ICANN gTLD Registry Failover Plan
15 July 2008

i. Background

The overall goals of ICANN's gTLD Registry Failover Plan are 1) the protection of registrants and 2) to ensure confidence in the DNS.[1]

The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized non-profit public benefit organization that administers certain features of the Internet's unique identifiers. As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes. A general description of ICANN is available at http://icann.org/tr/english.html.

Section 1.10.1 of the 2007-2008 ICANN Operating Plan stated 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 Fiscal Year 2009 ICANN Operating Plan (approved by the ICANN Board on 26 June 2008 during the ICANN Meeting in Paris), states that a key deliverable during FY09 is to "implement [the gTLD] registry failover plan including live testing with a registry or registries."

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.

Completion of the gTLD Registry Failover Plan achieves a key project in ICANN's Operational Plan. The development of the plan has been guided by the following ICANN Core Values:

1. Preserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet.

8. Making decisions by applying documented policies neutrally and objectively, with integrity and fairness.

9. Acting with a speed that is responsive to the needs of the Internet while, as part of the decision-making process, obtaining informed input from those entities most affected.

The gTLD Registry Failover Plan is being developed in advance of the implementation of the new gTLD process and as part of other Protections for Registrants contingency efforts, including the registrar failover plan and Registrar Data Escrow program.

[1] Confidence in the DNS refers to the degree of certainty that a user has in the ability to maintain a chosen domain name and for registries to maintain resolution services.

ii. History

ICANN published an initial draft for community input and comment from 20 October to 19 November 2007. A revised draft plan was published on 27 November 2007 incorporating feedback received during the comment period and the ICANN meeting in Los Angeles.

ICANN conducted its first gTLD Registry Failure Table Top Exercise on 24-25 January 2008.[2] The purposes of the exercise were to:

- validate and improve the draft gTLD Registry Failover Plan
- train staff for crisis response in the event of failure situations
- assess maturity of ICANN's decision making progress through simulated scenarios, and
- assess the requirements for completion of the gTLD Registry Failover Project

The gTLD Registry Failure Table Top Exercise confirmed the need for ICANN to improve internal information sharing and information flow among departments and executive management, as well as improve the external information sharing with registries, registrars and other stakeholders.

Following the exercise, ICANN revised the draft plan on 5 February 2008. The revised draft plan was circulated to the gTLD Registry Constituency and SSAC for review during the ICANN meeting in Delhi, India in February 2008.

On 7 April 2008, ICANN staff conducted an informal session with gTLD registries and a registry escrow provider in Crystal City, Virginia, to work through issues related to registry data escrow and options for data transition in the event of registry failure. As a result of that meeting, an updated draft was circulated on 24 April 2008. Following the North American Regional Registry-Registrar Gathering in New Orleans, Louisiana 30 April-1 May 2008, and continued improvement of the draft plan, ICANN staff prepared an updated draft on 16 May 2008. Further inputs were received in May and June 2008. ICANN staff completed consultations on the plan during the ICANN meeting in Paris, resulting in this version of the gTLD Registry Failover Plan.

iii. Registry Involvement

While outside the scope of this document, gTLD registries as a best practice should have a contingency plan in order to prepare for the possibility of registry failure and to address certain types of business, operational, and technical issues.

The goal of such plans is to maintain the critical functions of a registry for a period of time to the extent possible. These plans should also include mechanisms to provide recovery of contractually required 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. The plans should also address an alternative outcome in which the registry operator, absent the designation of a replacement, provides a notice period to registrars and registrants that the registry is closing.

[2] The exercise was conducted based on standard tabletop exercise protocol detailed in the National Institute of Standards and Technology (NIST) *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* (September 2006, see http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf).

iv. Definitions

The following definitions are used to describe the gTLD Registry Failover Plan.
Situation - An occurrence with the potential to produce an undesired consequence. In isolation, a situation is not significant enough to trigger an event. A Situation may cause or threaten to cause temporary or long-term failure of one or more of the critical functions of a (gTLD) registry.

Event – A Situation with a gTLD registry that requires a manager, a coordinated, inter-departmental response and coordinated outside communications, including communications to the ICANN Board. Events may be temporary or long-term.

Temporary Event – An Event where there is reasonable certainty of resolution of the Situation 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. An Event involving the resolution of names and maintenance of nameservers should be measured differently than an Event involving Publication of Registration Data.

Long-term Event – An Event 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 Event, depending on the type of critical function involved.

Crisis – A suddenly occurring or unstoppable developing Event with public impact involving a critical function of a gTLD registry.

Critical functions – those functions that are critical to the operation of a gTLD registry.

1. Maintenance of nameservers and DNS for domains
2. Shared Registration System
3. Data Security and Data Escrow
4. Accessibility of Registration Data
5. IDN Tables (if IDNs are offered by the registry)
6. DNSSEC Keys (if DNSSEC is offered by the registry)[3]

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 public access to registration data is down for a certain period of time.

Business Continuity – An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies, recovery plans, and continuity of services.[4]

[3] The gTLD Registry Failure Report from 1 June 2007 identified seven critical functions of a registry, although there may be others. See http://www.icann.org/registries/reports/registry-failover-01jun07.htm. From this list, and in consultation with registries, staff has produced a list of critical functions.
[4] Definition of Business Continuity from the National Fire Protection Association (NFPA) 1600 Standard on Disaster/Emergency Management and Business Continuity Programs (2007 Ed., http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf).

0. Overview

The gTLD Registry Failover Plan is intended to be a comprehensive guide covering a number of areas in which ICANN may act based on a specific situation involving a registry while not in conflict with individual registry agreements.

The plan is intended to define the roles of registries and ICANN in the event of registry failure. This assumption must be proven through a series of exercises with registries, registrars and others.

1. Information Sharing

1.1 ICANN recognizes that gTLD registries play an important role in upholding the operational security, stability, reliability and global interoperability of the Internet. As memorialized in their respective contracts, all gTLD registries agree to cooperate with ICANN as necessary to accomplish the terms of their registry agreements. This may include the sharing of data and information, as agreed by ICANN and the registries. It is essential that conditions for effective information sharing exist between gTLD registries and ICANN.

1.2 Information sharing can occur for routine Situations as well as Events affecting gTLD registries. The more information available to ICANN about Situations and Events affecting gTLD registries and DNS, the better able it will be to understand risks and, if necessary, provide assistance to ensure continuity of essential services. Information that should be shared includes information about threats, vulnerabilities, incidents, protection and mitigation measures, and best practices. Information sharing can be viewed as a means by which to better manage risk and, in turn, help deter, prevent, mitigate, and respond to Events.[5]

1.3 It is recognized that information sharing needs to take place in an environment of trust and confidentiality. Existing formats and mechanisms should be used for information exchange. as far as possible.

1.4 In order to facilitate effective communication during situation activities, ICANN will maintain a private directory of designated gTLD registry contacts. The list of registry contact types include:

- Designated Point of Contact
- Technical Point of Contact
- Legal Point of Contact

1.5 The accuracy of the directory information shall be reviewed quarterly by the ICANN gTLD registry team, with notices sent to the designated prime contacts at each gTLD registry. Each gTLD registry shall respond within 15 calendar days to the notice, affirming the accuracy of the provided information or providing updated information in its stead. In a similar fashion the ICANN gTLD registry team shall provide its most up-to-date contact information to the gTLD registry contacts on a quarterly basis, with changes highlighted.

1.6 In order to facilitate effective examination of Events (see “Event Management” below), ICANN may consult with technical experts as situations require. These experts or organizations will have experience in the operations of registry technology, especially the identified Critical

[5] Section adapted from Section 6.3 of the Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection, November 2004 (see http://www.publicsafety.gc.ca/prg/em/nciap/NSCIP_e.pdf).

Functions. ICANN will ensure that it has a non-disclosure agreement and, if required, a consulting services agreement with any experts consulted. This will enable ICANN to act quickly and leverage the technical expertise of the broader community as needs dictate. Because of competition concerns, experts consulted will not be an active competitor of a registry experiencing an Event.

1.7 In order to facilitate effective information flow, ICANN will establish a variety of mechanisms for communication among its own staff, the various communities, and its technical experts. These mechanisms will vary based on the scope and detail of the communications required and should range from the low-tech (e.g. teleconferencing numbers and a "phone tree" distributed in advance) to the high-tech (e.g. shared electronic Internet whiteboard).

1.8 ICANN must ensure that public statements are not material to a registry operator's business without consultation with the registry itself.

2. Situation Handling and Event Management

2.1 ICANN has developed the following high-level approach to situation handling:

- ICANN learns of or may receive information (via 24/7 hotline, email, or other means) of a Situation, from designated or other contacts at a gTLD registry, sponsor, registrar, or other member of the community. ICANN's gTLD registry team will most likely receive this information.

- The Situation shall be given a unique identifier, noted and logged by ICANN staff, and staff shall record
    - The timeline of the situation (time occurred, time identified, events, etc)
    - The Critical Function(s) involved,
    - The identity of the party providing the notification,
    - As much detail regarding the nature and impact of the situation as is available (and practically possible to collect).

- ICANN staff will study the information provided, and assess whether the information involves a critical registry function or specifically threatens to cause temporary or long-term failure of one or more of the critical functions of a gTLD registry. If possible, ICANN staff will respond to the party who notified ICANN, and promptly contact the registry via the registry's designated contacts (if the registry did not already notify ICANN staff).

2.2 ICANN staff will make a preliminary determination of the severity and consequences of the situation, document them, and communicate the results internally to the relevant staff. ICANN will follow Event Management procedures to ensure the appropriate level of response. An evaluation mechanism will be developed in consultation with gTLD registries to ensure open, fair and transparent treatment.

2.3 ICANN staff will conduct a preliminary examination based on facts known. 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.

2.4 ICANN staff will examine available options before taking next steps. If a Situation requires a manager, a coordinated, inter-departmental response and coordinated outside communications,

the Situation will be considered an Event and ICANN staff will coordinate with the affected gTLD registry to reach a resolution.

3. Crisis Response

3.1 Following contact with the gTLD registry or sponsor, or independent confirmation of the Event if 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. The decision to initiate the crisis team will be made by joint decision of Services and Legal staff. The crisis team will be initiated in events where there is public impact and the need for coordinated internal and external communications.

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

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

Each of these roles should have a designated back-up person. ICANN shall test its crisis management process on a regular basis, at least once per year. ICANN conducted its first test exercise of the process in January 2008.

3.3 The team shall inform the CEO, COO and Board of the Event, the type of Event and course of action, once sufficient details of the Event are known.

3.4 The VP of Corporate Affairs is ICANN's designated public spokesperson if ICANN's crisis team is assembled. ICANN shall make best efforts to coordinate with the affected registry media staff prior to making public statements. ICANN will inform the Internet community based on confirmed facts of the Event and references to Registry communications will be provided if available. Where the public is potentially impacted by an Event, a public awareness program may be implemented.

3.5 ICANN's Corporate Affairs team shall maintain an emergency public information capability that includes the following:

a. A central contact facility for the media
b. Systems for gathering, monitoring and disseminating emergency information
c. Pre-scripted information bulletins
d. A method to coordinate and clear information for release
e. The capability of communicating with stakeholders

3.6 Using previously established registrar communication channels, the gTLD registry (or the backup registry operations provider) shall inform registrars of the Event in line with the negotiated agreements. If the registry is a sponsored TLD, the sponsor should inform the members of its sponsored community (or delegate this responsibility to its registry provided. If

this is not possible, ICANN shall provide notice to the Internet community and make best efforts to provide notice to registrars and registrants.

3.7 ICANN will communicate with the registry or sponsor and provide technical assistance where appropriate or requested by the registry or sponsor.

3.8 In a long-term Event, ICANN shall, in consultation with the registry (if available), examine the cause of the failure and whether the Event occurred as a result of technical, business/financial or other reasons.

4. Communications

4.1 If a Situation or Event becomes known to ICANN, ICANN will attempt to communicate with the designated gTLD registry contact. This contact should be someone with a direct line of communication to someone authorized to act on behalf of the registry.

4.2 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 Event
2. The cause of the 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 the registry's critical functions

4.3 ICANN's determination on whether a registry can continue its critical functions operations will be made in consultation with the registry. As part of this determination, ICANN may consult with its panel of experts on registry functions (see above).

There may be circumstances when a registry can provide limited services (e.g. DNS, but not registration or change services) for a temporary period without the need to transition operations to a qualified backup provider.

4.4 If available, the designated gTLD registry or sponsor confirms contact and provides information on the suspected Event as temporary or long-term, or informs ICANN that no such Event has occurred or has been resolved.

4.5 If an 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. ICANN will attempt to reach all available contacts at the registry or sponsor before contacting an available backup registry operations provider or seeking alternative confirmation of the Event and contacting 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

4.6 If the registry's failover plan activates a backup registry operations provider, the registry must make contact with ICANN and confirm the level of service to be provided by the backup provider to registrars and registrants (full service or resolution-only service). ICANN may request a temporary agreement with the backup operations provider. It is the responsibility of the registry operator and its 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.

4.7 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. ICANN recommends that registry operators and their backup providers should conduct a test of contingency plans on a periodic basis.

4.8 Registrars are obligated by ICANN 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.

4.9 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.

4.10 The gTLD registry (or the backup registry operations provider) shall inform registrars of the failure. If the registry is a sponsored TLD, the sponsor (or its designee) 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.

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

5. Business Continuity

5.1 The gTLD Registry Failover Plan presumes that gTLD registries have their own continuity plans, and that ICANN has a duty to ensure the operational security, stability and reliability of the Internet's unique identifiers. Continuity of registry operations is a key element of the gTLD Registry Failover Plan.

5.2 If gTLD registry continuity plans identify a backup operations provider, the registries should inform ICANN under cover of full confidentiality unless otherwise agreed to by both parties.

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

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

5.5 The registry or sponsor shall provide notice to the community of the timeline for return to normal operations.

5.6 In the situation where the registry or sponsor cannot continue operations, the registry or sponsor will invoke its contingency plan or backup registry operations provider to ensure continuity of service for the TLD.

5.7 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.

5.8 If the registry's business continuity plan involves a backup registry provider, 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. ICANN will consult with existing gTLD registries on these requirements to address this topic.

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

5.10 If not already specified in registry agreements, ICANN recommends that registry operators conduct business continuity and disaster recovery testing at least once a year.

5.11 ICANN recommends that registry operators provide information to ICANN that the registry has a business continuity and disaster recovery plan and the plan has been tested.

6. Data Security and Data Escrow

6.1 ICANN requires gTLD registries under contract with ICANN to escrow registry data. The expectation of data escrow is to help restore or continue operation of a registry. Data escrow may be used to help ensure continuity of service in the event of a technical failure of a registry. More information than escrowed data may be needed to reconstitute service if a failure occurs. This information should be identified and specific plans should be developed and tested.

6.2 On 9 November 2007, ICANN announced the implementation of the Registrar Data Escrow Program (see http://www.icann.org/announcements/announcement-2-09nov07.htm).

6.3 In the event of a transition or termination, 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. ICANN's access to escrowed registry data is limited to the terms of relevant agreements.

6.4 ICANN staff is monitoring the results of the Registrar Data Escrow program for lessons that can be applied to a potential revised specification for registry data escrow. A revised registry data escrow specification will be developed for the base contract for the new gTLD process.

7. Transition of a TLD

7.1 A transition of a TLD is necessary when an event occurs that renders a registry or sponsor unable to execute critical registry functions and therefore unable, in the long term, to continue operation of the TLD. The registry or sponsor and ICANN shall cooperate in efforts to protect registrants, 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.

7.2 ICANN and the registry or sponsor will consult on transition of the TLD. If the registry or sponsor has made a decision to 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, with notice to the community.

7.3 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, as part of the new gTLD process.

7.4 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.

7.5 In situations where a buyer does not come forward, ICANN will publish a call for expressions of interest and seek input from the community. For sponsored or community-based gTLDs, ICANN may prepare a Request for Proposals (RFP) for a successor registry operator or sponsor and seek direct input from the sponsored community.

7.6 From those that respond to the expression of interest, ICANN will review the responses for technical capacity.

7.7 ICANN will make an effort to post the call for expressions of interest or RFP for at least 21 days, unless there is an urgent need for a shorter period of time.

7.8 ICANN shall post on its website the names of the applicants who submitted a response to the call for expressions of interest or 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.

7.9 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.

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

7.11 If there are multiple qualified applicants, an auction process might be a possibility for determining a successor.

7.12 If no qualified applicants are available for the TLD, ICANN can revise the expression of interest document, and republish it (causing the process to repeat), or will provide notice to the community, with a timeline on the impending closure of the TLD.

7.13 Once a successor has been designated, ICANN will coordinate with the registry or backend provider to ensure smooth transition of the TLD(s) to the successor registry.

7.14 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 termination process specified in the gTLD registry agreement. If the decision is made to proceed with the termination process, ICANN will invoke the 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.

7.15 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. The termination process will be managed by the Office of General Counsel.

8. Registry Closure

8.1 In the event that a call for expressions of interest, RFP or auction process fails to identify a successor registry operator or sponsor, ICANN will provide notice to the community and to registrants in the TLD(s).

8.2 If possible, the registry 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.

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

8.4 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.

9. Testing of the Failover Plan

9.1 ICANN shall test or exercise the registry failover plan and crisis communications plan at least once a year. This should be an all-inclusive test of the failover plan with multiple table top exercises or simulations.

9.2 Testing or exercises should be conducted in consultation with the Registry Constituency, and other members of the technical community. Such testing or exercises 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.

10. Plan Review

10.1 ICANN shall periodically review the failover plan and make modifications as necessary to stay current with registry practices. There should be a review of the plan following each exercise.

10.2 In the event of registry failure, ICANN will conduct a review of ICANN's actions and document the lessons learned. ICANN will consult with SSAC, external experts and constituency advisory groups for their input on ICANN's actions in response to the situation.