ICANN gTLD Registry Failover Plan
27 November 2007

Section 1.10.1 of the 2007-2008 ICANN Operating Plan states that ICANN will "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."

The 2006-2007 ICANN Operating Plan included the above language and stated that ICANN will "publish a plan supported by the infrastructure and data escrow procedures necessary to maintain registry operation." Based on community input received on the 1 June 2007 Registry Failure Report and Protections for Registrants Workshop in San Juan, Puerto Rico, ICANN developed a draft gTLD Registry Failover Plan.

ICANN published the draft for community input and comment from 20 October to 19 November 2007. ICANN has completed a revised draft plan incorporating feedback received during the ICANN meeting in Los Angeles and during the comment period. Comments are open on this draft until 15 December 2007.

The plan is based on the assumption that ICANN has a role in the event of a gTLD registry failure. gTLD registries must have a contingency plan 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 contact information (if maintained by the registry), 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 registrars and registrants that the registry is closing.

ICANN is coordinating the gTLD registry failover plan with the development of the new gTLD process and other contingency efforts such as the registrar failover plan and Registrar Data Escrow program.

1. Definitions

The following definitions are used to describe the gTLD Registry Failover Plan.
1.1 Initiating Event – The occurrence of an event with the potential to produce an undesired consequence. An initiating event is an event that causes or threatens to cause temporary or long-term failure of one or more of the critical functions of a (gTLD) registry.

Qualifying criteria for such an event may include:

- conditions, if continued for longer than (X time), have been shown, after diligent inquiry including consultation with registry staff, to be likely to cause temporary or long-term failure,
- Severe economic damage to registry services,
- a prolonged and irrevocable situation that cannot be solved by the registry without severe damages caused to the Internet community, and where
- the registry is accountable for the situation.

1.2 Temporary Failure - A registry failure where there is reasonable certainty of data recovery or restoration of service in a short duration of time. A short duration of time may be measured in minutes or hours, with recovery or restoration of service within a maximum of 24 to 72 hours, depending on the type of critical function involved in the failure. A failure involving the resolution

of names and maintenance of nameservers should be measured differently than a failure involving WHOIS service.

1.3 Long-term Failure – A failure rendering a registry or a critical function of a registry inoperable for an extraordinary length of time. An extraordinary period of time may be defined when commercially reasonable efforts fail to restore a registry or critical function of a registry to full system functionality within 24-72 hours after the termination of an initiating event, depending on the type of critical function involved in the failure.

1.4 Critical functions – those functions that are critical to the operation of a gTLD registry. The registry failure report published on 1 June 2007 identified seven critical functions of a registry, although there may be others.

1. Maintenance of nameservers and DNS for domains
2. Shared Registration System
3. WHOIS service
4. Registrar Billing and Accounting Information
5. Data Security and Data Escrow
6. IDN Tables (if IDNs are offered by the registry)
7. DNSSEC Keys (if DNSSEC is offered by the registry)

See http://www.icann.org/registries/reports/registry-failover-01jun07.htm. Within these critical functions there are levels of importance, with maintenance of nameservers and DNS for domains the most critical to the operation of a stable registry. A TLD can operate at a resolution-only level if SRS or WHOIS service is down for a certain period of time.

2. Notification When a Suspected Initiating event occurs

2.1 ICANN learns of or may receive information on a suspected initiating event from a gTLD registry, sponsor, registrar, or other member of the community.

2.2 The suspected initiating event creates a response time line from ICANN staff.

1. Suspected initiating event occurs at time X
2. Notification is provided by Y
3. Y is expected to provide ICANN with as much detail regarding the nature and impact of the event as is available (and practically possible to collect) within the time frame
4. ICANN staff studies information provided during time frame, ICANN responds to the party who notified ICANN, and if appropriate, contacts the registry (if the registry did not already notify ICANN staff)

2.3 Designated registry contacts may inform ICANN of initiating events via a 24/7 telephone hotline.

3. ICANN Preliminary Examination

3.1 ICANN staff conducts a preliminary examination based on facts known of the event. The staff examination may be conducted between members of the ICANN Office of General Counsel, Registry Liaison staff or other staff as appropriate. ICANN staff may also utilize experts with registry experience in this process.

3.2 ICANN staff will contact the designated registry representative, unless the registry has already contacted ICANN staff, to obtain information concerning a suspected initiating event.

4. Communication with gTLD registry or sponsor

4.1 As part of the ICANN preliminary examination, ICANN will attempt to communicate with the designated gTLD registry contact. This contact should be someone with authorization to act on behalf of the registry. The examination should be assessed as an operational issue. Legal issues will be assessed based on the terms of the registry agreement.

If the registry or sponsor can be reached, ICANN (and the gTLD Operator, if such gTLD Operator is cooperative) will attempt to determine the following:

1. The nature and circumstances surrounding the initiating event
2. The cause of the initiating event
3. The severity of the event and whether such event is likely to be temporary or long-term
4. Whether the registry can continue the registry's critical functions
5. Question what, if any, services will be unavailable or operated at a reduced level of service
6. Whether the registry has interim measures in place to protect registry services

The determination on whether a registry can continue its critical functions operations should be made in consultation with the registry. As part of this determination, ICANN may consult with an objective panel of experts on registry functions.

There may be circumstances when a registry can provide limited services (DNS, but not registration or change services) for a temporary period without the need to transition operations to a qualified backup provider. ICANN may utilize a pre-qualification or accreditation process to create a pool of available backup providers.

4.2 If available, the designated gTLD registry or sponsor confirms contact and provides information on the suspected initiating event as a temporary failure or long-term failure, or informs ICANN that no such event has occurred.

4.3 If an initiating event has occurred, the registry or sponsor cannot be reached and a backup registry operations provider is available, ICANN should contact the backup registry operations provider or seek alternative confirmation of the event and contact the third party data escrow provider. At this point, no decision is to be made on transition, only to seek confirmation of the event and secure data for the registry.

a. Execute agreement (or initiate procedure) for release of data from escrow
b. Obtain data from escrow and copy zone (if available) to maintain resolution of names

4.4 If the registry's failover plan activates a backup registry operations provider, the backup provider must make contact with ICANN and confirm the level of service to be provided to registrars and registrants (full service or resolution-only service). ICANN will consult with the backup provider to ensure that domain name registration and associated contact information are not inadvertently lost. Many registries have certain elements of uniqueness that would either require capable backup operators to develop those capabilities to support these unique practices or situations or to suspend those unique practices for a period of time.

4.5 The backup provider will use commercially reasonable efforts to ensure that critical functions of the registry are maintained to the extent possible, based on priority of the critical function and time frame for implementation. Backup providers should conduct a test of contingency plans on a periodic basis.

5. Internal Communications Plan

5.1 Following contact with the gTLD registry or sponsor, or independent confirmation of the initiating event in the situation where the gTLD registry or sponsor cannot be contacted, and depending on the type and severity of the event, ICANN may initiate its crisis response team.

ICANN's crisis response team shall consist of ICANN's:

a. VP of Corporate Affairs
b. Media adviser
c. General Counsel staff
d. SVP, Services
e. Registry staff
f. Registrar staff
g. Chief Security Officer
h. Chief Technical Officer
i. Compliance Program Director
j. If applicable, IDN Program Director
k. Other staff, as necessary

Each of these roles shall be clearly defined and preferably each role should have a designated back-up person. ICANN shall test its crisis management process on a regular basis, but in no event less than once per annum. ICANN staff is scheduled to test the process in January 2008.

5.2 The team shall inform the CEO, COO and Board of the event, the type of failure and course of action.

5.3 The VP of Corporate Affairs is ICANN's designated public spokesperson in the event ICANN's crisis team is assembled. ICANN will inform the Internet community based on the specifics of the event, the need to know and what is disclosed should be limited based on the perceived impact on affected parties.

5.4 The gTLD registry (or the backup registry operations provider) shall inform registrars of the failure. If the registry is a sponsored TLD, the sponsor should inform the members of its sponsored community. If this is not possible, ICANN shall provide notice to the community and make best efforts to provide notice to registrars and registrants.

5.5 ICANN may consult with a predetermined list of experts with registry experience based on the type of event and determination of the event as a technical failure, business failure or other failure.

5.6 In a temporary failure, ICANN will communicate with the registry or sponsor and provide technical assistance where appropriate or requested by the registry or sponsor.

5.7 In a long-term failure, ICANN shall, in consultation with the registry if available, examine the cause of the failure and whether the failure occurred as a result of technical, business/financial or other reasons. Based on the severity of the event, ICANN's communications plan may be invoked to ensure that the community is informed.

6. Communication with registrars and registrants

6.1 Registrars should be advised to maintain a copy of names under management in the TLD (or TLDs if the operator maintains more than one) and ensure proper escrow of registrant data in accordance with ICANN's registrar data escrow specification.

6.2 If necessary, Registrars shall be advised by the gTLD Registry Operator to plan for the application of transactions to the TLD database upon restoration of services in a timely and predictable format in the event that notification of transaction success is delayed.

6.3 The gTLD registry (or the backup registry operations provider) shall inform registrars of the failure. If the registry is a sponsored TLD, the sponsor should inform the members of its sponsored community. If this is not possible, ICANN shall provide notice to the community and make best efforts to provide notice to registrars and registrants.

6.4 ICANN will confirm with registrars on notice to the community and registrants.

7. Decision on whether the registry or sponsor can continue operations

7.1 The decision on whether the registry or sponsor can continue operations is not an easy one to make, and must be made in consultation with the registry. The decision will be based on the terms of the gTLD registry agreement.

7.2 If the registry or sponsor can continue operations, the registry will inform ICANN of the timeline for return to normal operations and on the status of the TLD zone.

7.3 ICANN may offer to provide or locate technical assistance to the registry or sponsor, if appropriate.

7.4 ICANN and the registry or sponsor shall provide notice to the community of the timeline for return to normal operations.

7.5 In the situation where the registry or sponsor cannot continue operations, the registry or sponsor will invoke its contingency plan to activate a mirror site or backup registry operations provider to ensure continuity of service for the TLD. ICANN may also offer temporary resolution-only service for the TLD if asked by the registry or sponsor.

7.6 ICANN will inquire whether the registry or sponsor has identified a backup registry operations provider and whether the registry's failover plan has been invoked. ICANN will inform the ICANN Board and advisory groups, as appropriate.

7.7 If the registry or sponsor has identified a backup registry operations provider, the registry or sponsor will follow its own registry failover plan to ensure continuity of service for the TLD.

7.8 Before a backup registry operations provider is engaged by the registry or sponsor, the backup registry operations provider must meet ICANN requirements for operating a TLD. ICANN shall obtain assurances of continuity from the backup registry operations provider.

7.9 If the registry or sponsor has not designated a backup registry operations provider, in an emergency, ICANN may provide temporary resolution-only services until the TLD can be transitioned to a successor.

8. Voluntary Transition Process

A voluntary transition of a TLD is necessary when an initiating event occurs that renders a registry or sponsor unable to execute one or more critical registry functions and therefore unable to continue operation of the TLD. The registry or sponsor and ICANN shall cooperate with ICANN in efforts to promote and facilitate the Security and Stability of the Internet and the DNS and to accomplish the terms of the registry agreement. A voluntary transition will occur under the cooperative terms of transition in the registry agreement.

8.1 ICANN and the registry or sponsor will consult on voluntary transition of the TLD. 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.

8.2 The registry or sponsor may locate a buyer for the TLD delegation within the transition timeframe for the remainder of the registry's contract. The buyer must meet ICANN criteria to operate the TLD. Such criteria will be specified in advance.

8.3 If the buyer meets the specified criteria, ICANN will confirm the buyer as the successor. Transition will be complete following notification to the community and registrar testing.

8.4 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.

8.5 For sTLDs, ICANN will seek input from the sponsored community on a successor. Applicants must meet certain successor criteria.

8.6 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.

8.7 Elements of the RFP may consist of the following, but could include additional items:

a. Application instructions
b. Application transmittal form
c. Proposal form
d. Financial Disclosure
e. Statement of Requested Confidential Treatment of Materials Submitted
f. Criteria to be used by ICANN to evaluate the proposals
g. Base Registry Agreement
h. If applicable, an application fee (with possible refund)
i. Description of what is being transferred

8.8 ICANN shall post on its website the names of the applicants who submitted a response to the RFP and post certain non-proprietary/non-confidential portions of the response on its website so as to provide the public with a reasonable period of time for which to comment.

8.9 ICANN shall conduct an evaluation of the applications and publish a staff recommendation and report. The evaluation and selection will be based on published criteria.

8.10 The staff recommendation and report will be provided to the ICANN Board for consideration and selection of the successor registry or sponsor.

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

8.12 In the event that ICANN does not receive sufficient proposals to operate the TLD, ICANN will publish a notice period to registrants and the community with a timeline on the impending closure of the TLD.

8.13 ICANN will follow IANA's procedures for removing a TLD from the root zone.

9. Non-voluntary Transition Process

9.1 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. 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.

9.2 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.

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

9.4 The non-voluntary transition process will be managed by the Office of General Counsel.

10. Closure of the registry

10.1 In the event that the RFP fails to identify a successor registry operator or sponsor, ICANN will provide notice to the community and to registrants in the TLD(s).

10.2 If possible, the registry, sponsor or backup registry operations provider will maintain operations for a designated period of time (30 to 90 days or more) in order to ensure that registrants have sufficient time to locate alternatives to the TLD.

10.3 After the designated period of time and notices to the community, the registry, sponsor or backup provider may terminate nameservers for the TLD.

10.4 Following determination of the Board, termination of the TLD and notices to the community, ICANN will follow IANA procedures for removing a TLD from the root zone.

11. Testing of Failover Plan

11.1 ICANN shall test the registry failover plan and crisis communications plan at least once a year.

11.2 Testing should be done in consultation with the Registry Constituency, and other members of the technical community. Testing may include registrars and third party data escrow providers. A joint panel of gTLD and ccTLD registry representatives may also provide assistance to ICANN in testing the registry failover plan.

11.3 Registry operators should conduct business continuity and disaster recovery testing at least once a year.

11.4 Registry operators should submit an Annual Certification document that states they have a business continuity and disaster recovery plan and it has been tested.

12. Failover Plan Review

12.1 ICANN shall periodically review the failover plan and make modifications as necessary to stay current with registry practices.

12.2 In the event of registry failure, ICANN will conduct a review of ICANN's handling of the event and document the lessons learned. ICANN will consult with SSAC, external experts and constituency advisory groups for their input on ICANN's handling of the event.