Comments of the GNSO gTLD Registries Stakeholder Group on

Proposed Final Report & Recommendations of the
Inter-Registrar Transfer Policy – Part B
Policy Development Process

29 March 2011

Request for public comments URL:

http://www.icann.org/en/public-comment/#irtp-b-proposed-final-report

Regarding the issue noted above, the following statement represents the views of the ICANN GNSO gTLD Registries Stakeholder Group (RySG) as indicated. Unless stated otherwise, the RySG position comments were arrived at through a combination of RySG email list discussion, surveys and RySG meetings (including teleconference meetings).

The comments below are organized in the order of the issues and associated recommendations of the IRTP Working Group.

A. Issue 1

Whether a process for urgent return/resolution of a domain name should be developed, as discussed within the Security and Stability Advisory Committee (SSAC) hijacking report (http://www.icann.org/announcements/hijacking-report-12jul05.pdf); see also (http://www.icann.org/correspondence/cole-to-tonkin-14mar05.htm).

Recommendation #1 of the IRTP Part B Working Group:

The WG is considering recommending requiring registrars to provide an Emergency Action Channel (as described in SAC007 [PDF, 400 KB]). The WG recognizes that there are further details that would need to be worked out. This Emergency Action Channel could also be used for non-transfer abuse issues.

RySG Response:
Overall, the members of the RySG are supportive of the recommendation of the IRTP Part B Working Group that registrars provide an Emergency Action Channel. One registry noted that the Emergency Action Channel should be developed but only within certain parameters. A longer time to respond (up to 72 hours) may be necessary to accommodate smaller registrars that are not staffed 24x7. Another item to consider is the extent to which registries should be involved. For those registries that are sponsored and a validation process is involved, registries may have more insight into who the registrant

is and could, perhaps, assist. It should be noted, however that this is not consistent across all registries so care should be taken to ensure that any developments in this area could be administered consistently across all registries and TLDs.

In response to the working group's request for input on several related questions, the RySG responds as follows:

Within what timeframe should a response be received after an issue has been raised through the Emergency Action Channel (for example, 24 hours – 3 days has been the range discussed by the WG)?
RySG Response: More than half of the registries believe that 24 hours is sufficient time for a response after an issue has been raised through the Emergency Action Channel, while one registry believes that 48 hours is sufficient and another believes that 72 hours is appropriate. Further, one registry feels that the time range specified is appropriate but prefers the 24 hour time period in accordance with their own abuse policy.

What qualifies as 'a response'?
RySG Response: Most members of the RySG feel that at a minimum, a positive confirmation of receipt and initial human contact is appropriate. Many members also believe that the specific information relating to the issue and the next steps to be taken to resolve the issue should be required while two registries feel that a satisfactory resolution is required for the response to qualify.

Is an auto-response sufficient?
RySG Response: Most registries believe that an auto-response is not sufficient while at least two registries feel that an auto-response may be sufficient. Those registries that felt that an auto-response is not sufficient indicated that the purpose of the Emergency Action Channel ("EAC") should be to commence investigation and actually resolve the issue by individuals at the registrar. An auto-response would indicate that the issue was received but not that anyone is actively working on it. Auto-response is meaningless in this context, except to suggest that action will start "soon". The goal of the EAC should be to resolve the issue not to merely advise the receiving registrar that an issue exists.

Should there be any consequences when a response is not received within the required timeframe?
RySG Reponse: All registries agree that there should be consequences when a response is not received. Common themes included having defined escalation paths and that the consequences should become more severe for multiple occurrences up to and including termination of the violating registrar's accreditation by ICANN. One registry indicates that multiple instances of non-response within the required time frame should result in a warning from either ICANN or the Registrar's Stakeholder Group (RrSG) and a proactive contact from ICANN to determine the reasons. This registry further indicates that during the first year after the implementation of the

Emergency Action Channel, consequences should be more lenient and suggests that after the first year, there should be graduated consequences that could be up to revocation of ICANN accreditation for those registrars whose actions, or lack thereof, condone or enable hijacking. Additional thoughts were that consequences should be consistent with registries' existing abuse policies.

Is there a limited time following a transfer during which the Emergency Action Channel can be used?

RySG Response: The answer to this question by members of the RySG range from one business day to ten days to time periods that are consistent with existing transfer policies. Since urgency is critical, it is anticipated that violations would be discovered very quickly (particularly after a DNS change has occurred) therefore it is recommended that that this channel must be invoked within 7 days of the alleged incident. After this period, and for other non-urgent or non-emergency situations, the existing communication channels and Transfer Dispute Resolution Policy process could be used. Some registries feel that, consistent with the Transfer Dispute Resolution Policy, the Emergency Action Channel should not be available if 6 months has passed since the alleged violation occurred. More discussion on the timing is recommended since there are many views on this particular item.

Which issues may be raised through the Emergency Action Channel?

RySG Response: There were various positions on this item from the RySG. It is suggested that the criteria detailed in the SSAC report would be a good starting point. These included: 1. Immediacy of the harm to the registrant if the transfer is not reversed (e.g., business interruption, security incidents). 2. Magnitude of the harm, or the extent to which the incident threatens the security and stability of the parties other than the registrant, including but not limited to users, business partners, customers, and subscribers of a registrant's services. 3. Escalating impact, or the extent to which a delay in reversing the transfer (and DNS configuration) would cause more serious and widespread incidents. Some registries feel that anything that is an emergency including illegal transfers (hijacking of domains) through fraudulent actions, hacking of registry, registrar sites, changes of contact information to lock out the rightful registrants; changes of DNS creating an adverse impact to the rightful registrant, as well as possibly including other malicious domain activities such as those involving botnet, phishing, etc. At least one registry would like to have more discussion surrounding this while another would be concerned about extending the use of this channel beyond things that might have an immediate negative impact to the registrant.

Who is entitled to make use of the Emergency Action Channel?

RySG Response: More analysis / discussion is warranted. However, some registries feel that it should only be available to the registrant. Others feel that it should be limited to an authorized list of registrar and registry contacts. Still another feels that it should be limited to binding or apparent authorities while another feels that it could be extended to registries,

gaining/losing (affected) registrars, ICANN and approved contacts of recognized security and stability oriented groups in the internet community.

Recommendation #2 of the IRTP Part B Working Group:
The WG recommends that registrants consider the measures to protect domain registrar accounts against compromise and misuse described in SAC044, Section 5.

RySG Response: Most of the registries agree with this recommendation. However, one registry feels that this is a valuation issue of an asset (i.e., the domain) which is not applicable to the registry.

ISSUE B
Whether additional provisions on undoing inappropriate transfers are needed, especially with regard to disputes between a Registrant and Admin Contact. The policy is clear that the Registrant can overrule the AC, but how this is implemented is currently at the discretion of the registrar.

Recommendation #3 of the IRTP Part B Working Group:
The WG recommends requesting an Issues Report on the requirement of 'thick' WHOIS for all incumbent gTLDs.

RySG Response: All but one registry agreed with this recommendation. The registry that disagreed with the response pointed out that ICANN staff and GNSO volunteers are overloaded at this time.

Recommendation #4 of the IRTP Part B Working Group:
WG recommends requesting an Issue Report to examine 'Change of Control' function, including an investigation of how this function is currently achieved, if there are any applicable models in the country-code name space, and any associated security concerns.

RySG Response: All but one registry agreed with this recommendation. The registry that disagreed did so stating, again, that ICANN staff and GNSO volunteers are overloaded at this time.

Recommendation #5 of the IRTP Part B Working Group:
The WG recommends modifying section 3 of the IRTP to require that the Registrar of Record/Losing Registrar be required to notify the Registered Name Holder/Registrant of the transfer out.

RySG Response: Again, all but one registry agreed with this recommendation. The registry that did not indicated that notification would be a good thing but only if the registrant is not held hostage by the losing registrar presenting misleading information. It should be a simple, standard e-mail to be sent to the registrant and admin contacts.

ISSUE C
Whether special provisions are needed for a change of registrant near a change of registrar. The policy does not currently deal with change of registrant, which often figures into hijacking cases.

Recommendation #6 of the IRTP Part B Working Group:
Modification of denial reason #6 so that language is expanded and clarified to tailor it more to explicitly address registrar-specific (i.e. non-EPP) locks in order to make it clear that the Transfer Contact (often the registrant) must give some sort of informed opt-in express consent to having such a lock applied, and the registrant must be able to have the lock removed upon reasonable notice and authentication.

RySG Response: Most registries agree with this recommendation of the IRTP working group. However, one registry points out that reasonable must be clearly defined as some registrants have been asked for rather onerous documentation requirements when a contact is no longer an employee/associated with a domain and a new contact is trying to prove that they are an authorized agent for the domain. Another registry indicates that the clarification needs to accommodate court orders, etc., that preclude the lock being removed even with reasonable notice and authentication.

ISSUE D
Whether standards or best practices should be implemented regarding use of Registrar Lock status (e.g. when it may/may not be applied).

Recommendation #7 of the IRTP Part B Working Group:
If a review of the UDRP is conducted in the near future, the issue of requiring the locking of a domain name subject to UDRP proceedings is taken into consideration.

RySG Response: All members of the RySG agree with this recommendation.

Recommendation #8 of the IRTP Part B Working Group:
The WG recommends standardizing and clarifying WHOIS status messages regarding Registrar Lock status.

RySG Response: Again, all members with this recommendation but one member indicates that it must be done in accordance with any existing ICANN/registry agreement requirements.

ISSUE E
Whether, and if so, how best to clarify denial reason #7: A domain name was already in "lock status" provided that the Registrar provides a readily accessible and reasonable means for the Registered Name Holder to remove the lock status.

Recommendation #9 of the IRTP Part B Working Group:
The WG recommends deleting denial reason #7 as a valid reason for denial under section 3 of the IRTP as it is technically not possible to initiate a transfer for a domain name that is locked, and hence cannot be denied, making this denial reason obsolete. Instead denial reason #7 should be replaced by adding a new provision in a different section of the IRTP on when and how domains may be locked or unlocked.

RySG Response: All members of the RySG agree with this recommendation.

Summary of RySG Support

1. Level of Support of Active Members: Supermajority
   1.1. # of Members in Favor: 9
   1.2. # of Members Opposed: 0
   1.3. # of Members that Abstained: 0
   1.4. # of Members that did not vote: 4
2. Minority Position(s): None
3. General impact on the RySG: Minimal
4. Financial impact on the RySG: Minimal
5. Analysis of the period of time that would likely be necessary to implement the policy: Minimal

General RySG Information

- Total # of eligible RySG Members[i]: 14
- Total # of RySG Members: 13
- Total # of Active RySG Members[ii]: 13
- Minimum requirement for supermajority of Active Members: 9
- Minimum requirement for majority of Active Members: 7
- # of Members that participated in this process: 13
- Names of Members that participated in this process:
  1. Afilias (.info & .mobi)
  2. DotAsia Organisation (.asia)
  3. DotCooperation (.coop)
  4. Employ Media (.jobs)
  5. Fundació puntCAT (.cat)
  6. Museum Domain Management Association – MuseDoma (.museum)
  7. NeuStar (.biz)

8. Public Interest Registry - PIR (.org)
9. RegistryPro (.pro)
10. Societe Internationale de Telecommunication Aeronautiques – SITA (.aero)
11. Telnic (.tel)
12. Tralliance Registry Management Company (TRMC) (.travel)
13. VeriSign (.com, .name, & .net)

- Names & email addresses for points of contact
  - Chair: David Maher, dmaher@pir.org
  - Alternate Chair: Keith Drazek, kdrazek@verisign.com
  - Secretariat: Cherie Stubbs, Cherstubbs@aol.com
  - RySG representative for this statement: Barbara Steele, bsteele@verisign.com

[i] All top-level domain sponsors or registry operators that have agreements with ICANN to provide Registry Services in support of one or more gTLDs are eligible for membership upon the "effective date" set forth in the operator's or sponsor's agreement (RySG Articles of Operation, Article III, Membership, ¶ 1). The RySG Articles of Operation can be found at <http://gnso.icann.org/files/gnso/en/improvements/registries-sg-proposed-charter-30jul09-en.pdf>. The Universal Postal Union recently concluded the .POST agreement with ICANN, but as of this writing the UPU has not applied for RySG membership.

[ii] Per the RySG Articles of Operation, Article III, Membership, ¶ 6: Members shall be classified as "Active" or "Inactive". A member shall be classified as "Active" unless it is classified as "Inactive" pursuant to the provisions of this paragraph. Members become Inactive by failing to participate in a RySG meeting or voting process for a total of three consecutive meetings or voting processes or both. An Inactive member shall have all rights and duties of membership other than being counted as present or absent in the determination of a quorum. An Inactive member may resume Active status at any time by participating in a RySG meeting or by voting.