The Internet Corporation for Assigned Names and Numbers

ICANN

2009 Joint ICANN-gTLD Registry Continuity Exercise

AFTER ACTION REPORT
30 April 2009

Held 28 January 2009

Table of Contents

Executive Summary

The Internet Corporation for Assigned Names and Numbers (ICANN) conducted a joint ICANN-gTLD Registry Continuity Exercise (Dot INFERNO II) with Afilias, NeuStar, Public Interest Registry and VeriSign on 28 January 2009. The exercise was designed to examine and test the *gTLD Registry Continuity Plan*[1].

A core planning team comprised of ICANN staff and gTLD registry representatives developed a scenario to be followed during the exercise. The scenario focused on ICANN/gTLD registry roles, responsibilities and obligations to assure continuity of service; gTLD registry responsiveness; and ICANN/gTLD registry actions, coordination and communication to address a gTLD registry failure.

The exercise produced a number of observations and recommendations for short and longer-term action. Sixty-five participants in the exercise included staff from ICANN and the four participating gTLD registries. The exercise was conducted in a largely virtual environment through use of Adobe Connect and a phone bridge to link the four main locations of participating organizations on the East Coast and West Coast of the United States.

Selected Observations

The exercise identified many issues that will be addressed and incorporated into the implementation procedures for the *gTLD Registry Continuity Plan*. ICANN is in the process of developing an Action Strategy following the exercise. This will need to be accomplished collaboratively by ICANN with its gTLD registry partners and other members of the Internet community.

Continuity-related requirements have already been incorporated as an integral element in the evaluation of new gTLD applications and part of the Base Agreement for new gTLDs that may be introduced in the future.

Selected Recommendations

- ICANN and the gTLD registries should further explore and delineate roles and responsibilities.

---

[1] The current version of the gTLD Registry Continuity Plan is located at
http://www.icann.org/en/registries/continuity/gtld-registry-continuity-plan-25apr09-en.pdf.

- ICANN, in collaboration with gTLD registries and other stakeholders should develop criteria and a process for data collection, verification, monitoring of service levels to supplement Monthly Reports.

- ICANN needs to ensure it has a formal crisis response management function with clearly defined roles, responsibilities and effective decision-making processes.

- ICANN and the gTLD registries should develop procedures to assure resumption of a failed registry's services (or closure of the TLD if appropriate).

2009 Joint ICANN-gTLD Registry Continuity Exercise

1. Background

From 2006-2008, ICANN developed a *gTLD Registry Continuity Plan* (formerly the *gTLD Registry Failover Plan*) in collaboration with experienced gTLD and ccTLD registries, registrars, and members of the Internet community. The plan provides a comprehensive set of processes and procedures 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 plan describes potential ICANN actions in specific situations involving a registry and is intended to define the roles of registries and ICANN if such events occur. The plan also includes provisions for information sharing, situation handling and event management, crisis response, communications, business continuity, data escrow and data security, and gTLD data transition and registry closure.

In January 2008, ICANN conducted a gTLD Registry Failover Exercise[2] — internally known as *Dot INFERNO* — to validate the draft plan and to test internal communications and processes centered on registry failure. Lessons learned were used to make improvements to the *gTLD Registry Continuity Plan* between April and July 2008. Improvements included changes in definitions for the designation of situations or events, communications process and detail on the process for forming a crisis response team.

Dot INFERNO II took the next important step of bringing together gTLD registries with ICANN staff and others to assess and test the updated plan and explore other related issues to further improve continuity planning and execution.

---

[2] After Action Report on January 2008 table-top exercise, see
http://www.icann.org/registries/failover/icann-aar-06apr08.pdf.

gTLD Registry Continuity Plan Timeline
2008 - 2009

Draft gTLD Registry Failover Plan

2007

JAN   APR   JUN   SEP   NOV   **2008**   JAN   MAR   APR   **2009**

ICANN Meeting Paris

ICANN Meeting Cairo

ICANN Meeting Mexico City

Internal ICANN gTLD Registry Failover Exercise

After Action Report

Plan renamed to gTLD Continuity Plan

Joint ICANN/Registry gTLD Continuity Exercise

After Action Report
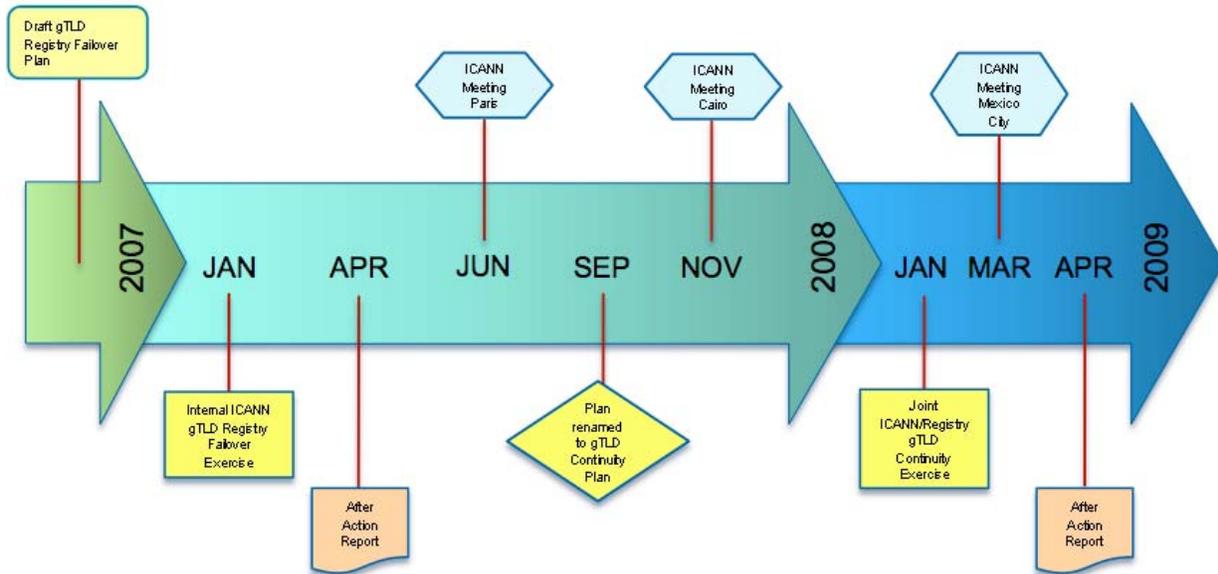
gTLD Registry Continuity Timeline
2009 – Jan 2010

ICANN Mexico City

ICANN Meeting Sydney

ICANN Meeting Seoul

JAN   MAR   APR   MAY   JUN   AUG   OCT   NOV   **2009**   JAN   **2010**

Joint ICANN/Registry gTLD Continuity Exercise

After Action Report

ICANN gTLD Registry Continuity Procedures

gTLD Registry Escrow Test Planning

• ccNSO Update
• Escrow Test Planning

Escrow Testing

Escrow Test Report
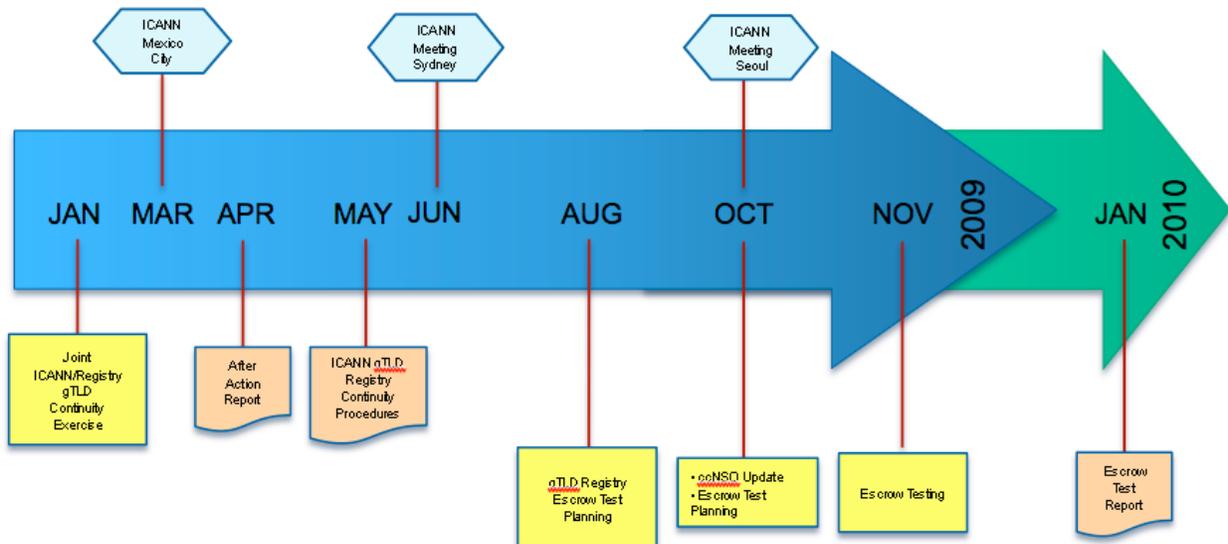
2. Overview

2.1. Purpose, Goal, and Objectives

The overall goal of the exercise was to further validate, test, and improve mutual processes and procedures associated with implementation of the *gTLD Registry Continuity Plan* and other measures to assure registry continuity and resiliency.

The Exercise Planning Team developed the following objectives:

1. Validate, test, and enhance the ICANN *gTLD Registry Continuity Plan.*

2. Enable participating registries to test and improve their contingency plans and procedures.

3. Explore and investigate how ICANN and registries coordinate activities and work together to handle crisis response and recovery.

4. Identify operational impacts and consequences of specific registry disruption and failure scenarios, including infrastructure interdependencies/cascading impacts, policy, legal, liability, security, and political issues that could complicate crisis response and/or impede recovery.

5. Identify potential economic and business impacts under certain situations.

6. Explore roles and responsibilities of ICANN, registries, sponsors, and other key organizations that would be involved in registry crisis response and recovery, including timelines.

7. Illuminate how decisions will be made, communicated, and implemented in the event of specific disruption/failure situations.

8. Identify readiness gaps and prevention/mitigation options that could harden against operational disruptions, assist crisis response, as well as accelerate recovery of a failing registry or facilitate expeditious reconstruction if necessary.

9. Examine how public information will be effectively coordinated and communicated in a timely manner.

2.2. Exercise Development

2.2.1. Focus and Scope

Dot INFERNO II was designed to build on the results of the January 2008 exercise and produce lessons learned that could be incorporated into an After Action Report (AAR) that in turn could lead to the development of a prioritized Action Strategy to address identified continuity gaps with solutions. The exercise was developed using a customized version of the National Institute of Technology Standards (NIST) Exercise Guidelines[3].

A small core planning team consisting of representatives from ICANN, Afilias, NeuStar, and VeriSign developed the exercise scenario and process. The core planning team provided perspectives to assist in developing the concept and objectives for the exercise by a broader group of Internet community organizations and senior ICANN management.

The core planning team held two face-to-face meetings (in Washington DC in September 2008 and in Cairo, Egypt in November 2008) and several conference calls over a four-month period to prepare for the exercise. *(See Appendix A for core planning team and Exercise Participants.)*

2.2.2. Scenario Overview

The scenario in *Dot INFERNO II* was based on a hypothetical series of events developed for the purpose of examining ICANN and registry continuity planning and procedures. Actions described in the exercise were selected to be illustrative of potential challenge areas and provided to facilitate maximum utility of the exercise. The scenario was focused on a fictitious registry (.DOG) that ultimately fails, with various repercussions that touch upon a range of continuity challenges, including information sharing, coordination, and legal, security, and public information issues.

The scenario was comprised of a series of 11 events, or "injects" divided into three parts:

- Part 1 focused on ICANN and registry roles, responsibilities, and obligations to assure service.

- Part 2 focused on registry reporting responsibilities and responsiveness, and ICANN options for action.

---

[3] NIST Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, Special Publication 800-84, Sept. 2006, http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf.

- Part 3 centered on ICANN and registry actions, coordination, and communication to address a registry failure.

For each inject, there was a series of questions designed to encourage discussion among participants on issues raised during the exercise.

The scenario begins with minor Service Level Agreement lapses by the registry at the end of an ICANN meeting.

During the scenario, .DOG Registry is purchased by Dogs International LLC. Registry performance begins to erode, and DNS outages occur on a more frequent basis.

The new operator goes into bankruptcy. After a period of time, the registry can no longer cover the costs for its data centers and power providers. The bankruptcy representative informs ICANN that services will be discontinued by a certain date. Before that date occurs, the registry experiences a significant DNS outage stretching beyond 11 hours.

Time passes and the registry no longer has employees actively monitoring. Registrars begin to complain about access to the registry.

International news media pick up on the events involving .DOG, and broadcast a story titled "A DOG in hot water".

2.2.3. Exercise Process

Exercise participants represented key functions and operations with roles and responsibilities in continuity planning and execution in ICANN and the participating registries. Participants were situated in their respective organizations for exercise play, either collectively or individually, and followed the exercise through remote participation via Adobe Connect.

Participants were provided an Exercise Guide that included instructions on accessing the exercise site. Each organization was asked to select one or more moderators to convey comments of their participating staff. Individual participants were also encouraged to express their views and ideas.

As the exercise play progressed, each inject was presented and participating organizations requested to take a specified amount of time to discuss selected issues questions or other issues of interest, and then respond in general discussion via the phone bridge. Participants were also asked to refer to their organization's plans and procedures by observing how well they provide necessary guidance in dealing with the events in the scenario.
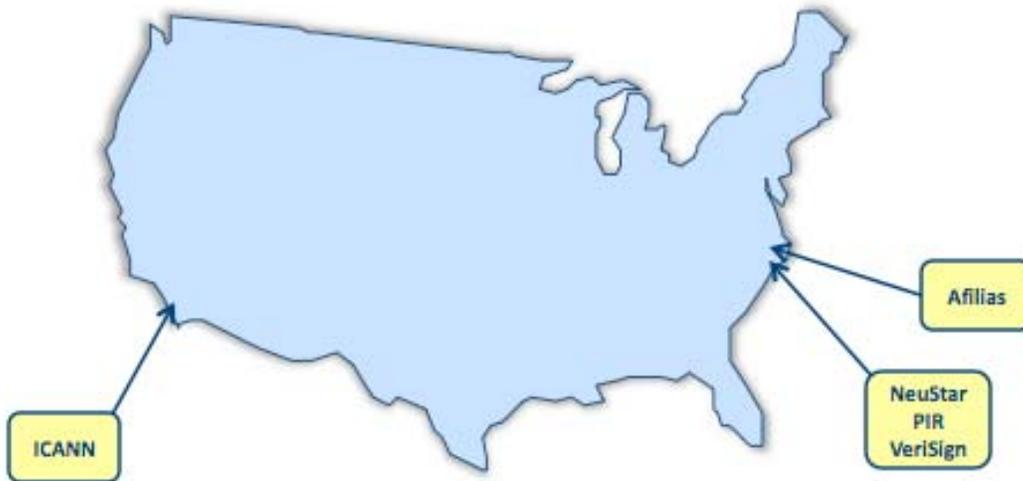
Data Collection Process, Hot Wash, and Next Steps

Participants were provided feedback forms to record their views, as well as note cards to provide comments and recommendations. Data collectors, assigned and sitting with the respective participating organizations, recorded observations using a provided template. At the end of the exercise play, the data collectors convened on the phone bridge and within their respective organizations and developed a PowerPoint presentation of their observations that was shared with the exercise participants for further discussion.

The exercise adjourned after a concluding session. Participants were told that an exercise After Action Report would be produced followed by an Action Strategy to address identified areas of enhancement in ongoing continuity planning and areas for further examination and testing by targeted exercises.

3. Observations and Recommendations

The following observations and recommendations are based on information and feedback collected during the exercise proceedings by Data Collectors and by participants.

Evaluation Criteria

The results were grouped in eight categories to address the exercise objectives: General Observations; Roles and Responsibilities; Communications and

Information Sharing; Decision-Making; Effectiveness of Response; Legal, Regulatory, Liability, and Policy Issues; Public Information and Media; and other areas for Improvement in Continuity Plans.

3.1. General Observations

3.1.1. Observations

The exercise identified many issues — technical, functional, legal — in the above criteria that need to be addressed and perhaps incorporated into the implementation procedures for the *gTLD Registry Continuity Plan* (formerly *gTLD Registry Failover Plan*).

The influx of new registries, many with potentially limited experience in continuity planning and execution, poses a major challenge.

Consequently, continuity-related requirements have been incorporated in the draft Base Agreement for new gTLDs and will be an integral element in the evaluation of new gTLD applications.

3.1.2 Recommendations

- ICANN, registries, and other organizations should collectively work to develop and implement a Registry Continuity Improvement Action Strategy of prioritized short-term and longer-term activities.

- Workshops and exercises, both targeted on specific continuity issues, and tabletops and functional exercises with a wider and more diverse number of organizations to identify areas of needed attention or further exploration.

3.2. Roles and Responsibilities

3.2.1. Observations

ICANN sees its responsibility to ensure registries meet their obligations and to ask questions on issues and what remedies will be undertaken.

ICANN and the gTLD registries see the need to ensure that end-users are protected and minimally impacted by potential issues. The registries also view protection of proprietary and sensitive information as a priority.

Monthly Registry Operator Reports are the formal mechanism in which the registries report their performance to ICANN and through which ICANN monitors registry compliance. ICANN can make formal requests for clarification or informal discussions can be held at any time if ICANN has questions about the data in these reports. There may also be other monitoring per gTLD agreements.

The registries are unclear and have concerns on how ICANN uses the information in the Monthly Reports.

The registries have security and continuity requirements in their registry agreements; however, ICANN must assume that a registry has security and continuity plans and safeguards/best practices in place, and is meeting obligations in the current gTLD registry agreements.

3.2.2. Recommendations

- ICANN and the registries should create a small working group to further explore and clearly delineate roles and responsibilities, and incorporate additional language to this effect in the *gTLD Registry Continuity Plan*.

- ICANN and the registries should designate and provide contact information for backup personnel in the event that primary contacts are unavailable.

- Safeguards should be considered in future registry agreements that address registry continuity and ownership changes.

3.3. Communications and Information Sharing

3.3.1. Observations

ICANN and the registries rely on both formal and informal communications and information sharing — current monthly reporting is adequate for formal purposes, and ICANN can informally pursue clarification as needed.

- While both types of communication are useful, reliance on informal communications may raise problems if it bypasses key operational and technical staff who have a need-to-know.
- Informal communications also lack documentation.
- As the number of registries increases significantly, informal communications will not be effective.

A secure, limited access ticketing system to log communications would be useful to document and verify information provided between ICANN and registries.

ICANN lacks clearly identified backup personnel in case the primary ICANN Registry Liaison team members are not available.

There have been examples in the past in which ICANN has learned in the media or from a third party that a registry has ownership changes. This problem may

be alleviated if new registry contracts include a clause that requires registries to provide ICANN with ten days notice of a change in ownership.

Control or operational changes of a registry may pose increasing problems for secure, stable, and resilient service delivery as the number of registries increases.

Registries may have confidentiality requirements or other issues that preclude them immediately notifying ICANN of pending ownership changes.

The influx of new gTLD registries will change the dynamics of coordination and communication with ICANN.

3.3.2. Recommendations

- ICANN in collaboration with registries and other appropriate organizations should develop criteria, a formal process, and a mechanism for performance data collection and verification; this process could include visits by ICANN to the registry to gather additional information, a review of registrar complaints (if any), and review of media sources, and checks with other registries to determine if they have relevant information to provide.

- ICANN and the registries should examine what baseline set of data is critical to risk of failure or continuity of registry operations and examine how ICANN could acquire this data to monitor service levels, possibly in real-time, independent of the registries' reports.

- ICANN should work with registries to define actions and outcomes expected to occur during the period of notification before a change of control, operation, or ownership.

3.4. Decision-Making

3.4.1. Observations

A key topic of discussion was how ICANN could improve its ability to monitor registry service levels, potentially in real-time, to supplement Monthly Reports. A registry representative noted that this would be a new requirement to monitor the provisioning system, which could be a burden on some registries.

It was noted that some monitoring could be met without adding new requirements to registry agreements, such as monitoring successful escrow deposits, bulk WHOIS, DNS zone file publication, and DNS server performance. Another registry participant raised the question of the feasibility of real time monitoring of hundreds of new registries, observing that the issue is more about

compliance to operating standards and that ICANN could collect weekly reports.

It was noted that ICANN currently has a flexible internal standard[4] it employs for determining an event or when it moves to the crisis stage[5] (although this was recommended in the development of the gTLD Registry Continuity Plan in order to accommodate events on a case by case basis). Also, there are no criteria, other than the draft gTLD Registry Continuity Plan, to determine at what point ICANN should move to take over a registry or procedures for how this will occur. At the same time, as a registry representative noted, there are provisions in registry agreements that must be considered in regard to theses decisions.

ICANN should not rely on a single source for information to confirm a situation or event on a registry service issue but may have to go to an independent source or other registries if this did not violate privacy or confidentiality.

ICANN internal procedures for notifying Board members, key personnel, or making a public notification in case of an event are unclear; likewise it is unclear when ICANN could contact other registries.

3.4.2. Recommendations:

- Criteria need to be developed to determine at what point small anomalies may constitute an event or crisis.

- A time limit and way to monitor resolution of the problems needs to be developed to assure the service problems are addressed.

- ICANN needs to ensure it has a formal, well-understood crisis response management function with clearly delineated roles and responsibilities and effective internal decision-making process to deal with escalating events that may require ICANN to step in and take over a registry.

---

[4] Definitions from the gTLD Registry Continuity Plan include:
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.

[5] The Crisis Response Team is described in Section 3 of the gTLD Registry Continuity Plan.

3.5. Effectiveness of Response

3.5.1. Observations

ICANN must allow the gTLD registries time to resolve service problems, in accordance with terms of the registry agreement.

If a registry may not be able to continue operations, ICANN should contact the backend provider for information, although the backend provider may not necessarily have a legal obligation to be responsive.

There are a broad array of issues and challenges associated with taking over a failing registry:

— There is neither definition for what "continuing operations" means nor procedures for verifying a registry is failing

— If the registry files for bankruptcy, there are legal issues, including terms in registry agreements that must take precedence, which can delay the process of registry continuity for months.

— In some cases, it may be necessary to provide technical assistance or temporary takeover of a failed registry by another registry to get it "back on its feet"; in this instance, making this decision must be consistent with a registry operator requesting assistance, or the terms of the registry agreement must take precedence.

— ICANN would need to determine if the candidate registry is in a position to receive and manage the failing registry's domain names.

The registries likely would be reluctant to take over a failed registry that was facing financial difficulties or in bankruptcy, or which had a reputation as a "bad actor" for security or other reasons.

It is not clear how the crisis response decision-making process would work, who would have authority over the data, or how data recovery would be addressed.

The worst-case scenario would be that a registry "gets wiped out" and the data no longer exists.

There is no selection process for a new registry candidate to takeover a failed registry.

Specific response procedures and agreements are needed to deal with failing registries and to "keep the lights on".

3.5.2. Recommendations

- ICANN in collaboration with gTLD registries and other appropriate organizations should create a working group to explore the range of issues associated with response to an imminent registry failure and develop a set of formal mechanisms and procedures to assure resumption of the failed registry's services. This would include:

  — Addressing what "continuing operations" means and procedures for ascertaining registry failure including independent verification, e.g., how to deal with legal, operational, and other challenges of taking over a failed registry to include defining conditions that it would be appropriate for a registry to fail, or otherwise be removed from the root zone.

- Once registry failure contingency procedures are implemented, ICANN and registries should conduct a real-world test of the process of escrowing/recovering data from escrow, and investigate challenges to the rapid restoration of service.

- A pre-approved list of backup registries could be developed with incentives, compensation, and protection provided.

3. 6. Legal, Regulatory, Liability, Policy Issues

3.6.1. Observations

Backup registries may require certain arrangements and agreements before they take on the responsibilities of a failed registry.

The registries will not want to take on failing/bankrupt registries because of business liability — bankruptcy problems will make enforcing contract arrangements troublesome and drawn out.

3.6.2. Recommendations

- ICANN and the gTLD registries need to explore contractual language regarding potential bankruptcy of a registry, based on local bankruptcy laws and practices, and obligations of that registry and rights of ICANN to continue service.

- Contractual requirements for new TLDs should include specific provisions requiring use of best practices IT security and continuity plans.

- ICANN and the gTLD registries should explore what legal and liability issues and what precautions need to be taken and incentives provided to

registries to deal with these issues. Other industries could be examined for precedents, such as the airline and telecommunications industries.

3.7. Public Information and Media

3.7.1. Observations

ICANN and the gTLD registries need a coordinated public information and media response capability to preserve consumer confidence.

ICANN needs to enhance its internal public information/media interface capabilities to be prepared for responding to events that may occur.

> - This should include accurate and regularly updated information and proactive outreach with the media

There should be communication among the registries so there is a coherent message from a collective source with everyone on the same page.

If there is a backup provider, ICANN should work closely with the provider to ensure the public has the necessary information to understand the situation.

3.7.2. Recommendations

- ICANN should ensure that it has an effective, centralized internal public information management process.

- ICANN and the gTLD registries should create a public information coordination working group that meets/has conference calls on a regular basis to develop a joint information plan based on realistic scenarios with Q's and A's for the media.

- ICANN should develop a contact list of public information points of contact at all registries.

- ICANN should identify a spokesperson who has technical and public information experience to interface with the media (this may be ICANN's Media Adviser or it could be another spokesperson depending on the type of event).

3.8. Other Areas for Improvement in the gTLD Registry Continuity Plan

3.8.1. Observations

There are currently no cyber security standards for registries and limited means for registries to readily acquire information on security best practices.

— This security "low-bar" approach remains a major gap and vulnerability.

It is unclear what role, if any, ICANN should have in monitoring for sound security practices.

ICANN could potentially be a resource for registries interested in cyber security training and information on best practices.

3.8.2. Recommendations

- ICANN, registries, and other Internet members should develop basic standards for IT security and continuity plans that can be used by registries and other community organizations.

- ICANN should investigate ways to foster best security practices and help registries test and improve continuity planning through providing education, training, and opportunities for targeted exercises.

- Registries with technical competence in cyber security and continuity planning should investigate with ICANN how they could provide this expertise to registries needing this assistance.

4. Exercise Utility

The exercise received positive evaluation from participants. Participants overall rated the exercise in the good to excellent range, finding it a useful way to have good discussions on a wide range of complex issues and effectiveness of procedures.

Examples of comments on participant feedback forms included:

"The exercise was helpful to timeline a complex process and bring a real-life example to help understand and approach the issue." — Registry Product Development/Management

"Overall a good effort on a difficult subject." — ICANN Staff

"Appreciated the opportunity to voice our opinion in advance of a crisis situation." — Registry Representative

"I believe that this is a scenario that can occur and requires a sound process to ensure the end-users are minimally impacted." — ICANN Technical Operations Staff

"Running through scenarios saves a lot of time when something does happen—which is very valuable." — ICANN Corporate Affairs

"I believe the exercise was a good starting point but I also think more should be done." — Registry Contracts Management

"There are still areas of a fail-over process where the various parties are unclear as to who is responsible for what, and how to proceed while protecting everyone's interests. I think (hope) that all came away with some added insight as to the imperatives of the other parties." — ICANN Staff

Areas of particular interest that participants cited in their feedback forms included:

- The point at which ICANN might step in to address a registry performance issue;
- Aspects surrounding registry bankruptcy and how this would affect the Internet community;
- Technical aspects of issues raised in the scenario, particularly aspects of registry failure recovery; data "ticketing" system, need for centralized registry contact information.

Topics that participants believed needed further attention or examination included: communications issues, inclusion of additional Internet community organizations in future exercises, impacts of potential new registries, ideas for new gTLD contracts, and examination of what will occur if a registry is no longer in business and how this would affect the Internet community.

There were a number of comments on the virtual format of the exercise. While participants saw the utility for exercises in which there are many participants followed remotely, they found it limited interaction and dialogue. As one participant observed, it gave the perception of "them versus us".

The recommendation was that when possible, staff from various organizations should participate together (in the same location) in exercises to facilitate information sharing and build trust.

On the data collection process and exercise recap (hotwash), some participants felt that Data Collectors should record and classify their observations according to the evaluation criteria during each inject discussion period, enabling the Data Collection Team to systematically build the exercise outcomes briefing throughout the exercise rather than trying to create it in a short period of time at the end of exercise play.

Several participants had recommendations for future exercises, included focusing on specific technical issues and functional areas and using small groups to more deeply investigate key issues and processes. Some participants saw it useful to include more registries, registrars, and other Internet organizations.

5. Path Forward

Dot INFERNO II provided valuable insights into continuity issues and areas where further attention is needed. The exercise also produced ideas and recommendations for useful enhancements, including:

- Development with registries of a prioritized Registry Continuity Improvement Action Strategy from the *Dot INFERNO II* results;

- Incorporation of lessons learned from the exercise into implementation procedures for the *gTLD Registry Continuity Plan*;

- Collaboration by ICANN, the gTLD registries, and other organizations to implement the Registry Continuity Improvement Action Strategy, with focuses on priority issues;

- Development and conduct of additional continuity exercises, some targeted on specific topics, such as the data escrow process and recovery and other issues raised in the scenario, and additional exercises with a broader set of organizations in interactive environments to explore specific technical issues and to test, in both simulated and real-world conditions, continuity procedures and how quickly services can be brought back.

Per the above, the lessons learned from *Dot INFERNO II* in this After Action Report will be incorporated into a draft strategy of activities with an accelerated implementation timeline for consideration by the organizations participating in the exercise at an Action Strategy Workshop to be held at a future date in Fiscal Year 2009-2010. The Action Strategy will be utilized by ICANN, the gTLD registries, and other Internet community stakeholders to build upon and enhance the implementation of the gTLD Registry Continuity Plan and undertake additional collective and individual efforts to improve continuity and resilience.

6. Appendices

Appendix A. Exercise Planning Team and Exercise Participants

Afilias

Michael Young	*Exercise Planning Team*
Michael Szucs	Manager, Production Control
Terrence Graham	Senior Director, Development
Greg Aaron	Director, Key Accounts & Security
Heather Read	Senior Director of Communication
Debra Wong	Manager, Technical Support
David Knight	Director, Resolution Services
Scott Hemphill	VP, Legal Counsel

ICANN

Patrick Jones	*Exercise Planning Team* (Registry Liaison Manager)
Greg Rattray	*Exercise Planning Team* (Chief Internet Security Advisor)
Doug Brent	Chief Operating Officer
Kurt Pritz	Senior Vice President, Services
John Jeffrey	General Counsel
Theresa Swinehart	VP, Global & Strategic Partnerships
Dan Halloran	Deputy General Counsel
Geoff Bickers	Director of Security Operations
John Crain	Chief Technical Officer
David Conrad	VP of Technology & Infrastructure
Roman Pelikh	Director, Application & Services Development
Kim Davies	Manager, Root Zone Services
Craig Schwartz	Chief Registry Liaison
Barbara Roseman	General Operations Manager of IANA
Mandy Carver	Deputy General Manager, Global Partnerships
Anne-Rachel Inne	Manager, Regional Relations - Africa
Veni Markovski	Manager, Regional Relations
Shernon Osepa	Manager, Regional Relations - Caribbean
Baher Esmat	Manager, Regional Relations - Middle East
Pablo Hinojosa	Manager, Regional Relations – Latin America
Massimiliano Minisci	Manager, Regional Relations - Europe
Savenaca Vocea	Manager, Regional Relations – Australasia/Pacific Islands
Kieren McCarthy	General Manager for Public Participation
Mike Zupke	Registrar Liaison Manager

Joette Youkhanna   Project Coordinator

Data Collectors:
Kevin White   Loyola Law School
Marc Breverman   Loyola Law School

NeuStar

Eric Brown   *Exercise Planning Team*
Jeff Neuman   Policy/Legal
Ivor Sequeira   Registrar Relations
Fernando Espana   Registrar Relations
John Spengler   Product Mgmt
Les Chasen   Engineering/Ops
Keith Drazek   ICANN Relations
Nasiombe Mutonyi   Customer Support
Judy Song-Marshall   Note taker

PIR
Adam Palmer   Law & Policy Council
Michele Coon   Operations & Compliance Manager

VeriSign

Joe Waldron   *Exercise Planning Team*
Pat Kane   VP, Naming Services
Chuck Gomes   Policy
Jonathan Spencer   Legal
Will Shorter   Product Management
Barbara Steele   Compliance
Inez Toppin   Contract
Mike Kaczmarek   Technical Operations
David Ashley   Note taker

The Scalingi Group

Paula Scalingi   *Exercise Planning Team (support)*
Gerald Kiernan   *Exercise Planning Team (support)*

Appendix B. Exercise Agenda

EXERCISE AGENDA (times are PST)

8:00 – 8:10	Welcome and Introductions/Purpose and Exercise Overview
8:10 – 8:20	Highlights of ICANN gTLD Registry Continuity Plan
8:20 – 8:30	Exercise Format, Process, and Rules of Engagement
8:30 – 9:40	<u>PART 1</u> ICANN/Registry Roles, Responsibilities, and Obligations to Assure Service
9:40 –10:00	Break (Lunch set-up for East Coast)
10:00 –11:40	<u>PART 2</u> Registry Reporting Responsibilities, Responsiveness, and ICANN Options for Action
11:40 –12:00	Break (Lunch set-up for West Coast)
12:00 – 1:30	<u>PART 3</u> ICANN and Registry Actions, Coordination, and Communication to address a Registry Failure
1:30	End of Exercise Play
1:30 – 2:00	Data Collectors collectively prepare the Hotwash briefing; Participants confer within their organizations on lessons learned
2:00 – 2:45	Hotwash brief by Data Collector Team; report out from registries followed by general participant discussion
2:45 – 3:00	Wrap up / Next steps
3:00	Adjourn