ICANN

gTLD Registry Failover Exercise

After Action Report

6 April 2008

THIS PAGE INTENTIONALLY LEFT BLANK

Contents

EXECUTIVE SUMMARY

The Internet Corporation for Assigned Names and Numbers (ICANN) executed a gTLD Registry Failover Exercise on 24 – 25 January 2008. The exercise was designed to validate the processes and procedures associated with implementation of the draft *ICANN gTLD Registry Failover Plan*, and test internal communication and processes around registry failure.

The exercise objectives were as follows:

- Validate and harden the draft *ICANN gTLD Registry Failover Plan*
- Train the staff for crisis response to specific failure situations
- Assess maturity of ICANN's technical decision making progress
- Achieve completion of a key ICANN project during fiscal year 07-08
- Provide clear, concise definitions and labels for each stage of this process

Exercise participants examined high-level issues related to the implementation of failover procedures. Discussions focused on following the draft *ICANN gTLD Registry Failover Plan* contingency planning elements:

- Notification when a suspected initiating event occurs
- ICANN preliminary examination
- Internal communications plan
- Communications with gTLD registry or sponsor
- Communications with registrars and registrants
- Decision on whether the registry or sponsor can continue operations
- Transition processes
- Closure of a registry

The exercise was developed and executed 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)[1]. The

[1] See http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf.

exercise was designed around five independent and distinct scenarios. Tools enabled the real-time participation by ICANN staff not physically present at the exercise location, from eight locations worldwide and seven different time zones.

Each scenario began with background information shown to the exercise participants. Additional information was provided via scenario-specific fact sheets prior to scenario execution. Scenarios progressed through the use of exercise injects. Participants followed the draft *ICANN gTLD Registry Failover Plan*[2] when formulating courses of action. Each scenario was executed to a logical conclusion.

This report provides details of the scenario, timeline, and lessons-learned from the exercise.

Significant Observations

Six major observations of exercise execution:

Observation 1: ICANN Role during Significant Domain Name System Events

The exercise highlighted opinions on aspects of the role of ICANN during an event that potentially affects the Domain Name System (DNS). There was active discussion on ICANN's role as an organizational facilitator during an event as opposed to a more limited informational role.

Observation 2: Definition of Event and Other Terminology

The draft *ICANN gTLD Registry Failover Plan* relies on the declaration of an event to initiate many of the significant internal responses. The clear definition of an event was initially not well-defined and it was therefore difficult to identify its occurrence. As a result of the exercise, the ICANN staff has revised the definitions in the failover plan.

Observation 3: Supporting Plans/Procedures for an Event

The draft *ICANN gTLD Registry Failover Plan* provides strategic guidance, but (by design) lacks the detailed internal ICANN event-specific steps for implementation. The exercise highlighted the need for additional internal ICANN supporting plans/procedures to aid in all facets of execution during normal operations or event response.

Observation 4: Internal Communication Flow during Normal Operations

The exercise highlighted the need for a more-formalized process for internal information flow during normal operations.

Observation 5: Registry Transition Procedures and Bankruptcy

The draft *ICANN gTLD Registry Failover Plan* anticipates procedures for the voluntary and non-voluntary transition of a registry. The exercise highlighted the need to define

---

[2] The participants worked from the 20 October 2007 draft of the failover plan (see http://www.icann.org/registries/failover/draft-plan-20oct07.htm). ICANN staff released an updated version of the gTLD Registry Failover Plan on 5 February 2008 based on lessons learned from the test exercise.

transition elements, in cooperation with existing registries.

Observation 6: Additional Observations

The exercise highlighted a variety of miscellaneous observations that do not conveniently fit into other observation categories.

Next Steps

ICANN is moving to turn the lessons learned from the gTLD Registry Failover Exercise into solutions. These include, but are not limited to, revisions to the draft *ICANN gTLD Registry Failover Plan*, discussions on the development and implementation of more-formalized internal procedures, policies, exercise development, and organizational changes.

The community must continue to improve its ability to effectively respond to and recover from a variety of potential crisis events. In doing so, ICANN can learn from these efforts to formalize practices into standard operating procedures. These procedures will help to clarify the roles and responsibilities of key stakeholders and organizations during an event involving a gTLD registry. In addition, the community should explore opportunities for further training and exercises.

INTRODUCTION

Overview

ICANN executed the gTLD Registry Failover Exercise on 24 – 25 January 2008. This event was the first-ever exercise designed to validate various aspects of company processes and procedures regarding the orchestration of DNS operations. Exercise execution was conducted in Marina del Rey, California and via collaborative tools and teleconferencing for remote participants in eight locations worldwide.

Purpose and Objectives

ICANN developed, implemented, and coordinated all aspects of the tabletop exercise, in consultation with experts from Delta Risk LLC. The exercise was designed to examine and validate the processes and procedures associated with the implementation of the draft *ICANN gTLD Registry Failover Plan*.

The exercise was designed to improve the readiness of ICANN and help refine draft *ICANN gTLD Registry Failover Plan* procedures. Exercise execution enabled the facilitation of communication among select personnel regarding the orchestration of ICANN recovery operations following events that could cause disruption to the DNS from a technical, business or other failure of a registry operator.

Scope

The exercise was developed and executed based on standard tabletop exercise protocol detailed in the NIST *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*. The exercise was designed around five independent and distinct scenarios. Each scenario had a logical starting and ending point. What transpired in the middle was largely up to the exercise participants. Scenarios were presented via collaborative tools such as Microsoft PowerPoint and the Adobe Connect Professional. This technology enabled the real-time participation by ICANN staff from eight locations worldwide.

Each scenario began with background information shown to the exercise participants. Additional information was provided via scenario-specific fact sheets prior to scenario execution. Scenarios progressed through the use of exercise injects and each scenario was executed to its logical conclusion. Participants followed the guidance offered in the draft *ICANN gTLD Registry Failover Plan* when formulating specific courses of action.

Exercise participants examined high-level issues related to the implementation of failover procedures. To achieve the exercise's stated objectives, discussions focused on following the draft *ICANN gTLD Registry Failover Plan* contingency planning elements:

- Notification when a suspected initiating event occurs
- ICANN preliminary examination
- Internal communications plan
- Communications with gTLD registry or sponsor

- Communications with registrars and registrants
- Decision on whether the registry or sponsor can continue operations
- Transition processes
- Closure of a registry

The gTLD Registry Failover Exercise provided participants with a controlled environment in which to exercise coordinated incident responses, including information sharing mechanisms, procedures for establishing situational awareness, public and private organizational decision making, and public communications during significant events. The exercise tested internal communication and processes around registry failure scenarios.

Key Achievements

The gTLD Registry Failover Exercise was an important milestone for ICANN. The following list highlights key exercise achievements:

- Executed a multi-scenario, multi-location DNS tabletop exercise with participants worldwide
- Organized and simultaneously exercised the response capability of ICANN, including the IANA function.
- Achieved internal and external coordination points during crisis response at the operational, policy, and public affairs levels
- Tested a full range of response policies, doctrine, and communication methodologies that would be utilized during a real-world event
- Identified needs for future preparation for and response to DNS community incidents
- Identified a variety of issues that warrant additional review through collaboration between participants and stakeholders, especially registry operators

SUMMARY OF MAJOR OBSERVATIONS

The gTLD Registry Failover Exercise yielded six major observations with significant impact to ICANN operations. Exercise participants and observers/controllers provided input and feedback, creating the aforementioned observations. Input was captured through direct observations during the exercise, as well as participant responses during post-exercise discussions.

Observation 1: ICANN Role during Significant Domain Name System Events

The exercise highlighted opinions on aspects of the role of ICANN during an event that potentially affects the DNS. There was active discussion of ICANN's role as an

organizational facilitator during an event, as opposed to a more limited informational role.

Discussion: ICANN Role during DNS Event

Exercise participants engaged in discussion of ICANN's role during an event involving the failure of a gTLD registry. Participants focused attention on the duty to registrants during an event, the elements that trigger ICANN involvement, and the flow of communications during an event. Participants noted that it would be useful for the Board and executive management to discuss ICANN's role in events.

Recommendation

Consideration be given to define ICANN's role and responsibilities regarding DNS event mitigation to staff and stakeholders. This clarification is important, especially within the context of the growth in the number of gTLD and ccTLD registries anticipated in the near future.

Note: ICANN has developed Internet Coordination Policies (ICPs), such as ICP-1, which describe the Internet Domain Name System structure and delegation and the IANA function's role as the overall authority for day-to-day administration of the DNS (see http://www.icann.org/icp/icp-1.htm). The *ICANN gTLD Registry Failover Plan* reflects a balance of ICANN's Core Value #1, "preserving and enhancing the operational stability, reliability, security and global interoperability of the Internet" and Core Value #9, "acting with a speed that is responsive to the needs of the Internet while, as part of the decision-making progress, obtaining informed input from those entities most affected."[3]

Discussion: Managing Events or Managing Appearance

Discussion amongst exercise participants centered on whether the ICANN role was to manage DNS events or to manage appearance. Many participants believed that both aspects were important.

Recommendation

See recommendation for ICANN Role during DNS Event.

Observation 2: Definition of Event and Other Terminology

The draft *ICANN gTLD Registry Failover Plan* relies on the declaration of an event to initiate many of the significant internal responses. The clear definition of an event was initially not well defined, making it difficult for personnel to declare one. This difficulty might put ICANN into a reactive posture throughout a failure.

Discussion: Definition of an Event

ICANN rewrote the definition of an event, and practiced the new definition during the exercise. By the end of the exercise, the new definition helped provide better

[3] ICANN Core Values, see http://www.icann.org/general/bylaws.htm#I.

guidance to participants.

Note: As a result of the exercise, staff revised the definitions for an "event" and added sections to the Failover Plan on situation handling and information sharing with gTLD registries.

Recommendation

ICANN to develop a term (e.g., incident) which allows for the internal tracking and notification of an item of interest that does not currently rise to the level of an event.

Recommendation

ICANN should develop procedures to formalize an internal Incident Response Team. This team would address issues relating to incidents (when appropriate) and work to find solutions before the incident becomes an event and requires the assembly of Crisis Response Team.

Discussion: Internal ICANN Coordination

The exercise highlighted the need to ensure greater coordination among ICANN departments leading up to the declaration of an event.

Recommendation

Consideration be given for ICANN to develop procedures for the internal information sharing and storage of incident/event information. These procedures might include utilization of a data fusion (e.g., dashboard) system that employees and leadership can access to view/update information.

Discussion: Denial of Service (DoS) Attacks

Exercise participants discussed ICANN responses to large-scale distributed DoS attacks. Discussion centered on whether the organization had the ability to detect an attack, and how information would flow to operators for event mitigation. IANA staff noted they currently do not undertake proactive monitoring of name servers. ICANN staff noted that they would not be involved unless an attack hit the root operators. The exercise demonstrated that tools to facilitate information sharing during an event would be beneficial.

Recommendation

Consideration be given for ICANN and IANA to develop a process for DoS attack-monitoring and information sharing. Suggestions offered during the exercise include contacting the relevant government authorities or registry operators.

Discussion: DNSSEC Compromise

One exercise scenario centered on the compromise of DNSSEC keys. Participants discussed numerous options, including the removal of the top-level domain from the root and retirement of the top-level domain under the emergency removal procedure. DNSSEC keys are considered a critical function of a registry (for a registry that has implemented DNSSEC) under the draft *ICANN gTLD Registry*

Failover Plan, yet exercise participants were reluctant to declare an event and form the Crisis Response Team.

Recommendation

Consideration be given for ICANN to clearly define what constitutes its involvement in management/orchestration of critical registry functions.

Discussion: DNSSEC Implementation

Exercise participants discussed how to ensure proper DNSSEC implementation and security. Although this was outside the scope of the exercise, it may be a worthwhile internal ICANN discussion on the process for validating and certifying DNSSEC registries.

Recommendation

Consideration be given for ICANN to investigate the value of auditing registries that implement DNSSEC to ensure all aspects are properly conducted.

Observation 3: Supporting Plans/Procedures for an Event

The draft *ICANN gTLD Registry Failover Plan* provides strategic guidance, but requires detailed internal ICANN event-specific steps for implementation. The exercise highlighted the need for additional internal supporting plans/procedures to aid in all facets of execution during normal operations or event responses. For example, a plan should be developed that documents the procedures for assembling a Crisis Response Team. The plan should clearly identify the event manager, identify who initiates a crisis team recall, details the procedures for contacting recalled personnel, provides guidance on each participant's role and responsibility, and provides generic templates (e.g., public release statements), etc.

Discussion: Lack of Documented Internal Procedures

Many internal ICANN procedures (normal operations and event responses) are not documented. The draft *ICANN gTLD Registry Failover Plan* relies on ICANN personnel to execute their portion of the plan, but many of these procedures have not been formally documented. Execution is based solely on the expertise and experience of the individuals conducting the response. When an individual is unavailable or no longer with ICANN, the ability of the company to effectively respond is potentially diminished.

Recommendation

ICANN to develop and document detailed plans and procedures to address normal operations and event responses. The plans should be tested routinely to ensure they continue to meet the organizational requirements.

Discussion: Event Manager

The exercise highlighted the need for a clearly defined Event Manager to handle and orchestrate ICANN's incident and event responses. Discussion centered on the appointment of an Event Manager (by the CEO or COO) so normal operations could continue, and ICANN would be postured to handle a second event if needed.

Recommendation

ICANN should develop procedures to assign an Event Manager to orchestrate and track internal incident/event responses. This individual would be responsible for the analysis of disparate information into a single common operational picture, tracking internal responses to incidents/events, ensuring leadership remains informed, and when necessary initiating/and tracking the whereabouts of the crisis response team.

Discussion: Ensuring Event Procedures are Accomplished

Declaration of an event initiates a series of internal and external ICANN responses. The process for ensuring completion of each response is not clearly delineated, nor is it centrally orchestrated.

Recommendation

See recommendation for Event Manager.

Discussion: Initial Event Investigation

The draft *ICANN gTLD Registry Failover Plan* calls for a preliminary examination of an event to determine its severity and to provide leadership with an initial analysis. The plan does not identify the individual responsible for this investigation, nor is it clear how the information is shared within ICANN.

Recommendation

See recommendation for Event Manager.

Discussion: Internal Information Flow

Information flow during an event is generally accomplished though *informal* mechanisms (email, personal one-on-one interaction, etc.). Informal information flow hinders efforts to build a common operational picture of the event, and ultimately slows ICANN's responses and effectiveness.

Recommendation

See recommendation for Internal ICANN Coordination (Observation 2).

Discussion: Information Capture

Information capture during an incident or event must be formally accomplished. Exercise discussion centered on the need to keep important information (logged phone calls, system files, registries information, etc.) that could be utilized by the Office of General Council if necessary during post-event investigation.

Recommendation

See recommendation for Internal ICANN Coordination.

Discussion: Process Maps/Decision Trees

Exercise participants were greatly aided by the use of process maps and decision trees. These tools guided incident response discussion and helped participants arrive at logical conclusions more quickly. Exercise discussion focused on tying these tools to qualifying criteria in service-level agreements and adding a level of

specificity based on each agreement.

Recommendation

ICANN to refine the process maps/decision trees based on participant discussion and lessons-learned from exercise execution. In addition, recommend inclusion in forthcoming internal ICANN procedures and support plans to the *ICANN gTLD Registry Failover Plan.*

Discussion: ICANN External Contacts List

During the course of a discussion a question was posed by a participant as to whether ICANN had a consolidated list of external contacts – registries, backend providers, etc., to use during an incident or event. It is not clear whether a consolidated is available for internal use.

Recommendation

ICANN should develop a consolidated list of contacts for notification during an incident or event.

Discussion: Public Affairs Releases

During the course of numerous scenarios, corporate public affairs representatives highlighted the need for a proactive public information process. This public affairs campaign should include positive events as well as the official ICANN position relative to the exercise (or real-world) scenario.

Recommendation

ICANN to develop a full-range of proactive public affairs procedures to ensure a single, consolidated message is presented. This plan should include procedures to route phone calls received at the reception desk, public affairs contact with registries to ensure the proper/correct message is being presented, and internal procedures for employees to follow when discussing the official ICANN position with external customers.

Observation 4: Internal Information Flow during Normal Operations

The exercise highlighted the need for a more-formalized process for internal information flow during normal operations. Intelligence indicators (e.g., late data escrow, delinquent payments, contract compliance issues, etc.,) are tracked by individual departments, but the fusion of these disparate indicators into a single sight-picture is missing.

Discussion: Data Collection/Fusion Capability

ICANN lacks a centralized data collection capability for use during normal daily operations. Exercise participants discussed real-world situations relating to late data escrow deposits, late payments, etc., and concluded these disparate pieces of information may appear in isolation, but collectively present a different picture – one that would be discussed internally within ICANN if collectively known.

Recommendation

Consideration be given for ICANN to develop and implement procedures for the

internal information sharing and storage of incident/event information during normal daily operations. These procedures might include utilization of a data fusion (e.g., dashboard) system that employees and leadership can access to view/update information.

Observation 5: Registry Transition Procedures and Bankruptcy

The draft *ICANN gTLD Registry Failover Plan* has procedures for the transition of a registry. The exercise highlighted the difficulty in implementing portions of the plan when a company has declared bankruptcy or is in receivership.

Discussion: Bankruptcy of a Registry/Backend Provider

Declaration of bankruptcy by a registry or backend provider could place the company under control of the courts, and potentially negatively impact registrants and affect the level/quality of DNS service within the affected TLD. The exercise highlighted difficulty in the implementation of portions of the plan when a company has declared bankruptcy or is in receivership.

Recommendation

ICANN to undertake a more-thorough examination of the affect of bankruptcy on the draft *ICANN gTLD Registry Failover Plan*. Recommend the development of detailed internal procedures and courses of action to provide guidance during a registry bankruptcy on registrants of the affected gTLD.

Discussion: Data Transition

Participants discussed the need for better understanding of the requirements for transition of a registry from one operator to another, and suggested active discussion with gTLD registries to improve needs in this area of the draft plan.

Recommendation

Further work should be conducted on the development of a data transition plan to identify the instances in which a registry can be transitioned from one operator to a successor, and on the process to follow if such a transition is to occur. Staff has arranged a series of meetings in April and May 2008 to move this work forward.

Observation 6: Additional Observations

The exercise highlighted a variety of miscellaneous observations that do not conveniently fit into other observation categories.

Discussion: Neutral Holding Facility

Exercise discussions highlighted the potential need for a neutral holding facility that could be utilized as a data repository during an event. For example, the holding facility could be used during a bankruptcy period to ensure uninterrupted DNS service during the crisis period.

Recommendation

Consideration be given for ICANN to engage the community on the feasibility of establishing a neutral holding facility in the event of registry failure.

Discussion: Temporary Resolution-only Services

The draft *ICANN gTLD Registry Failover Plan* has a provision that offers ICANN temporary resolution-only services until a top-level domain can be transitioned to a successor. Exercise discussions highlighted the fact that this implementation has not been thoroughly vetted and could potentially result in reactive implementation.

Recommendation

Consideration be given for ICANN to develop internal procedures to allow for the smooth transition of services. These procedures should include hardware and software requirements to clone a DNS server, the procedures for obtaining data escrow, reviewing and planning for potential billing/financial issues, and identifying individuals responsible for implementing this portion of the plan. Staff should also engage in further discussions with the gTLD registries on elements necessary for data transition in the event of registry failure.

Discussion: Data Escrow

Exercise discussions highlighted data escrow as an area where more work is necessary. Exercise participants voiced the need to conduct a thorough sample of data. The discussion focused on the lack of procedures for validating information deposited into escrow. Participants noted that the registry data escrow specifications may need to be updated.

Recommendation

Consideration be given to an examination of ICANN's need for a more-robust toolset to help analyze data escrow files (when necessary). The registry data escrow specifications should be updated prior to the publication of the Request for Proposals for new gTLD applications.

Discussion: Backend Registry "Certification" or "Qualification"

Exercise discussions highlighted the general lack of interaction/connection between ICANN and backend registry operators. Exercise participants were in favor of a more robust relationship with the backend provider community and a certification or qualification program for backend registry operations.

Recommendation

Consideration be given to backend registry operator certification or qualification to assist with registry failover and prepare for the launch of the new gTLD process. In the alternative, staff should explore standard or "best practices" criteria for the operation of critical registry functions.

EXERCISE PLAY

The exercise was developed and executed around five scenarios to simulate a variety of registry and DNS system issues directed against fictional registrars and registries. The intent of the scenarios was to initiate elements of the draft *ICANN gTLD Registry Failover Plan* and identify areas for improvement. Scenarios were developed with the assistance of industry experts and were executed in a closed and secure environment.

The exercise was a simulated event with no real-world effects on, tampering with, or damage to any critical infrastructure. While the scenarios were based on hypothetical but possible situations, they were not intended as a forecast of future registry or DNS-related events. The gTLD Registry Failover Exercise scenarios had ten major stimuli (injects):

- Escalation of temporary events
- Technical failure of a registry
- Security breach of a registry and compromise of DNSSEC keys
- Scenario involving an IDN registry
- Scenario involving a backend registry operator running both ccTLDs and gTLDs
- Natural disaster affecting a registry
- Terrorist attack affecting a registry
- Malfeasance affecting a registry
- Business failure of a registry
- Government intervention in a gTLD registry

The stimuli did not represent a specific or existing registry, domain, group, or nation state. Injects were designed to affect the trusted domain systems, the physical environment of notional registries, and call into question the business acumen of notional registry stakeholders. Effective responses to scenario injects were designed to require rapid communication between exercise participants in all sectors and organizations, as well as strategic integration of information to gain accurate situational awareness.

It is important to emphasize that the exercise scenarios were neither a forecast of particular threats/vulnerabilities nor were they an expression of any specific concerns. Rather, the exercise scenarios were designed to elicit participant action based off guidance offered in draft *ICANN gTLD Registry Failover Plan*. Descriptions of the scenarios discussed during the exercise are included in the Annex to this report.

CONCLUSION

The gTLD Registry Failover Exercise provided ICANN, IANA and DNS stakeholders with a neutral and controlled environment in which to exercise their response procedures to significant series of events. The exercise examined information sharing mechanisms, procedures for establishing situational awareness, coordinating internal and external decision-making processes, and communication of appropriate information to the public during DNS incidents of significance.

ICANN and DNS stakeholders are moving to turn exercise lessons-learned into solutions. These include, but are not limited to revisions to the draft *gTLD Registry Failover Plan*,

internal procedures, policy and practice development, and recommendations for organizational changes. Other exercise participants are also taking measures to address observations related to their organization.

The exercise presented many in the DNS community with scenarios not yet extensively dealt with during real-world operations. In order to effectively respond, the participants needed to communicate at the highest levels, with information requiring correlation, coordination, and collaboration. By and large, the participating organizations and their practices met the challenges presented, and where necessary improvised agreements and relationships to handle unexpected issues. A broader and deeper understanding of the draft *gTLD Registry Failover Plan* is needed by all members of the community.

The stakeholder community must continue to improve its ability to effectively respond to and recover from significant DNS-related events. The community should consider formalizing many of these practices into standard operating procedures and contingency plans. In addition, they should clarify the roles and responsibilities of each stakeholder and organization. Consideration be given to further training and exercises as an opportunity to validate these expanding support elements.

The interdependencies, gaps in response structure, and positive collaboration are critical parts of the gTLD Registry Failover Exercise lessons-learned and will have an enduring impact on the participant community.

Annex – Exercise Scenarios

Scenario 1

Scenario 1 focused on an escalation of temporary failures involving a fictional United States-based registry (.MOE). The scenario began with a US-based registrar informing ICANN's Registrar Liaison that it is having problems accessing the .MOE registry Shared Registry System (SRS). During the scenario, participants were told that the .MOE registry operated its own thick registry and did not have a backend registry operator.

.MOE reported the SRS problem to ICANN. A number of temporary outages continued throughout the scenario, including nameserver outages and WHOIS outages and missed data escrow deposits.

Staff discussed options for addressing temporary outages, including offering to locate or provide technical assistance to the registry, or helping the registry find a backend registry operator.

Scenario 2

The second scenario focused on issues related to a TLD with strict authentication requirements, limited to a specific community of business registrants. The TLD had signed its zone through deployment of DNSSEC.

In the scenario, a security breach occured resulting in the compromise of the registry's DNSSEC keys. Domain names from the TLD were used for phishing, which triggered an investigation from data protection authorities. The loss of confidence in the TLD resulted in bankruptcy.

Exercise participants discussed critical functions of a registry and registry failure involving a signed zone.

Scenario 3

This scenario centered on a fictional for-profit company that operates the بازار. IDN gTLD (*.bazaar/.market* in Urdu).

- A Category 5 cyclone hit the country where the gTLD is located
- Widespread destruction but the gTLD nameservers functioned with no loss of service
- The IDN TLD had not deposited its variant tables with the IANA IDN Registry
- The country's ccTLD was knocked off-line due to infrastructure damage from the cyclone
- Government infrastructure was unable to keep up with demands
- The IDN TLD switched operations to its secondary site located out of country
- Martial law and nationalization orders were issued in the country

- IANA received a delegation request from the national government for the ccTLD and the gTLD (now operated out of country)

Exercise participants determined that initial information on the cyclone from the affected country did not warrant initiation of the crisis response team. Discussions centered on whether there was a process for passing information internally within ICANN to keep leadership informed during this period.

IANA received reports of widespread damage and the inability of the government infrastructure to keep up with the demand. Exercise participants noted that the crisis response team had not yet been formed. The discussions centered on if/when an event is declared that an individual would be appointed as the event manager to coordinate the ICANN response.

ICANN was notified that IDN TLD had successfully transferred operations to its backup location outside the country. The discussions centered on whether ICANN should provide informational details on its website to keep the community informed. In addition, there were numerous discussions on the public relations aspect and the importance of managing communications.

After receiving the delegation request from the government, exercise participants focused on the technical and political ramifications of transferring the registry service back into the country. Participants discussed the feasibility of maintaining DNS service in a country beset with power outages, potential telecommunication service interruptions, and a government operating under martial law. Specific concerns were raised over the status of the backup and original registry location, status of data escrow, and on the dialog with the affected government. It was suggested that these actions would generate political pressure on ICANN from numerous fronts, and internal communications with the general area council were warranted.

Additional discussions centered on the status of the affected ccTLD and IANA/ICANN role in supporting its operations during this critical period. Robust discussions occurred on the level of contact between IANA and external stakeholders during these events.

Scenario 4

Scenario 4 described a complex attack on a backend registry operator. In the scenario, the registry operator services over 30 million registrations worldwide across five ccTLDs and eight gTLDs, and maintains a headquarters in Europe with operations centers in Europe and North America.

The registry announced that it had won a contract to provide backend registry services for a fictional IDN TLD using the Arabic script. The backend provider was hit with a DoS attack, followed by a terrorist attack. The registry operator activated its secondary backend location, but not all of the services rolled over to the secondary site. Some of the supported ccTLDs and gTLDs contacted IANA for assistance. The backend provider also terminated its agreement with the fictional IDN TLD as a result of the attack, leaving the new IDN TLD without a backend operator.

Exercise participants engaged in a lengthy discussion on backend registry providers and

ICANN's lack of direct contractual relationship with backend providers. Participants also touched on the sensitive political and communications issues raised by the scenario.

Scenario 5

The second day of the exercise was devoted to the fifth scenario. This scenario described "bad acts of a registry" as demonstrated by the fictional .MOE gTLD (used previously in Scenario 1). This scenario followed an escalation of bad acts, including:

- Failure to submit monthly report to ICANN
- Failure to submit data escrow deposit to escrow agent (followed by the transmission of corrupt data to the escrow agent)
- Misuse of company funds by management
- Federal Trade Commission and Internal Revenue Service investigation of registry
- Failure to make payments to ICANN
- Implementation of registry service (wildcard) without contract approval
- Registry turns off Registry-level WHOIS
- Failure to renew registrations
- Litigation forces registry into bankruptcy