DRAFT ICANN gTLD Registry Failover Plan
Best Practices Recommendations

Patrick Jones
20 October 2007

1 Executive Summary

The 2006 ICANN Strategic Plan (Section 1.1.2 and 1.1.6-7) set forth as one of the key goals implementation of "procedures for dealing with key business failure of key operational entities," including contingency plans for registry failover in order to appropriately protect registrants (this project was carried over into the 2007-2008 ICANN Strategic Plan as Section 1.10.1).

The Operational Plan states that a key goal 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."

ICANN has conducted significant research and outreach on registry failover. Based on community input received on the 1 June 2007 Registry Failure Report and Protections for Registrants Workshop in San Juan, Puerto Rico, ICANN has developed a draft gTLD Registry Failover Plan. The plan includes the delivery of best practices recommendations for registry failover mechanisms for gTLD registries.

The best practices recommendations will be incorporated into ICANN's draft base contract for new gTLDs, and incorporated into existing gTLD registry agreements as they are renewed.

2 Glossary

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.[1]

- 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

[1] Liu & Albitz, DNS & BIND, 5th Ed. (May 2006), page 22.

stored in the domain namespace, including Start of Authority records, NS (nameserver) records, Address records, and PTR (pointer) records.[2]

- 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.[3]

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

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."[4]

"These registries have typically served two main domain functions: as the registry for a gTLD or as a registry for a ccTLD. In some instances, one entity will operate multiple TLD's, both of the gTLD and ccTLD type. A gTLD or ccTLD domain registry operator may be a governmental entity, non-governmental, non-commercial entity, or a commercial entity."[5]

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]

2.4 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/.

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).

---

[2] Id., page 16, 55-61.
[3] Id., page 26.
[4] Id., page 41.
[5] RFC 3707, 2.1.1, ftp://ftp.rfc-editor.org/in-notes/rfc3707.txt.
[6] Id., page 41.
[7] http://www.rfc-editor.org/rfc-online.html.

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).

RFC 3707, Cross Registry Internet Service Protocol (CRISP) Requirements, (ftp://ftp.rfc-editor.org/in-notes/rfc3707.txt).

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).

---

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

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 Current Functional and Performance Specifications

All gTLD registry agreements have minimum ICANN-required performance and functional specifications for registry services.[10] These specifications are typically defined in the

[10] .AERO: http://www.icann.org/tlds/agreements/sponsored/sponsorship-agmt-att7-13oct01.htm and http://www.icann.org/tlds/agreements/sponsored/sponsorship-agmt-att6-08sep01.htm
.ASIA: http://www.icann.org/tlds/agreements/asia/appendix-7-06dec06.htm
.BIZ: http://www.icann.org/tlds/agreements/biz/appendix-07-29jun07.htm and SLA at http://www.icann.org/tlds/agreements/biz/appendix-10-08dec06.htm
.CAT: http://www.icann.org/tlds/agreements/cat/cat-appendix7-22mar06.htm
.COM: http://www.icann.org/tlds/agreements/verisign/appendix-07-01mar06.htm and SLA at http://www.icann.org/tlds/agreements/verisign/appendix-10-01mar06.htm
.COOP: http://www.icann.org/tlds/agreements/coop/appendix-7-01jul07.htm
.INFO: http://www.icann.org/tlds/agreements/info/appendix-07-08dec06.htm and SLA at http://www.icann.org/tlds/agreements/info/appendix-10-08dec06.htm
.JOBS: http://www.icann.org/tlds/agreements/jobs/appendix-7-05may05.htm
.MOBI: http://www.icann.org/tlds/agreements/mobi/mobi-appendix7-23nov05.htm
.MUSEUM: http://www.icann.org/tlds/agreements/sponsored/sponsorship-agmt-att6-08sep01.htm and http://www.icann.org/tlds/agreements/sponsored/sponsorship-agmt-att7-13oct01.htm
.NAME: See Appendix 7
.NET: http://www.icann.org/tlds/agreements/net/appendix7.html and SLA at http://www.icann.org/tlds/agreements/net/appendix10.html
.ORG: http://www.icann.org/tlds/agreements/org/appendix-07-08dec06.htm and SLA at http://www.icann.org/tlds/agreements/org/appendix-10-08dec06.htm
.PRO: http://www.icann.org/tlds/agreements/pro/registry-agmt-appc-30sep04.htm and http://www.icann.org/tlds/agreements/pro/registry-agmt-appd-02mar02.htm, SLA at http://www.icann.org/tlds/agreements/pro/registry-agmt-appe-29dec01.htm
.TEL: http://www.icann.org/tlds/agreements/tel/appendix-7-07apr06.htm
.TRAVEL: http://www.icann.org/tlds/agreements/travel/travel-appendix-7-12apr06.htm

performance and functional specification appendices, and cover the use of Extensible Provisioning Protocol (EPP), supported initial and renewal periods, grace periods, nameserver requirements and WHOIS.

4 Critical Functions of a Registry

1. Maintenance of nameservers and DNS
2. SRS
3. WHOIS
4. Registrar Billing and Accounting Information
5. Data security and data escrow
6. IDN Tables (for those registries offering IDNs)
7. DNSSEC keys

ICANN's 1 June 2007 document, *Building Towards a Comprehensive Registry Failover Plan* (http://www.icann.org/registries/reports/registry-failover-01jun07.htm) identified seven critical functions of a registry. The following functions are described in detail with recommendations on best practices for registry failover.

Registries must have their own contingency plans, including the designation of a backup registry operations provider if necessary, to maintain the critical functions of a registry for a period of time:

- To provide recovery and escrow of domain name registration information and registrant account information, so that
- A replacement operator or sponsor can be found and a transfer effected, or
- Absent the designation of a replacement, provide a notice period to registrants that the registry is closing.

Registries should provide contingency plans to ICANN on a confidential basis for review and consultation. Contingency plans must be tested on a periodic basis.

Registries shall have a designated contact person who is authorized to act on behalf of the registry, and who can serve as a point of contact with ICANN on critical registry functions.

The monthly report format should be updated to include diversity and contingency progress and status metrics.

Registries should set aside necessary financial resources, such as a bond, to provide temporary funding of registry functions until a successor registry can be named.

4.1 Maintenance of nameservers and DNS for domains

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.

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. 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. 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 shall 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.[11] 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.

Many gTLD registry agreements define “Core Internet Service Failure" as an extraordinary and identifiable event beyond the control of Registry Operator affecting the Internet services. Such events include but are not limited to congestion collapse, partitioning, power grid failures, and routing failures.

The Registry Operator will use commercially reasonable efforts to restore the critical systems of the Core Services within 24 hours after the termination of a force majeure event and restore full system functionality within 48 hours after the termination of a force majeure event. Outages due to a force majeure will not be considered Service Unavailability.

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

A force majeure event is defined as any loss or damage resulting from any cause beyond [a registry operator's] reasonable control including, but not limited to, insurrection or civil disorder, war or military operations, national or local emergency, acts or omissions of government or other competent authority, compliance with any statutory obligation or executive order, industrial disputes of any kind (whether or not involving either party's employees), fire, lightning, explosion, flood subsidence, weather of exceptional severity, and acts or omissions of persons for whom neither party is responsible. Upon occurrence of a Force Majeure Event and to the extent such occurrence interferes with either party's performance of this Agreement, such party shall be excused from performance of its obligations (other than payment obligations) during the first six months of such interference, provided that such party uses its best efforts to avoid or remove such causes of nonperformance as soon as possible.

ICANN recommends an update to the functional and performance specifications in gTLD registry agreements to be current with accepted standards.

4.2 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 the registry, and "its purpose is to create an environment conducive to the development of robust competition among domain name registrars."[12]

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.

4.3 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.

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

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.

4.4 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.

4.5 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.

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."[13]

In response to the registry data escrow report and the draft Registrar Data Escrow specifications[14] 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)[15]
    - Escrow of status of the name registration
    - Escrow of Any registration "features" (locks, domain proxy, etc.)
    - Escrow of 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

[13] 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.
[14] http://www.icann.org/announcements/rfp-registrar-data-escrow-svs-17may07.pdf.
[15] RFC 4930, ftp://ftp.rfc-editor.org/in-notes/rfc4930.txt.

- 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
- Use of an ISP carrier grade data center environment
- Use of a 48 hour service level agreement on data processing and digital signature checks
- ICANN specifying the XML format for all Registries & Escrow Agents
- Verification of incoming data including both digital signature checks AND verification of XML data deposits against ICANN's XML schema
- Escrow agent certification to confirm that escrow agent can perform all contractually required duties
- Support of an ICANN specified format for release of Registry data
- Annual certification test to demonstrate capabilities and compliance with SLA's
- Escrow agent prevented from outsourcing on work related to Registry Data Escrow
- Collection of Zone File information through Zone File Access Agreement
- Use of all data fields currently described in EPP 1.0

These suggested improvements should be discussed in greater detail. ICANN staff is currently reviewing the registry data escrow provisions to be included in the base contract for new gTLDs, and may recommend changes to be incorporated into an updated Registry Data Escrow Specification and updated Registry Data Escrow Agreement.

ICANN recommendations on release of data from escrow include the following:

- Release of escrow should only occur when the registry data is no longer publicly available
- Registry change of ownership
- Notification of bankruptcy
- Sustained inability to meet service or agreement obligations
- Integrity checking and validation
- Technical failure
- Court determination that the registry is in breach of contract
- By agreement of registry and ICANN

ICANN will, in consultation with gTLD registries and the community, define the requirements for accessing data in escrow and the data elements necessary for a successor operator to provide registry services.

4.6 IDN Tables

ICANN has made a commitment to Internationalized Domain Names (IDNs). ICANN's Affirmation of Responsibilities[16] states that "ICANN shall maintain and build on processes to ensure that competition, consumer interests, and Internet DNS stability and security issues are

[16] 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).

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

4.7 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."[17]

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.

5 Transition Elements

5.1 Current 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. 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 provisions on termination do not specify how ICANN would transition a registry in the event that termination is invoked. ICANN, in consultation with the registries constituency and community, may recommend improvements to gTLD registry agreements to better address transition situations. These recommendations may take the form of an emergency situations policy, and will follow formal consideration of the ICANN gTLD registry failover plan by the ICANN Board of Directors.

5.2 Voluntary Transition

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

As part of the draft ICANN gTLD Registry Failover Plan, ICANN will follow a voluntary transition plan in consultation with the affected registry or sponsor. If a decision is made to voluntarily transition a TLD to a new operator, ICANN and the registry or sponsor shall provide notice to the community of the timeline for transition.

If the registry or sponsor has made a decision to voluntarily transition the TLD, ICANN and the registry or sponsor will agree to work cooperatively to facilitate and implement the transition of the registry for the TLD in a reasonable timeframe (30-90 days), with notice to the community.

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 must include the designation of a back-up or temporary provider, or description of mirror site and contingency plan.

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.

A clearly documented transition process shall provide

a. 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.

ICANN will prepare a Request for Proposals (RFP) for a successor registry operator or sponsor. ICANN will schedule a Board meeting to discuss the transition and intent to seek a successor registry. For sTLDs, ICANN will seek input from the sponsored community on a successor. Applicants must meet certain successor criteria. ICANN will make an effort to post the RFP for at least 21 days, unless there is an urgent need for a shorter period of time.

ICANN will coordinate with the registry or backend provider to ensure smooth transition of the TLD(s) to the successor registry.

5.3 Non-voluntary Transition

In the event that a registry or sponsor cannot continue operations and does not agree with ICANN on voluntary reassignment, ICANN will make a legal determination whether to proceed with the non-voluntary termination process. This process will be managed by ICANN's Office of General Counsel. If the decision is made to proceed with the non-voluntary transition process, ICANN will invoke the breach process based on the terms of the registry agreement and provide notice to the registry or sponsor. The community will be informed of a decision to invoke the breach process.

Under the terms of the gTLD registry agreement, ICANN must provide notice and opportunity to cure or initiate arbitration within thirty calendar days after ICANN gives registry or sponsor written notice of breach.

In the event of a non-voluntary transition, ICANN may invoke the registry data escrow agreement and contact the third party escrow provider for a copy of all escrowed data related to the registry.

5.4 Transition Elements

Transition of a TLD from one registry operator to another should involve the following elements:

5.4.1 Technical transition – data transfer from former registry operator to new operator
5.4.2 Testing by new operator
5.4.3 Parallel nameserver operation
5.4.4 IANA nameserver delegation process
5.4.5 Registrar transition time and testing
5.4.6 Timed cutover from former registry operator to new operator
5.4.7 Data contingency plan during transition
5.4.8 Data migration plan
5.4.9 Notification to the community

In the event of transition, Registry Operator will work in conjunction with ICANN, the registrars constituency and the Internet community at large to maximize the notification process by using a multitude of mechanisms including: the Registry Operator website, a transition website, email announcements; registrar communiqués; press releases, and other methods.