2.2.2 System Failure

A system failure – resulting from a hardware or software failure, or configuration error - could disrupt any or all the services a registrar or registry operator provides. A system failure is likely to be a temporary failure.

Other potential system failures may include:

- Applications-cluster processor fails
- EPP/RRP server processor fails
- Web server processor fails
- Database server processor fails
- Database disk drive fails
- Database crashes
- Authentication server fails
- Whois-cluster processor fails
- Billing and collections server fails
- Internet or VPN link fails
- Router or firewall fails
- Physical site becomes inoperable for more than 24 hours
- Both the primary and secondary data centers become inoperable

- Operating system or application software fails
- Operating system configuration errors
- security system configuration errors
- Name, web, database, and transaction server configuration errors

5.2.2.3 Infrastructure problems

Poor or insufficient infrastructure, whether within or beyond the control of the registry, may cause a temporary failure for a registry. Local infrastructure conditions should be considered in registry contingency planning. Potential infrastructure problems may include:

- Insufficient capacity
- Insufficient diversity and redundancy in WANs (access circuits), LAN infrastructure (switching), security systems, applications servers and storage facilities
- Power facilities
- HVAC facilities

5.2.2.4 Name server problems

The operation of nameservers is a critical function of a registry. In the event that IANA notices the nameservers for a registry are offline, IANA attempts to contact the registry and assist with restoring service.

Such failures could include loss of primary database server, which would result in switchover of the registry to a secondary database server. In the event of multiple database server failures, a registry could switchover to a mirror site, if one was available.

Some registries provide advance notice of outages, in order to avoid disruption to users.[25]

5.3 Other Failure Scenarios as described below

There are a number of potential failure scenarios involving direct government intervention that do not clearly fall under the category of financial, business or technical failure. While many of these scenarios are unlikely at this time, as ICANN approves new TLDs in the future, the potential for government involvement in registry operations may arise.

5.3.1 Government Takeover/Coup

A change of government by takeover, revolution or coup could lead to instability or failure for a registry operator. Political instability has not to date had a direct impact on registry operations, but direct intervention by governments into registry operations could occur in the future. The GAC and GNSO may wish to address this issue.

5.3.2 Regulatory-imposed shutdown

A court, government or government agency could attempt to order a registry operator to halt its operations. The GAC, GNSO and ICANN Board may wish to examine this issue in greater detail.

[25] An example of a ccTLD providing notice of planned outages is AusRegistry's planned outages page, see http://www.ausregistry.com.au/outages.php.

5.3.3 Government Seizure of Registry Operator

A government could assume control over a registry operator, either through seizure of registry operations or nationalization of operations. Re-delegation of ccTLDs from individuals to government agencies provide examples of government assumption of control over registry operations. Re-delegation of a registry should include measures to ensure stable transition of registry operations.

A seizure of operations could occur in a manner that results in loss of registry data, registrant contact information or damage to nameservers. A seizure could result in a temporary or long term failure of a registry or the transition of a registry to a new operator. A registry operator could be adversely affected by an order from a government to remove the registry's TLD from the root zone maintained by IANA.

The IANA consideration of a hostile redelegation focuses on the competencies of the new operator to provide a stable service, but also the ability to transfer both DNS zone information, and relevant customer records, to the new registry. IANA expects the new operator to have a transition plan to perform the transfer without undue hardship to registrants, or undue instability to the ccTLD. There would need to be benefit outweighing any risk in such a change.

The competencies of the new operator include technical and operational competency, government support and local Internet community support. The operator must also demonstrate they will operate in a fair and equitable manner.

6. Elements of the Registry Failover Plan

In order to provide guidance to the development of the comprehensive registry failover plan, ICANN is seeking input from all interested stakeholders on the issues described in this report. The scenarios described in this report are intended to serve as examples that will help inform and guide failover plan development. A definition of failure should be developed, and ICANN's role in the event of failure should be clearly established. The registry failover plan should incorporate measures that minimize the risk to a domain name registrant should a registry cease operation and the registrant's domain name cannot be resolved.

Considerable additional study is needed to develop a robust registry failover plan. However, based on the critical functions, transition experiences and failure scenarios described in this (interim) report, registries should consider at least the following measures:

I. Provide for geographic diversity of name servers and have contingency plans in place. Include diversity and contingency progress and status reports in monthly reports to ICANN.

II. Document contingency plans, provide this documentation on a confidential basis to ICANN for review and consultation, and test the plans on a periodic basis.

III. Document archival and accuracy measures performed during the monthly reporting period, and information regarding incidents (e.g., problems completing zone changes, and attacks against the registry infrastructure).

IV. With ICANN, establish a clear communication plan for informing affected registrants, registrars, users and Internet community in the event of a registry failure. Commmunicate the reasons for the failure and available options.

V. As part of the new gTLD process, applicants should submit a TLD transition plan which identifies the critical functions of the registry and describes how each of those functions would be transitioned to a new operator in the event of registry failure This plan may include the identification of a back-up or temporary provider. The applicant may designate this section of the gTLD agreement or application as confidential. The transition plan is to be retained by the registry as part of the registry's overall failover plan. The transition plan requirement follows the recommendations in the GAC Principles on New gTLDs related to registry failover and continuity practices for new gTLDs.

VI. A clearly documented transition process:
   a. that provides instructions and notices to registrars,
   b. requirements for data accuracy measures, and
   c. a contingency plan for registrars that do not become accredited in the successor registry.

VII. Registries may consider establishing a bond to provide necessary financial resources to a temporary provider until a successor registry is named.

7. Areas for Further Study and Recommendations for ICANN

In the event of registry failure, ICANN should identify the type of failure as a technical, business or other failure and determine whether the failure is long-term or temporary. A temporary failure would trigger an established set of responses from ICANN, while a long-term failure would trigger a different set of responses.

ICANN should define metrics for failover in the gTLD registry agreements to the same degree that it does for DNS availability. Failover practice and testing obligations in gTLD registry agreements should be clarified.

ICANN should consider convening advisory panels, including members of the technical community and constituencies. ICANN's Security and Stability Advisory Committee may provide assistance in its role as an advisory committee to the Board and convene quickly in the event of a registry failure. This assistance may include advice on the level of ICANN involvement in a given situation.

In addition, a constituency based advisory group consisting of a small number of members from the Registry Constituency and ccTLD managers may serve as a standing team to provide guidance in the event of a registry failure. This team could suggest best practices for registry operations as well.

ICANN should establish a process for designating a replacement registry operator. In the event that a replacement cannot be found, ICANN should have a process for closing registry operations.

TLD transition should be studied in greater detail, and ICANN should look closely at the transition and termination provisions in the existing registry agreements to determine whether these provisions should be clarified.

The provisions on termination do not specify how ICANN would transition a registry in the event that termination is invoked. This is an area for further study.

Further study of TLD transition should examine scenarios and issues such as:

- What would happen if there was lack of cooperation between the current registry operator and the designated successor or a hostile reassignment of a registry?
- Data is lost or integrity of the data is in question.
- The continuing and overlapping name service arrangements, and the duration of those arrangements.
- A determination should be made on the standard metric for outage of registry services in a transition from one operator to another.
- What registrar testing should occur in the event of TLD transition?
- ICANN’s role in transition should be defined.
- How registrars and registrants are notified of the transition should be defined.
- Failure scenarios involving DNSSEC keys and signed zones.