JAS COMMUNICATIONS LLC
INFORMATION TECHNOLOGY · RISK MANAGEMENT · GOVERNANCE

After Action Report

IANA Full-Scale Business Continuity Exercise

Conducted 19 January 2010

JAS Communications LLC

23 February 2010

Founded in 2003, JAS Communications LLC is a unique professional services firm delivering risk management, technology, and governance solutions to a wide range of commercial and government clients.

http://www.jascommunications.com

Table of Contents

1 Executive Summary

JAS Communications LLC was engaged by ICANN in November 2009 to assist in the execution of a full-scale business continuity exercise. The exercise was designed to validate a yearlong effort by ICANN to improve the resiliency of critical business processes in ICANN's performance of the IANA functions.

Over the second half of 2009, ICANN undertook a series of discussion-based exercises culminating in the 19 January 2010 no-notice full-scale business continuity/disaster recovery exercise. In the full-scale exercise, production systems were taken offline and Marina del Rey-based IANA department staff were disallowed from working without advance notice.[1] All exercise scenarios were predicated on a massive disaster affecting the greater Los Angeles area, which rendered all systems and personnel in that geographical area unavailable for the duration of the exercise.

The Homeland Security Exercise and Evaluation Program (HSEEP) as specified by the U.S. Department of Homeland Security defines a full-scale exercise as *"…a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, emergency operation centers, etc.) and 'boots on the ground' response."* The 19 January 2010 exercise met this criterion by involving multiple functions within ICANN (including the IANA, IT, Security, and Communications Departments as well as Executive Management), and staff in the field working to restore production systems.

The primary objective of the exercise was to restore the production systems enumerated in the IANA Business Continuity Plan within four hours from the declaration of the disaster, leveraging remote staff and the Reston, Virginia, US hot site. Secondary objectives included validating several newly implemented communications and technical systems and processes.

The exercise was deemed a success in that most critical systems were restored within the first 30 minutes of the exercise and all systems were restored within 90 minutes. This is well within the four-hour timeframe. Additionally, stakeholders indicated that internal and external communications were appropriate and well received, and new procedures and systems functioned well.

JAS first had the opportunity to review ICANN's IANA Department operations in August 2009. We would like to call attention to and congratulate ICANN and IANA staff for the rapid pace of continuity planning and business process improvement that has taken place since then. The 19 January 2010 full-scale exercise was informed by a 24 November 2009 tabletop/discussion-based exercise and other ICANN business continuity activities. The Initial Planning Conference (IPC) for the 19 January 2010 exercise was held on 14 December 2009. The remainder of this document will focus on the 19 January 2010 full-scale exercise.

The ICANN exercise methodology is based on the U.S. Department of Homeland Security "Homeland Security Exercise and Evaluation Program" (HSEEP). HSEEP is a capabilities and performance-based exercise program which provides a standardized policy, methodology, and terminology for exercise

[1] Internal and external stakeholders were provided advanced notice via several communications describing the upcoming exercise in general terms and specifying a weeklong timeframe in which the exercise would occur.

design, development, conduct, evaluation, and improvement planning.[2] Adherence to the HSEEP framework ensures that exercise programs conform to established best practices and helps provide unity and consistency of effort for exercises throughout ICANN.

Key features of an HSEEP-derived exercise program include: clear exercise objectives, a structured Initial Planning Conference (IPC), execution pursuant to a Master Scenario Events List (MSEL), a "hotwash" debrief immediately following the exercise, and a timely After Action Report (AAR).

[2] **Homeland Security Exercise and Evaluation Program (HSEEP).** Federal Emergency Management Agency (FEMA), U.S. Department of Homeland Security (DHS). http://hseep.dhs.gov

2 Objectives

Clear objectives provide a framework for scenario development, guide development of individual organizational objectives, and supply evaluation criteria. HSEEP states that the best objectives are "Simple, Measurable, Attainable, Realistic, and Task-oriented" (SMART).

The discussion-based and full-scale exercises shared the following objectives:

1. Validate and demonstrate to internal and external stakeholders the resiliency of ICANN's IANA Department's critical business processes;
2. Validate assumptions concerning the physical distribution of IANA staff which affect business continuity;
3. Test and evaluate new technical business continuity measures, including the standby site in Reston, VA, US, and associated technical systems;
4. Test and evaluate communications mechanisms and messaging for communicating with multiple IANA function stakeholder groups during a continuity event;
5. Provide IANA staff valuable operational experience detecting and responding to a significant continuity event under stress;
6. Validate newly developed IANA Department Contingency Plan;
7. Validate newly developed IANA Department Continuity Guidebook;
8. Increase internal sophistication of business continuity planning in anticipation of forthcoming continuity improvements in other ICANN departments;
9. Capture lessons learned and identify opportunities for improvement.

3 Participants and Scope

The scope of the discussion-based and full-scale exercises included the entire IANA Department and ICANN Security, IT, and Communications Departments. Logistical assistance was provided by the Project Department. All departments were represented during the discussion-based exercises and during the planning and execution phases of the full-scale exercise.

Participant	Title	Home Base	Location during Ex	Role
Bickers, Geoff	Director, Security Operations	LA	Out-of-play	Observer - Security
Brent, Doug	Chief Operating Officer	LA	Marina del Rey, CA	Observer - COO
Closson, David	Director, IT Operations	LA	Marina del Rey, CA	Observer - IT
Conrad, David	VP Research & IANA Strategy	LA	Marina del Rey, CA	Observer - IANA
Cotton, Michelle	Manager, IETF Relations	Reno, NV	Reno, NV	Player - self
Davies, Kim	Manager Root Zone Services	LA	Out-of-play	Observer - IANA
Jones, Patrick	Senior Manager, Continuity & Risk	LA	Marina del Rey, CA	Exercise Controller
Jourdan, Michele	Communications	LA	Marina del Rey, CA	Observer - Comms
Lemont, Cinda	JAS	N/A	Via Telephone	Observer/Data Collection - JAS
Rattray, Greg	Chief Internet Security Advisor	San Antonio, TX	San Antonio, TX	Player - self
Roseman, Barbara	IANA Project Manager	Olympia, WA	Olympia, WA	Observer - IANA
Schmidt, Jeff	JAS	N/A	Marina del Rey, CA	Observer - JAS
Schruth, Cory	IANA Network Engineer	Portland, OR	Portland, OR	Player - self
Schwartz, Craig	Chief gTLD Registry Liaison	DC	Washington, DC	Player - stand-in for Brad White
White, Kevin	JAS	N/A	Via Telephone	Observer/Data Collection - JAS
Youkhanna, Joette	Project Office	LA	Marina del Rey, CA	Data Collection

4 Exercise Execution

The 19 January 2010 exercise was, in HSEEP parlance, a no-notice full-scale exercise. This means that the exercise involved multiple functional areas within ICANN, including field responders, and participation went beyond that of a 'thought exercise' to actual manipulation of production systems.

4.1 Risk Management

Because the exercise was performed on production systems, ICANN took measures to proactively and affirmatively manage the risk associated with performing a 'live fire' exercise. ICANN set a firm requirement that, under no circumstances, would downtime during the exercise exceed two hours, and set a procedure for handling priority work items arriving during the exercise, should this occur.

The exercise was scheduled to commence at 14:00 (US Pacific Time). A checkpoint was set at 15:30 PT (90 minutes into the exercise) at which time the state and availability of all production systems would be assessed by Exercise Control. If production services were not available at that time, the Exercise Controller could abort the exercise and instruct ICANN IT to immediately restore primary systems in Los Angeles.

ICANN IT thoroughly tested the involved IT systems during a series of tests in first week of January 2010. These tests occurred during published maintenance windows. ICANN IT was charged with documenting the techniques and procedures that would be used to take down and restore the IANA Departmental systems during the exercise, and specifically to provide confidence that the exercise could be aborted and LA systems restored in less than 30 minutes. ICANN IT provided a "thumbs-up" during the week of 11 January 2010.

A final go/no-go determination was made as scheduled on 19 January 2010 at 13:30 PT (30 minutes prior to exercise commencement). The Exercise Controller made the “go” determination after consulting with IANA Department management, ICANN IT, and Security.

4.2 Communications

On 11 January 2010, the ICANN Executive team received email notification that a no-notice business continuity exercise would be executed sometime during the next week (18-22 January). This email also described the general scenario, participants, evaluation criteria, and expected communications before, during, and after the exercise. A more general 'heads-up' was also provided to ICANN Staff by email later in the week of 11 January.

On 19 January, immediately following final go/no-go determination, email notification was sent to key internal and external stakeholders, including ICANN executive management, the RIRs, VeriSign, the chairs of the IETF and IAB, and the IANA Functions Contract Contracting Officer Technical Representative (COTR). This email informed these stakeholders of the pending continuity exercise, set expectations for system availability, and described the overall timeline. For internal stakeholders, this communication also described marking procedures in use during the exercise (for example, emails will contain the phrase "THIS IS AN EXERCISE").

As this was a no-notice exercise, remote participants were left to learn of the outage through technical monitoring systems and eventually through simulated media events that were a part of the exercise. When the exercise commenced, IANA staff physically present in Marina del Ray were asked to step away from their desks until further notice.

At 15:49 PT, after successful completion of the exercise, all internal and external stakeholders were notified by email of the successful conclusion of the exercise.

4.3 Exercise Timeline

While the complete Master Scenario Events List (MSEL) appears in Appendix A, what follows is a summary of the exercise planning and execution timeline. Note that this exercise was informed by a series of discussion-based exercises dating back to the fall of 2009; AARs for these exercises are available separately.

14 December 2009	Initial Planning Conference (IPC)
Week of 28 December 2009	ICANN IT prep/validation
Week of 11 January 2009	ICANN IT prep/validation; 'heads-up' communications
14 January 2009	Final Planning Conference and preliminary go/no-go
19 Jan 13:30 PT	Final go/no-go determination
19 Jan 14:00 PT	**Exercise commences**
19 Jab 14:54 PT	Most services back online; one minor issue remains
19 Jan 15:36 PT	Remaining minor issues resolved; fully operational
19 Jan 16:00 PT	Exercise complete; hotwash begins
19 Jan 16:00 PT	Controlled fail-back through the evening

5 Observations and Findings

In general, the exercise was a success in that the four-hour service restoration objective was met. Additionally, JAS observed that the team was competent, professional, organized, methodological, and worked well together under stress.

5.1 Workload was manageable

While under stress, participants were able to complete their tasks pursuant to the timeline in the continuity plan. Importantly, all communications to external stakeholders were dispatched on schedule with expected content.

5.2 Participants were adequately resourced

Participants had the knowledge, tools, and access to complete their tasks. This includes relevant access to backup systems, access terminals, communications tools, and account passwords/credentials. Additionally, participants had local access to relevant procedural documentation. Participants had received training on these systems and were well positioned to execute the continuity plan when called upon. Participants were in near constant communication among themselves and with stakeholder group representatives in a "Jabber" instant messaging conference room.

5.3 Work was structured and methodological

Participants followed the continuity plan to the best of their ability and methodologically evaluated checklists, performed scripted communications tasks, and kept careful track of time. Even when presented with a difficult and evolving scenario, at no time during the exercise did JAS perceive the response had devolved into an unorganized or ad-hoc endeavor.

5.4 Interrupt-driven communications were not debilitating

Participants did not appear to be overwhelmed by interrupt-driven communications, status requests, and other low value communications activities.

In JAS's experience, we have found that the burdens associated with providing timely updates to relevant internal and external stakeholders often overwhelm field responders. Specifically, we find that interrupt-driven requests must be carefully managed in order to not hinder the response activities. In addition, the more *accessible* the field responders, the greater the danger of being overwhelmed with status update requests; advances in communications technology have made field responders increasingly accessible, necessitating careful management of this issue.

We observe that ICANN managed this risk by instructing cross-functional representatives to silently observe the primary Jabber room (i.e. "lurking"). We found this approach to be an effective mechanism for providing real time situational awareness to an array of stakeholder representatives without being disruptive to field responders.[3] JAS notes that enforcing this discipline during an actual event is often challenging.

[3] In fact, JAS plans to explore the use of Jabber in this capacity with other clients.

5.5 Participants dealt with communications overload

While they were not overly burdened with interrupt-driven communications, several participants noted that they were overwhelmed by communications modalities, including monitoring telephone, Jabber, email, and SMS communications. The responsibility to monitor and be responsive across several forms of communication appeared distracting, but not debilitating.

Additionally, several Jabber conference rooms were in use, and there was initial confusion about who belonged where and which communications were appropriate for which room. In the end, activity essentially consolidated in one room.

5.6 Some participants unable to join the Jabber room promptly

Localized technical and/or training issues prevented some participants from joining the Jabber conference room quickly.

5.7 Lack of clarity in several areas of the contingency plan and guidebook

Participants noted several areas of the newly developed contingency plan and guidebook that were not clear. Exercise participants provided several recommendations regarding wording clarity and general organization of these documents.

5.8 Minor technical issues during failover

Several relatively minor technical issues surfaced during the failover and subsequent operation in Reston. These issues were, in general, scripting and configuration issues that were quickly detected and rectified manually. These issues have been noted by ICANN IT and IANA staff for follow-up.

5.9 Technical difficulties during fail-back

Failing back from the Reston facility to the Los Angeles facility after the exercise completed also presented some technical difficulty. This included data duplication and data loss in several Request Tracker (RT) tickets. ICANN IT and IANA staff anticipated these challenges prior to the exercise, documented the issues as they arose, rectified the issues manually following the exercise, and planned to follow-up with the RT software vendor for permanent solutions.

5.10 Summary of Findings

In general, JAS finds that the issues encountered were normal for a continuity exercise of this type - particularly for the first exercise undertaken by the organization. One of the primary objectives of a full-scale exercise is to identify the sort of relatively minor "gotchas" that were encountered during this exercise. In fact, typically these "gotchas" can *only* be identified during a full-scale exercise. The lessons learned during this exercise were valuable and will directly inform the next revision of the continuity plan and future exercises.

Some of the technical issues encountered during fail-back were slightly more concerning. The IT systems that support the IANA Department - particularly the Request Tracker ticketing system (RT) and the MySQL database RT uses for a data store - were implemented prior to the creation of the hot site in Reston, VA. Although RT and MySQL are mature technologies, they were selected and deployed prior to

the requirement to function in a multi-site failover architecture. JAS recommends that the selection and sufficiency of these systems be revisited in light of the new functional requirements.

6 Recommendations

6.1 Continue the exercise program

Business continuity procedures have a nasty habit of becoming 'stale' quickly. Business procedures and personnel change rapidly, and quite often continuity planning doesn't keep pace. ICANN has set a very good baseline for its performance of the IANA Functions.

6.2 Exercise a variety of scenarios

While destruction of the Los Angeles area was a relevant and challenging scenario for ICANN, other scenarios are also important and will stress different areas of the system. For example, JAS believes a valuable future exercise scenario could involve a 'for cause' termination of a trusted insider. Additionally, JAS believes a scenario where Internet connectivity was not available to participants would be instructive.

6.3 Consolidate communications modalities with succession plan

Several participants noted that they faced overload from an abundance of communications modalities. The primary and most effective communications modality was the Jabber conference room and JAS recommends that primary communications among active participants be consolidated there by policy and practice. Additional clarity is needed on the number of Jabber conference rooms, which roles should be represented in each room, and protocols for both active participants and silent observers in the event that the pace of activity (and the stress level of the participants) so dictates.

Jabber is a key component of ICANN's overall business communications infrastructure. As such, ICANN has deployed redundant Jabber servers in both its' Los Angeles and Reston datacenters. As leveraging such a service requires that all participants have Internet access, the IANA Departmental continuity plan defines a succession plan that includes the use of mobile phones, GETS/WPS, and satellite phones in the event Internet connectivity is unavailable.

JAS recommends an affirmative process be documented in the continuity plan for testing communications modalities and coming to agreement on the primary and secondary mechanism among all participants. This process should be executed soon after an event is declared and periodically thereafter to allow for changing communications capabilities and to discover newly available participants. In JAS' experience, this affirmative process typically results in a procedure akin to a Byzantine agreement protocol where all participants test all communications modalities and triangulate the common ground.

6.4 Continue to focus on roles instead of specific personnel

ICANN has increased the maturity of its service offerings by documenting business processes, roles, and responsibilities in its performance of the IANA functions. ICANN is fortunate to have a staff in its IANA Department predominately comprised of highly qualified experts with many years of loyal service. As ICANN continues to mature their processes, JAS encourages ICANN to sustain the focus on roles over the specific personnel filling those roles.

6.5 Formalize business continuity training

ICANN has made tremendous progress developing and formalizing business continuity procedures for its performance of the IANA functions. It is critical that recurring training on these procedures be systemic and incorporated into each employee's routine employment training regimen. In particular, several participants had technical difficulty accessing the Jabber conference room in a timely fashion; JAS believes this was largely a training issue and easily rectified.

6.6 Re-evaluate technology selections in light of new requirements

Pursuant to commentary in Section 5.10, JAS observes that core technology selections were made and implemented prior to the creation of the hot site in Reston. With the procurement of the Reston facility, a new series of requirements have emerged, necessitating performance in a multi-site failover architecture. JAS recommends that the selection and sufficiency of these systems be revisited in light of the new functional requirements.

6.7 Formalize personnel location policies

ICANN's IANA Department is critically dependant on several key employees based throughout the United States. The 19 January 2010 exercise confirmed that the geographic diversity was sufficient to survive a major disaster impacting the headquarters location in Los Angeles. However, these key employees travel frequently, often to the same meetings/locations worldwide. JAS believes the risks associated with co-located key personnel warrant formal policies.

7 Appendix A: Complete Master Scenario Events List (MSEL)

IANA Business Continuity Exercise - MSEL
January, 2010
ICANN CONFIDENTIAL

ID	Time/Trigger	Source	Event
	Week Of 21-Dec	Kim Davies	Heads-up in Holiday schedule email
	Week Of 11-Jan	Patrick Jones	Heads-up to Staff and key internal and external stakeholders
	Week Of 11-Jan	Patrick Jones	Final emergency comms check (no GETS/WPS for this exercise)
	Week Of 11-Jan	IT	Final "thumbs-up" from IT
	Day of Ex (all times PT)		**Start Time: 1400 PT**
-3	13:30	Controller	Final go/no-go determination
-2	13:30	Controller	Announcement to executive leadership, NTIA, and other key stakeholders. Begin marking all communications "THIS IS AN EXERCISE."
-1	13:45	IT	IT confirmation: ready to take down production systems
0	14:00	Controller	Event occurs. IT takes down production systems. Confirmation from IT to Controller that systems are down.
1	14:05	Controller	Survivors begin to receive a steady stream of status requests from a variety of internal and external stakeholders by phone, SMS, and online chat (ICANN email not operational).
2	14:10	Controller	Broadcast message to all players: "Media reporting major natural disaster in LA. All telecom networks swamped and unreliable nationwide. No more detail available at this time."
3	14:30	Controller	Status Check. ICANN email remains unavailable due to 3rd party dependency.
4	14:45	Controller	Broadcast message to all players: "Media reporting major natural disaster affecting Los Angeles area. Massive devastation and loss of life."
5	Cory advises all systems operational + 10 minutes	Controller	Phone call from XXX to Cory stating system YYY is unavailable.
6	ID 4 + 45 minutes	Controller	ICANN email begins to stabilize. Survivors are flooded with email status requests from all stakeholders.
7	15:00	Controller	Status Check.
8	15:15	Controller	Broadcast message to all players: "President Obama press conference. Confirms massive event. Military and national guard deployed to Southern California to assist."
9	15:30	Controller	90 minute fail-out checkpoint. If services are NOT verified operational in Reston, instruct IT to fail-back to LA production systems and abort the exercise.
10	16:00	Controller	2 hour checkpoint. Assure production systems are available, either in Reston or LA if the exercise was aborted.
11	16:30	Controller	Status Check. Check for "real" inbound requests; simulate several service requests if none in queue.
12	17:00	Controller	Status Check. Verify that real and/or simulated requests are being processed.
13	17:30	Controller	Status Check.
14	18:00	Controller	Status Check. 4 hour target service restoration window.
15	18:30	Controller	Status Check.
16	19:00	Controller	Status Check.
17	19:30	Controller	Status Check. IT instructed to restore LA systems, revert operations back to LA, and wind-down Reston operations.
18	20:00	Controller	Exercise ends. Confirm operation of production systems from LA. Send notice to all stakeholders confirming exercise conclusion. Cease marking communications as EXERCISE.