Final Report on the Inter-Registrar Transfer Policy - Part B Policy Development Process

STATUS OF THIS DOCUMENT

This is the Final Report on IRTP Part B PDP, prepared by ICANN staff, for submission to the GNSO Council on 30 May 2011, following public comments on the Initial Report of 29 May 2010 and the proposed Final Report of 21 February 2011.

SUMMARY

This report is submitted to the GNSO Council as a required step of the GNSO Policy Development Process.

TABLE OF CONTENTS

1. Executive Summary

1.1 Background

- The Inter-Registrar Transfer Policy (IRTP) aims to provide a straightforward procedure for domain name holders to transfer their names from one ICANN-accredited registrar to another should they wish to do so. The policy also provides standardized requirements for registrar handling of such transfer requests from domain name holders. The policy is an existing community consensus policy that was implemented in late 2004 and is now being reviewed by the GNSO.
- The IRTP Part B Policy Development Process (PDP) is the second in a series of five PDPs that address areas for improvements in the existing transfer policy.
- The GNSO Council resolved at its meeting on 24 June 2009 to launch a PDP to address the following five issues:
  a. Whether a process for urgent return/resolution of a domain name should be developed, as discussed within the SSAC hijacking report (http://www.icann.org/announcements/hijacking-report-12jul05.pdf; see also http://www.icann.org/correspondence/cole-to-tonkin-14mar05.htm);
  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;
  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 in hijacking cases;
  d. Whether standards or best practices should be implemented regarding use of Registrar Lock status (e.g., when it may/may not, should/should not be applied);
  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.

- The IRTP Part B Working Group published its Initial Report on 29 May 2010 in conjunction with the opening of a public comment forum (see section 6 for further details).
- As, based on the review of the public comments and further deliberations, the WG made substantial changes to the proposed recommendations, the WG put forward a proposed Final Report for Community consideration. Following review of the public comments and additional consideration on some of the items as outlined in the proposed Final report, the WG has now finalized the report for submission to the GNSO Council.

1.2 Deliberations of the Working Group

- The IRTP Part B Working Group started its deliberations on 25 August 2009 where it was decided to continue the work primarily through first bi-weekly and then weekly conference calls, in addition to e-mail exchanges.
- Section 5 provides an overview of the deliberations of the Working Group conducted both by conference call as well as e-mail threads.

1.3 Recommendations of the Working Group

All the recommendations listed below have full consensus support from the Working Group.

- Recommendations for Issue A

  Recommendation #1 – The WG recommends requiring registrars to provide a Transfer Emergency Action Contact (TEAC). To this end the WG recommends to update the language of section 4 (Registrar Coordination) and Section 6 (Registry Requirements of the Inter-Registrar Transfer Policy as follows:

  Transfer Emergency Action Contact (Append to Section 4)

  Registrars will establish a Transfer Emergency Action Contact (TEAC) for urgent communications relating to transfers. The goal of the TEAC is to quickly establish a real-time conversation between registrars (in a language that both parties can understand) in an emergency. Further actions can then be taken towards a resolution, including initiating existing (or future) transfer dispute or undo processes.

Communications to TEACs will be reserved for use by ICANN-Accredited Registrars, gTLD Registry Operators and ICANN Staff. The TEAC point of contact may be designated as a telephone number or some other real-time communication channel and will be recorded in, and protected by, the ICANN RADAR system.

Communications to a TEAC must be initiated in a timely manner, within a reasonable period of time following the alleged unauthorized loss of a domain.

Messages sent via the TEAC communication channel must generate a non-automated response by a human representative of the gaining Registrar. The person or team responding must be capable and authorized to investigate and address urgent transfer issues. Responses are required within 4 hours of the initial request, although final resolution of the incident may take longer.

The losing registrar will report failures to respond to a TEAC communication to ICANN Compliance and the registry operator. Failure to respond to a TEAC communication may result in a transfer-undo in accordance with Section 6 of this policy and may also result in further action by ICANN, up to and including non-renewal or termination of accreditation.

Both parties will retain correspondence in written or electronic form of any TEAC communication and responses, and share copies of this documentation with ICANN and the registry operator upon request. This documentation will be retained in accordance with Section 3.4 of the Registrar Accreditation Agreement (RAA). Users of the TEAC communication channel should report non-responsive Registrars to ICANN. Additionally, ICANN may conduct periodic tests of the Registrar TEAC communication channel in situations and a manner deemed appropriate to ensure that registrars are indeed responding to TEAC messages.

(Append to Section 6) 6 iv. Documentation provided by the Registrar of Record prior to transfer that the Gaining Registrar has not responded to a message via the TEAC within the timeframe specified in Section 4.
In addition, update section 6 to reflect that the registry, in case of a transfer undo, will reverse the transfer and reset the registrar of record filed to its original state ('In such case, the transfer will be reversed and the Registrar of Record field ~~domain name~~ reset to its original state').

Recommendation #2 - The WG notes that in addition to reactive measures such as outlined in recommendation #1, proactive measures to prevent hijacking are of the utmost importance. As such, the WG strongly recommends the promotion by ALAC and other ICANN structures of the measures outlined in the recent report of the Security and Stability Advisory Committee on A Registrant's Guide to Protecting Domain Name Registration Accounts (SAC 044). In particular, the IRTP WG recommends that registrants consider the measures to protect domain registrar accounts against compromise and misuse described in SAC044, Section 5. These include practical measures that registrants can implement "in house", such as ways to protect account credentials and how to incorporate domain name registrations into employee or resource management programs typically found in medium and large businesses. It suggests ways that registrants can use renewal and change notifications from registrars as part of an early warning or alerting system for possible account compromise.

- Recommendations for Issue B

  Recommendation #3 - The WG recommends requesting an Issues Report on the requirement of 'thick' WHOIS for all incumbent gTLDs. The benefit would be that in a thick registry one could develop a secure method for a gaining registrar to gain access to the registrant contact information. Currently there is no standard means for the secure exchange of registrant details in a thin registry. In this scenario, disputes between the registrant and admin contact could be reduced, as the registrant would become the ultimate approver of a transfer. Such an Issue Report and possible subsequent Policy Development

Process should not only consider a possible requirement of 'thick' WHOIS for all incumbent gTLDs in the context of IRTP, but should also consider any other positive and/or negative effects that are likely to occur outside of IRTP that would need to be taken into account when deciding whether a requirement of 'thick' WHOIS for all incumbent gTLDs would be desirable or not.

Recommendation #4: The WG notes that the primary function of IRTP is to permit Registered Name Holders to move registrations to the Registrar of their choice, with all contact information intact. The WG also notes that IRTP is widely used to affect a "change of control," moving the domain name to a new Registered Name Holder. The IRTP Part B WG recommends requesting an Issue Report to examine this issue, including an investigation of how this function is currently achieved, if there are any applicable models in the country-code name space that can be used as a best practice for the gTLD space, and any associated security concerns. The policy recommendations should include a review of locking procedures, as described in Reasons for Denial #8 and #9, with an aim to balance legitimate transfer activity and security. Recommendations should be made based on the data needs identified in the IRTP Part B workgroup discussions and should be brought to the community for public comment. The WG would like to strongly encourage the GNSO Council to include these issues (change of control and 60-day post-transfer lock) as part of the next IRTP PDP and ask the new working group to find ways to quantify their recommendations with data.

Recommendation #5: 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. The Registrar of Record has access to the contact information for the Registrant and could modify their systems to automatically send out the Standardized Form for Losing Registrars ("Confirmation FOA") to the Registrant.

- Recommendation for Issue C

  Recommendation #6: The WG does recognize that the current language of denial reason #6 is not clear and leaves room for interpretation especially in relation to the term ‘voluntarily’

and recommends therefore that this 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 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. The WG recommends to modify denial reason #6 as follows:
Express objection to the transfer by the authorized Transfer Contact. Objection could take the form of specific request (either by paper or electronic means) by the authorized Transfer Contact to deny a particular transfer request, or a general objection to all transfer requests received by the Registrar, either temporarily or indefinitely. In all cases, the objection must be provided with the express and informed consent of the authorized Transfer Contact on an opt-in basis and upon request by the authorized Transfer Contact, the Registrar must remove the lock or provide a reasonably accessible method for the authorized Transfer Contact to remove the lock within five (5) calendar days.

- Recommendations for Issue D

  Recommendation #7: The WG recommends that 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.

  Recommendation #8: The WG recommends standardizing and clarifying WHOIS status messages regarding Registrar Lock status. The goal of these changes is to clarify why the Lock has been applied and how it can be changed. Based on discussions with technical experts, the WG does not expect that such a standardization and clarification of WHOIS status messages would require significant investment or changes at the registry/registrar level. The WG recommends that ICANN staff is asked to develop an implementation plan for community consideration which ensures that a technically feasible approach is developed to implement this recommendation.

- Recommendation for Issue E

  Recommendation #9: 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. The WG recommends that ICANN staff is asked to develop an implementation plan for community consideration including proposed changes to the IRTP to reflect this recommendation.

1.4 Public Comment Period on the Proposed Final Report

- The public comment period on the Proposed Final Report resulted in seven (7) community submissions. The summary and analysis of the comments received can be found in section 6.5. The Working Group reviewed and discussed the public comments received using a public comment review tool that details the Working Group's responses to the public comment received and the actions taken as a result.

1.5 Conclusions and Next Steps

- The WG has submitted this report to the GNSO Council for its consideration.

2. Objective and Next Steps

This Final Report on the Inter-Registrar Transfer Policy (IRTP) Part B PDP is prepared as a required step in the GNSO Policy Development Process (PDP) as described in the ICANN Bylaws, Annex A (see http://www.icann.org/general/bylaws.htm#AnnexA). It is based on the Initial Report of 29 May 2010 and the proposed Final Report of 21 February 2011 and has been updated to reflect the review and analysis of the comments received by the IRTP Part B PDP Working Group in addition to further deliberations. This report is submitted to the GNSO Council for its consideration. The conclusions and recommendations for next steps on the five issues included in this PDP are outlined in Section 7.

3. Background

- The issues that IRTP Part B Policy Development Process addresses are:
  a. Whether a process for urgent return/resolution of a domain name should be developed, as discussed within the SSAC hijacking report (http://www.icann.org/announcements/hijacking-report-12jul05.pdf; see also http://www.icann.org/correspondence/cole-to-tonkin-14mar05.htm);
  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;
  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 in hijacking cases;
  d. Whether standards or best practices should be implemented regarding use of Registrar Lock status (e.g., when it may/may not, should/should not be applied);
  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.
- The GNSO Council resolved at its meeting on 24 June 2009 to launch a PDP on these five issues and adopted a charter for a Working Group on 23 July 2009 (see Annex B WG Charter).
- The IRTP Part B Working Group published its Initial Report on 29 May 2010 in conjunction with the opening of a public comment forum (see section 6 for further details).
- Based on the review of the public comments and further deliberations, the WG made substantial changes to the proposed recommendations and put forward a proposed Final Report for Community consideration. Following review of the comments received on the proposed Final Report, the WG has now finalized its report and submits it to the GNSO Council for its consideration.

For further background information on the issues as well as the process, please see Annex A.

4. Approach taken by the Working Group

The IRTP Part B Working Group started its deliberations on 25 August 2009 where it was decided to continue the work primarily through first bi-weekly and then weekly conference calls, in addition to e-mail exchanges. The Working Group agreed to start working on the five different issues in parallel to the preparation of constituency statements and the public comment period on this topic. In order to facilitate the work of the constituencies, a template was developed for responses (see Annex B).

4.1 Members of the IRTP Part B Working Group

The members of the Working group are:

Name	Affiliation*	Meetings Attended (total # of meetings: 59)
Simonetta Batteiger[1]	RrSG	22
James Bladel	RrSG	53
Eric Brown	RySG	6
Berry Cobb	CBUC	52
Michael Collins[2]	Individual	27
Chris Chaplow	CBUC	47
Graham Chynoweth	RrSG	2
Paul Diaz	RrSG	55
Kevin Erdman	IPC	45
Anil George	IPC	29
Rob Golding[3]	RrSG	18
Oliver Hope[4]	RrSG	13
George Kirikos[5]	Individual	2

[1] Joined the WG on 13 August 2010
[2] Left the WG on 15 November 2010
[3] Joined the WG on 24 June 2010
[4] Joined the WG in June 2010 to replace Matt Mansell
[5] Joined the WG on 31 May 2010, left WG on 17 July 2010

Name	Affiliation*	Meetings Attended (total # of meetings: 59)
Mark Klein	RrSG	0
Matt Mansell[6]	RrSG	4
Bob Mountain[7]	RrSG	34
Michele Neylon (WG Chair)	RrSG	54
Mike O'Connor	CBUC	51
Mike Rodenbaugh	CBUC	1
Tim Ruiz (Council Liaison)	RrSG	6
Boudouin Schombe	NCUC	21
Matt Serlin	RrSG	35
Barbara Steele	RySG	46
Rudi van Snick	At Large	3
Miriam Trudell[8]	IPC	2
Danny Younger	At Large	0

The statements of interest of the Working Group members can be found at http://gnso.icann.org/issues/transfers/soi-irtp-b-sep09-en.htm.

The attendance sheet can be found here.

The email archives can be found at http://forum.icann.org/lists/gnso-irtp-b-jun09/.

RrSG – Registrar Stakeholder Group

RySG – Registry Stakeholder Group

CBUC – Commercial and Business Users Constituency

NCUC – Non Commercial Users Constituency

IPC – Intellectual Property Constituency

[6] Joined the WG on 22 March 2010 and was replaced by Oliver Hope in June 2010
[7] Joined the WG on 30 April 2010
[8] Left the WG in September 2010

5. Deliberations of the Working Group

This chapter provides an overview of the deliberations of the Working Group conducted both by conference call as well as e-mail threads. The points below are just considerations to be seen as background information and do not necessarily constitute any suggestions or recommendations by the Working Group, apart from those specifically labelled 'recommendation'.

5.1 Working Group Deliberations

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

- The WG reviewed the SSAC hijacking report, as well as the more recent report on Measures to Protect Domain Registration Services Against Exploitation or Misuse (SAC40) and discussed these with Dave Piscitello, ICANN's Senior Security Technologist. Piscitello explained that the interest of the Security and Stability Advisory Committee (SSAC) in unauthorized transfers was mainly related to unauthorized transfers as a result of hijacking whereby a third party gains unauthorized access to the domain name registration and transfers the registration to another registrar. As a result, SAC 40 is mainly focused on how to prevent the unauthorized take-over of a domain name registration. One of the suggestions made was to consider a multi-party confirmation before a transfer would be carried out.
- The question was raised whether there are ways to identify a 'hijacked domain name registration' transfer from a 'normal' transfer, but Piscitello noted that he was not aware of any study in anomaly detection. He added that there might be some markers that together could form a fingerprint of malicious behaviour, but this could only be done on a case-by-case basis. He suggested that one approach would be to look at the quality of registration data, e.g. a long-standing client, with accurate information is suddenly updated with 'inaccurate' contact details.

- Some pointed out that even though an urgent return of a domain name might be desirable, due diligence would be required by registrars, which normally takes time, unless there would be a safe harbour provision that would limit liability.
- The question was raised what the role of the registry is in hijacking incidents and it was noted that the registry is more of a bystander in the process as it relies on the information provided by the registrar and will only get involved if a dispute is filed under the Transfer Dispute Resolution Policy (TDRP). It was noted that certain registry providers offer special registry lock services which allow for locking of a domain name registration at the registry level, requiring two-factor authentication to make changes to the status of the domain name.
- The WG noted that instead of starting with developing a separate procedure, the group should start with reviewing the existing Transfer Dispute Resolution Policy in order to determine whether it would be possible to adapt this policy to allow for an urgent return / resolution of a domain name registration. A detailed presentation on the TDRP was provided by Eric Brown, Neustar. In reviewing the TDRP, the WG concluded that the TRDP is a relatively little used method for disputing / undoing inter-registrar Transfers as:
  a. For Registrants, especially those who are victims of "hijacking," the process is too slow, and potentially expensive.
  b. For Registrants and Internet Users, the Harm of a name resolving to a disputed site (or not resolving at all) persists while the TDRP proceeding is ongoing.
  c. For Registrars, the TDRP is seen as too slow, resource expensive, and could yield unpredictable outcomes.
  d. Larger Registrars have developed informal procedures to work together to rapidly reverse transfers that were erroneous or fraudulent, but still wish to preserve a formal policy to escalate matters to the Registry in the event that registrars cannot agree on the remedy.
  e. Some registered name holders have eschewed the TDRP and Registrar contact entirely, and prefer to work directly with ICANN to resolve disputed transfers.
  f. VeriSign has adopted it's own procedure under its Supplemental Rules to augment the TRDP whereby the registry facilitates the “undo” of a transfer upon agreement and consent of both the gaining and losing registrars. This procedure significantly shortens the transfer dispute process in those cases where both the gaining and losing registrars agree that a transfer was

processed in violation of the IRTP and that the domain name should be reinstated with the losing registrar. Other registries may have equivalent procedures, or may seek to develop them. It was noted that the TDRP is slow and resource intensive, in addition it was pointed out that a dispute under the TDRP can only be filed by a registrar, not a registrant. Some noted that in its current form it might not be workable to open the TDRP to registrants, but that it might be worth providing more information about this policy to registrants as well as registrars as one of the possible avenues to be explored in the case of a dispute.

- The WG also discussed in which circumstances an urgent return / resolution might be desirable such as when unauthorized changes to the DNS and registrant contact details have taken place which might result in the loss of control by the registered name holder of the domain name registration resulting in an unauthorized transfer. Nevertheless, the WG agreed that it would not be possible to establish a list of criteria that would qualify a transfer for an urgent return / resolution, but that the trigger would be a registrant contacting their registrar with the claim that their domain name registration was transferred as a result of a hijack.
- Several of the registrars participating in the WG pointed out that in practice registrars will work together to solve these kinds of situations, but it was noted that an escalation process might be desirable in cases where a registrar would be unresponsive or unwilling to co-operate.
- The WG discussed how to unite the need for urgent return / resolution with due process in one procedure as it was recognized that in the former speed is of the essence, while for the latter appropriate time would be needed to make an accurate assessment of the situation. Some suggested that a way forward might be to consider a procedure which, when invoked, would result in the immediate return to the situation prior to the transfer (e.g. DNS and registrant details), with no possibilities for further changes (e.g. Registry Lock) until an assessment of the situation had occurred and a determination had been made whether the transfer was legitimate or not.
- In order to explore the options for an urgent return / resolution in further detail, the WG formed a sub-team to prepare a proposal for an Expedited Transfer Reverse Procedure (ETRP) (see Initial Report for further details).
- The proposal for an ETRP received a substantial amount of comments during the public comment period (see Chapter 6).

- In addition, the WG carried out an aftermarket survey to receive further input on the need for an ETRP and specific comments on the proposed procedure (see http://forum.icann.org/lists/gnso-irtp-b-jun09/msg00531.html).
- The Working Group reviewed the comments received, the results of the aftermarket survey and the original proposal and has arrived at the conclusion that the ETRP, as drafted, is complicated and could generate severe unintended consequences. One of the main issues identified with the ETRP approach was the need for registrars and/or registries to judge the merits of a hijacking claim by the losing registrant – essentially making them responsible for high-speed dispute evaluation/resolution and leaving the process open to gaming. The Working Group therefore proposes to drop the ETRP proposal.
- As noted before, in practice most registrars work together to address issues like hijacking and resolve these in an expedient manner, a problem occurs when a registrar is non-responsive. To this end, the WG discussed the possibility of requiring registrars to provide a Transfer Emergency Action Contact (as also proposed in SAC007). As described in SAC 007 the objective of a Transfer Emergency Action Contact (TEAC) would be 'to provide 24 x 7 access to registrar technical support staff who are authorized to assess the situation, establish the magnitude and immediacy of harm, and take measures to restore registration records and DNS configuration to what is often described as "the last working configuration". An urgent restoration of a hijacked domain may require the coordinated efforts of geographically dispersed registrars, operating in different time zones. The emergency action channel requires a contact directory of parties who can be reached during non-business hours and weekends'. The WG recognized that further details would need to be worked out and therefore asked specific input during the public comment period on the following questions:
    - Within what time should a response be received after an issue has been raised through the Transfer Emergency Action Contact (for example, 24 hours – 3 days has been the range discussed by the WG)?
    - What qualifies as 'a response'? Is an auto-response sufficient?
    - Should there be any consequences when a response is not received within the required timeframe?
    - Is there a limited time following a transfer during which the Transfer Emergency Action Contact can be used?

- Which issues may be raised through the Transfer Emergency Action Contact?
- Who is entitled to make use of the Transfer Emergency Action Contact?

Following review of the public comments received and continued deliberations, the WG developed a detailed proposal for the TEAC as outlined in recommendation #1 below. In addition, the WG developed a FAQ that aims to answer the main questions in relation to the TEAC, which can be found in Annex C.

- The WG also reviewed the Security and Stability Advisory Committee's Advisory titled 'A Registrant's Guide to Protecting Domain Name Registration Accounts' (SAC 044). SAC 044 discusses, amongst others, the importance of maintaining accurate domain name contact information. It discusses the value of diversifying domain contact information (for example, creating separate identities for registrant, technical, administrative, and billing contacts) and methods to protect email delivery to the registrant's points of contact against disruption attacks. SAC044 also identifies types of documentation registrants should maintain to "prove registration" in cases where disputes might arise. SSAC recognizes that certain registrants may want external parties to manage nearly all aspects of domain registration. SAC 044 identifies questions related to domain account security that registrants can ask so they can make an informed choice when selecting a registrar or third party (such as an online brand protection agent or hosting provider).

Recommendations for Issue A

Recommendation #1 – The WG recommends requiring registrars to provide a Transfer Emergency Action Contact (TEAC). To this end the WG recommends to update the language of section 4 (Registrar Coordination) and Section 6 (Registry Requirements of the Inter-Registrar Transfer Policy as follows:

Transfer Emergency Action Contact (Append to Section 4)

Registrars will establish a Transfer Emergency Action Contact (TEAC) for urgent communications relating to transfers. The goal of the TEAC is to quickly establish a real-time conversation between registrars (in a language that both parties can understand) in an emergency. Further actions can then be taken towards a resolution, including initiating existing (or future) transfer dispute or undo processes.

Communications to TEACs will be reserved for use by ICANN-Accredited Registrars, gTLD Registry Operators and ICANN Staff. The TEAC point of contact may be designated as a telephone number or some other real-time communication channel and will be recorded in, and protected by, the ICANN RADAR system.

Communications to a TEAC must be initiated in a timely manner, within a reasonable period of time following the alleged unauthorized loss of a domain.

Messages sent via the TEAC communication channel must generate a non-automated response by a human representative of the gaining Registrar. The person or team responding must be capable and authorized to investigate and address urgent transfer issues. Responses are required within 4 hours of the initial request, although final resolution of the incident may take longer.

The losing registrar will report failures to respond to a TEAC communication to ICANN Compliance and the registry operator. Failure to respond to a TEAC communication may result in a transfer-undo in accordance with Section 6 of this policy and may also result in further action by ICANN, up to and including non-renewal or termination of accreditation.

Both parties will retain correspondence in written or electronic form of any TEAC communication requests and responses, and share copies of this documentation with ICANN and the registry operator upon request. This documentation will be retained in accordance with Section 3.4 of the Registrar Accreditation Agreement (RAA). Users of the TEAC communication channel should report non-responsive Registrars to ICANN. Additionally, ICANN may conduct periodic tests of the Registrar TEAC communication channel in situations and a manner deemed appropriate to ensure that registrars are indeed responding to TEAC messages.

(Append to Section 6) 6 iv. Documentation provided by the Registrar of Record prior to transfer that the Gaining Registrar has not responded to a message initiated via the TEAC communication channel within the timeframe specified in Section 4.

In addition, update section 6 to reflect that the registry, in case of a transfer undo, will reverse the transfer and reset the registrar of record filed to its original state ('In such case, the transfer will be reversed and the Registrar of Record field ~~domain name~~ reset to its original state').

Implementation Recommendations for Recommendation #1

- In the first phase of implementation, the WG recommends that the ICANN Registrar Application and Database Access Resource (RADAR) system is used to record the TEAC point of contact.
- In order to avoid potential abuse of the TEAC for non-emergency issues or claims that TEAC messages did not receive a timely response, the WG recommends that the RADAR system is adapted, as part of a second phase implementation, so that registrars log in to send or respond to a TEAC, with both transactions time stamped with copy to ICANN and the Registry.
- The Working Group recommends that the GNSO perform a follow-up review of the TEAC 12 to 24 months after the policy is implemented to identify any issues that may have arisen and propose modifications to address them. This review should specifically address whether the TEAC is working as intended (to establish contact between registrars in case of emergency), whether the TEAC is not abused (used for issues that are not considered an emergency) and whether the option to 'undo' a transfer in case of failure to respond to a TEAC should be made mandatory.

Recommendation #2 - The WG notes that in addition to reactive measures such as outlined in recommendation #1, proactive measures to prevent hijacking are of the utmost importance. As such, the WG strongly recommends the promotion by ALAC and other ICANN structures of the measures outlined in the recent report of the Security and Stability Advisory Committee on A Registrant's Guide to Protecting Domain Name Registration Accounts (SAC 044). In particular, the IRTP WG recommends that registrants consider the measures to protect domain registrar accounts against compromise and misuse described in SAC044, Section 5. These include practical measures that registrants can implement "in house", such as ways to protect account credentials and how to incorporate domain name registrations into employee or resource management programs typically found in medium and large businesses. It suggests ways that registrants can use renewal and change notifications from registrars as part of an early warning or alerting system for possible account compromise.

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

- The WG noted that in 'thin'[9] registries no registrant email addresses are collected which makes it complicated for the gaining registrar to contact the registrant to confirm the transfer. At the same time, it was pointed out that if such information would be available for all registries, it might make the system more vulnerable to hijacking, although it was also noted that just because additional information is collected under a 'thick' WHOIS model, it does not necessarily mean that such information is publicly displayed. It was pointed out that the current proposals in the new gTLD process require all new gTLD registries to run a 'thick[10]' WHOIS.
- Most agreed that the possibility for the registrant to overrule the administrative contact should be preserved as a security measure.
- It was pointed out that under the current rules, the Form of Authorization (FOA) is used by the Gaining Registrar to obtain express authorization from either the Registered Name Holder or the Administrative Contact. It was suggested that a possible way forward would be to require first contacting the Registered Name Holder, in those cases where the contact information would be available, followed by contacting the Administrative Contact as a second option, with the Registered Name Holder remaining authoritative. It was noted that this would not address the situation for transfers in 'thin' registries, as no contact information for the Registered Name Holder is publicly available. It was noted that it might be worth reviewing the work on the WHOIS service requirements that is currently being undertaken to determine whether it addresses this issue. It was suggested in one of the public comments received on the Initial Report that a more consistent use of the FOA among losing registrars might help reduce the number of instances when a transfer dispute arises.
- It was also suggested in one of the public comments received on the Initial Report that registrars should consider implementing a consistent policy regarding the proof required to undo a domain name transfer, which was supported by a number of WG members.

[9] A thin WHOIS output includes only a minimum set of data elements sufficient to identify the sponsoring registrar, the status of the registration, and the creation and expiration dates of each registration.
[10] Thick WHOIS output includes a broader set of data elements including contact information for the registrant and designated administrative and technical contacts.

- The WG discussed section 3 of the IRTP which currently offers the option to the Registrar of Record to notify the registrant that a transfer has been requested. The WG agreed that requiring this notification might alert the registrant at an earlier stage that a transfer has been requested, which as a result would bring any potential conflicts to light before a transfer has been completed and therefore might reduce the number of conflicts between the admin contact and registrant that would require undoing a transfer.
- To facilitate the discussion, the WG developed an overview of standard use cases (see Annex E).

Recommendations for Issue B

Recommendation #3 - The WG recommends requesting an Issues Report on the requirement of 'thick' WHOIS for all incumbent gTLDs. The benefit would be that in a thick registry one could develop a secure method for a gaining registrar to gain access to the registrant contact information. Currently there is no standard means for the secure exchange of registrant details in a thin registry. In this scenario, disputes between the registrant and admin contact could be reduced, as the registrant would become the ultimate approver of a transfer. Such an Issue Report and possible subsequent Policy Development Process should not only consider a possible requirement of 'thick' WHOIS for all incumbent gTLDs in the context of IRTP, but should also consider any other positive and/or negative effects that are likely to occur outside of IRTP that would need to be taken into account when deciding whether a requirement of 'thick' WHOIS for all incumbent gTLDs would be desirable or not.

Recommendation #4: The WG notes that the primary function of IRTP is to permit Registered Name Holders to move registrations to the Registrar of their choice, with all contact information intact. The WG also notes that IRTP is widely used to affect a "change of control," moving the domain name to a new Registered Name Holder. The IRTP Part B WG recommends requesting an Issue Report to examine this issue, including an investigation of how this function is currently achieved, if there are any applicable models in the country-code name space that can be used as a best practice for the gTLD space, and any associated security concerns. The policy recommendations should include a review of locking procedures, as described in Reasons for Denial #8 and #9, with an aim to balance legitimate transfer activity and security. Recommendations should be made based on the data needs identified in

the IRTP Part B workgroup discussions and should be brought to the community for public comment. The WG would like to strongly encourage the GNSO Council to include these issues (change of control and 60-day post-transfer lock) as part of the next IRTP PDP and ask the new working group to find ways to quantify their recommendations with data.

Recommendation #5: 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. The Registrar of Record has access to the contact information for the Registrant and could modify their systems to automatically send out the Standardized Form for Losing Registrars ("Confirmation FOA") to the Registrant.

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 in hijacking cases

- The WG discussed the practice that is currently applied by various registrars to lock a domain name registration for a sixty day period following a change of registrant to prevent hijacking and/or unauthorized transfer of a domain name registration. It was pointed out that registrants receive a clear warning when changing the registrant details, noting that it will not be possible to transfer the domain name registration for a period of 60 days. It was also pointed out that in these circumstances, a registrant could first carry out a transfer and then change the registrant details in order to prevent the 60-day lock. It was noted that some registrars do provide the possibility for registrants to unlock the domain in the 60-day period if the appropriate credentials are provided.
- Further clarification on this practice was also provided by ICANN Compliance which noted amongst others that: 'At the outset, it's helpful to point out the distinction between changes to Whois information where the registrant simply updates the Whois contact information (i.e., Whois Update) versus where Whois information is updated as a result of the registered name holder being changed from an existing registrant A to a new registrant B (Registrant Change). We understand GoDaddy.com's 60-day lock only applies to the Registrant Change scenario. If the 60-day lock is applied to the Whois Update scenario, it would be inconsistent with the Registrar Advisory Concerning the Inter-Registrar Registrant Change Policy (3 April 2008) (Advisory), since registrants and registrars are obligated to keep Whois information up-to-date. Requiring registrants to agree to

such terms would contradict with these obligations. The Advisory, however, only addresses mandatory updates to Whois contact information, not a transfer or assignment to a new registrant (i.e., the Registrant Change scenario, which is not a service that registrars are required to provide under the RAA). Further, the transfer policy does not prohibit registrars from requiring registrants to agree to the blocking of transfer requests as a condition for registrar facilitation of optional services such as the transfer of a registration to a new registrant' (see original email for further details).

- It was also pointed out that some registrars do not allow a transfer of a domain name registration for 60-days following a transfer which is an option foreseen under reason of denial #9 in the IRTP: 'A domain name is within 60 days (or a lesser period to be determined) after being transferred (apart from being transferred back to the original Registrar in cases where both Registrars so agree and/or where a decision in the dispute resolution process so directs). "Transferred" shall only mean that an inter-registrar transfer has occurred in accordance with the procedures of this policy'. Some suggested that it should be explored whether this should be a mandatory instead of optional provision. Some suggested that it should not be an issue if a lock in these circumstances would be applied as long as there would be a possibility for the registrant to unlock the domain, provided that the appropriate credentials are provided. The working group discussed whether the introduction of stricter locking procedures after a domain name transfer might be prudent to ease the resolution of hijacking issues, as well as other enforcement / takedown problems. At this point the working group lacked access to data on the number of hijacking cases with resolution problems due to the transfer hopping practice vs. the number of legitimate transfers benefitting of a less stringent locking policy and could therefore not come to consensus on the locking topic. Data on the frequency of hijacking cases is a pivotal part of this analysis. Mechanisms should be explored to develop accurate data around this issue in a way that meets the needs of registrars to protect proprietary information while at the same time providing a solid foundation for data-based policy-making. Data on legitimate transfer activity benefitting from the current locking policy wording needs to be collected. The WG notes that the 60-day post-transfer lock is currently optional (IRTP Reason for Denial #9), and that most large registrars follow this practice. It is however currently possible to ask for the removal of a lock (or not apply it in the first place) which would no longer exist should the policy be changed. The WG would like to emphasize that reason of denial #9 relates to a transfer, not to a change of control (change of registrant), although the WG realized as a result of its deliberations

that transfers are often closely linked to a change of control. The WG recommends that the issue of transfer 'hopping' after hijacking be considered in conjunction with the issue of the lacking "change of control" function while also taking a review of the domain locking options in IRTP into account. All three pieces should be included as part of the Issue Report on "change of control" (see recommendation #4).

- Currently some registrars do allow for unlocking when appropriate credentials are provided, while others do not. Some expressed concern regarding the voluntary nature of this practice as required under denial reason # 6 if there is no possibility to remove the lock, noting that a 60-day lock might not be considered problematic, but what if it would be applied for an unspecified duration. It was suggested that registrars should make clear in the registration agreement or a separate policy how a registrant can remove a voluntarily lock if so desired.
- In relation to this issue (Charter Question C and denial reason #6), it was suggested by ICANN staff that it might be beneficial to expand and clarify this language to tailor it more to explicitly address registrar-specific (i.e. non-EPP) locks in order to make it clear(er) that 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. This denial reason could potentially be split into two reasons of registrant objection for denial -- (1) express objection to a particular transfer, and (2) a general indefinite request to deny all transfer requests.
- There was agreement that a clear and concise definition needs to be developed of what constitutes a ‘change of registrant’. Most agreed that a change of only the email address does not consist of a registrant change, but it was noted that in some ccTLDs such as .uk any change to the registrant field is considered a change of registrant.
- The WG discussed how to prove the identity of the registrant and there were suggestions to have a consistent way across registrars to validate the identity of a registrant. Others pointed out that uniformity might not necessarily be a good thing from a security perspective as a single standard could result in unintended consequences. The WG debated how to go about avoiding minimum standards resulting in lowest common denominator while at the same time trying to raise the standard for those below par.
- The WG concludes that a change of registrant near a change of registrar is a substantial "indicator" of fraudulent activity. However, it also concludes that the event per say is not a special event and is

commonly performed by registrants moving domains between registrars immediately prior to a transfer.

- Go-Daddy's solution to preventing transfers, where the registrant has elected to do so, in this scenario is applauded for best practice, but it would be overly onerous to impose the same model on the registrar base as a whole. The "indicator" however remains valuable and registrars should be encouraged to use this information to prevent fraudulent activity as best practice. Any move to implement policy to force use of this indicator or provide such information to the receiving registrar will be documented policy and therefore short lived fraud protection.

Recommendation for Issue C

Recommendation #6: The WG does recognize that the current language of denial reason #6 is not clear and leaves room for interpretation especially in relation to the term 'voluntarily' and recommends therefore that this 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 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. The WG recommends to modify denial reason #6 as follows:

Express objection to the transfer by the authorized Transfer Contact. Objection could take the form of specific request (either by paper or electronic means) by the authorized Transfer Contact to deny a particular transfer request, or a general objection to all transfer requests received by the Registrar, either temporarily or indefinitely. In all cases, the objection must be provided with the express and informed consent of the authorized Transfer Contact on an opt-in basis and upon request by the authorized Transfer Contact, the Registrar must remove the lock or provide a reasonably accessible method for the authorized Transfer Contact to remove the lock within five (5) calendar days.

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

- Some noted that the current language of the IRTP where it is noted that a 'Registrar of Record may deny a transfer request' results in different approaches as there is no obligation for the Registrar of

Record to deny a transfer in the specific instances identified in the policy. This might lead to confusion for registrants.

- All agreed that any standards or best practices discussed in this context should only apply to the "Registrar Lock" status as defined in RFC 2832, or its equivalent, "Client Delete Prohibited/Client UpdateProhibited/Client Transfer Prohibited" (see RFC 5731). It should not refer to any internal flag or status termed "lock" which a registrar may be using.
- The WG discussed one of the ideas raised in the context of the public comments which noted that in the EPP protocol it is possible to associate each status value, such as clientDeleteProhibited, clientUpdateProhibited and clientTransferProhibited, with a message which would be displayed in Whois, which might be used to provide further details on why the Lock has been applied and what can be done to change the status. In order to explore this idea further, Scott Hollenbeck from VeriSign and author of EPP, participated in one of the WG meetings to provide further insight into the technical requirements for this option. He pointed out that additional extensions to a status value are technically possible, but they would be optional in the protocol and the needed capability may already be present by using the optional message field. He added, that a way to mandate the content and use of such an option linked to the registrar lock status would be to adopt it as part of the IRTP.
- The WG agreed that in order to manage expectations it might be helpful to set certain parameters in relation to the locking and unlocking of domain names.
- In order to clarify the different status values, the WG, in co-operation with the ICANN Communications Department, developed an EPP Status Codes overview that can be found in Annex F and which will be posted on the relevant sections of the ICANN web-site.
- In response to a comment received from WIPO, the WG agreed that locking a domain name registration subject to a UDRP dispute should be a best practice. In addition, the WG noted that any changes to making this a requirement should be considered in the context of any potential UDRP review.

Recommendations for Issue D

Recommendation #7: The WG recommends that 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.

Recommendation #8: The WG recommends standardizing and clarifying WHOIS status messages regarding Registrar Lock status. The goal of these changes is to clarify why the Lock has been applied and how it can be changed. Based on discussions with technical experts, the WG does not expect that such a standardization and clarification of WHOIS status messages would require significant investment or changes at the registry/registrar level. The WG recommends that ICANN staff develop an implementation plan for community consideration which ensures that a technically feasible approach is developed to implement this recommendation.

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

- The WG noted that in order to address this issue, a first point of discussion would be to define 'readily' and 'reasonable'. Some suggested that providing some examples of what is considered 'readily' and 'reasonable' might help, instead of providing a rigid definition.
- There was some support for one of the ideas raised during the public comment period to require ICANN Compliance to conduct yearly checks to verify that registrants can lock and unlock domains as intended by the policy.
- Some suggested that registrars should be required to provide further information to registrants as to why a domain name registration is in lock status.
- The WG reviewed the new language for denial reason #7 proposed by the Registry Stakeholder Group ("Prior to receipt of the transfer request, the domain name was locked pursuant to the Registrar's published security policy or at the direction of the Registered Name Holder provided that the Registrar includes in its registration agreement, the terms and conditions upon which it locks domains and further that the Registrar provides a readily accessible and reasonable means for the

Registered Name Holder to remove the lock status. If the Registrar does not provide a means to allow a Registered Name Holder to remove the lock status themselves, then Registrar must facilitate removing the lock within 5 calendar days of receiving a request from the Registered Name Holder."), but some questioned whether 5 days would be too long. The WG also discussed what should be considered as unresponsive and noted that international standards might differ.

- At the request of the WG, additional feedback was received from the ICANN Compliance and Legal Department in relation to this issue noting that:
  - Lack of definition of "readily accessible and reasonable means" – what is reasonable will depend on registrar practices and designated security level of a particular domain. Hence it is difficult to set or apply a standard or definition to all.
  - Denial reason #7 – this seems superfluous as a ground for denying a transfer request. If a domain is in "lock status", the registry cannot initiate a transfer request (so there will not be a ground for denial based on #7). As such, this might be best deleted as a valid reason for denial under section 3 of the IRTP and instead replaced (by adding a new provision in a different section of the IRTP) on when and how domains may be locked or unlocked.
  - It would be helpful if registrars are required to publish on their website their security policy (terms and conditions upon which it locks domains), which must be consistent with bullet the recommended new provision, if it becomes available. This will hopefully more prominent or noticeable for registrants and others (than "buried" in the registration agreement).

Recommendation for Issue E

Recommendation #9: 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. The WG recommends that ICANN staff is asked to develop an implementation plan for community consideration including proposed changes to the IRTP to reflect this recommendation.

5.2 Input provided by ICANN Compliance

On the request of the WG, the ICANN Compliance Department provided further information on the number and type of complaints received in relation to IRTP. The information provided is based on an analysis of IRTP related complaints received between July and November 2009 (1329 complaints). On the basis of that information, the following issue ranking (from most to lowest complaints) was provided:

1. EPP / Authinfo Code (24%)
2. Reseller (24%)
3. Failure to unlock domain by registrar (15%)
4. Registrant does not understand transfer process / transfer denied (9%)
5. Expiring domains (6%)
6. Ownership (6%)
7. Control Panel (4%)
8. Nacking / wrongful denial of transfer by registrar (4%)
9. Whois Issues (4%)
10. Stolen Domain / Hijacking (3%)
11. Privacy / Proxy (1%)

For further information, please see the detailed data provided by the ICANN Compliance Team.

6. Stakeholder Group / Constituency Statements & Public Comment Periods

This section features issues and aspects of the IRTP Part B PDP reflected in the statements from the GNSO stakeholder groups / constituencies and comments received during the public comment period.

6.1 Initial Public Comment Period

The public comment period ran from 14 September 2009 to 5 October 2009. Seven (7) community submissions from six different parties were made to the public comment forum. Three submissions related to issues not of relevance to the charter questions, such as WHOIS accuracy, privacy and a complaint relating to a specific registrar. The other contributors provided input on the different charter questions or other related issues for consideration. A summary of all comments can be found here: http://forum.icann.org/lists/irtp-b/msg00007.html. The public comments on this forum are archived at http://forum.icann.org/lists/irtp-b/. The IRTP Part B WG reviewed and discussed the public comments received thoroughly with the assistance of an analysis grid developed for that purpose. There were relevant and appropriate, information and suggestions derived from the public comments received have been included in chapter 5.

6.2 Constituency / Stakeholder Group Statements

The Constituency Statement Template was sent to all the constituencies and stakeholder groups. Feedback was received from the Registrar Stakeholder Group, the Registry Stakeholder Group, Business and Commercial Users' Constituency and the Intellectual Property Interests Constituency. These entities are abbreviated in the text as follows:

Registrar Stakeholder Group - RrSG

Registry Stakeholder Group - RySG

Business and Commercial Users' Constituency – BC

Intellectual Property Constituency - IPC

6.3 Constituency / Stakeholder Group Views

The full text of the constituency statements that have been submitted can be found on the IRTP Part B WG Workspace. These should be read in their entirety. The following section attempts to summarize key constituency views on the issues raised in the context of IRTP Part B PDP. In order to facilitate the review of the comments received, the WG developed this analysis grid in which the WG's response and views to each of the comments can be found.

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

The RrSG suggests that a possible adjustment and refinement of the Transfer Dispute Resolution Policy (TDRP) could be considered to reduce the overall timeframe to resolve disputes. In addition, it suggests that the WG could discuss best practices for the voluntary transfer of domain name registrations in cases of fraud. The RySG, on the other hand, suggests that the development of such a process should be addressed separately from the IRTP and TDRP, but adds that a quick resolution of this type is normally best served when addressed at the registrar level. The IPC is of the opinion that a process for urgent return / resolution should be developed. The BC agrees that registrants need a mechanism to quickly restore a domain to its prior state when hijacking occurs and a robust process to resolve the dispute in a timely manner. The BC does note that hijacking issues may be best addressed outside of the IRTP and TDRP.

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

The RrSG notes that the current policy is clear; if the policy is not adhered to, ICANN should consider providing additional guidance in the form of an advisory. The RySG recommends implementing a consistent policy regarding the proof required to undo a domain name transfer in this scenario, such as a notarized affidavit signed by the registrant and proof of identity. In addition, it suggests that a template could be provided as a guide. The IPC agrees that additional provisions are needed to have a uniform and consistent policy. The BC asserts that registrants need a way to address all inappropriate transfers; a speedy mechanism to return the domain name registration to its previous operational state coupled with a consistent, robust, transparent and timely dispute resolution process. In addition, it notes that such a dispute resolution process would depend for the most part on registrars, but should allow for escalation when a registrar is unable or unwilling to participate.

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 in hijacking cases**

The RySG is of the opinion that this issue is best addressed separately from the IRTP, as the IRTP only concerns transfers between registrars, not registrants. Nevertheless, the RySG would support a modification to the list of reasons for denying a transfer to include this as a valid reason provided that registrars include a provision within their registration agreements with registrants detailing this restriction and employing a mechanism by which a registrant may provide specific proof of rights to the domain in order to by-pass the 60 day restriction requirement. In addition, the RySG notes that there is a need to develop a clear and concise definition of what constitutes a 'change of registrant'. The IPC agrees that special provisions are needed as part of a system of uniform frontline measures that can aid in uncovering potential hijacking attempts. The BC suggests that this might be addressed by arriving at a consistently applied post-transfer hold policy.

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

The RySG notes that it should be left up to the individual registrars how and when a registrar lock status may / should or may not / should not be used. On the other hand, the IPC and BC are of the opinion that standards or best practices should be implemented.

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**

The RySG recommends that in order to provide a consistent user experience, registrars should use the EPP statuses to 'lock' domains and proposes to include the terms and conditions of the practice of locking domains in the registration agreement. In addition, it provides the following proposed language for denial reason #7: "Prior to receipt of the transfer request, the domain name was locked pursuant to the Registrar's published security policy or at the direction of the Registered Name Holder provided that the Registrar includes in its registration agreement the terms and conditions upon which it locks domains and further that the Registrar provides a readily accessible and reasonable means for the Registered Name Holder to remove the lock status. If the Registrar does not provide a means to allow a Registered Name Holder to remove the lock status themselves, then Registrar must facilitate removing the lock within 5 calendar days of receiving a request from the Registered Name Holder." The IPC agrees that it may be reasonable to clarify denial reason #7 so that it expressly states that such denial may include actions to address red flags that registrars become aware of, relating to denial reason #1 concerning evidence of fraud.

6.4 Public Comment Period on Initial Report

Following the publication of the Initial Report on 29 May 2010, a public comment forum was opened to which seventeen (17) community submissions from thirteen (13) different parties were made. The contributors are listed below in alphabetical order (with relevant initials noted in parentheses):

- Andrew Allemann (AA)
- Steve Crocker (SC)
- Internet Commerce Association by Phil Corwin (ICA)
- George Kirikos (GK) – five submissions
- Donna Mahony (DM)
- Brian Null (BN)
- Oversee.net by Mason Cole (ON)
- Eric Shannon (ES)
- Peter Stevenson (PS)
- Registrar Stakeholder Group by Clarke Walton (RrSG)
- Registries Stakeholder Group by David Maher (RySG)
- Jeffrey Williams (JW)
- Roy White (RW)

Three submissions (BN, DM, GK) requested an extension of the deadline for submission of public comments, which was subsequently extended by the IRTP Part B PDP WG for two weeks. Despite four other submission, one submission of GK notes that he 'will passively resist by not participating in a process that only leads to predetermined outcomes', noting that he 'may or may not support aspects of the current topic or proposal'. The other submissions provided input on the content of the Initial Report with a particular focus on the proposed Expedited Transfer Reversal Policy. A summary of these comments has been provided below.

General Comments

JW points out the importance of a registrant request and/or approval before a domain name registration is transferred. RW notes that he does not support the changes proposed in the report. Without going into further detail, he considers that 'these changes are inherently dangerous to anyone who might at one time or another actually sell a domain name/website'. The RrSG notes that the WG seems to have spend a substantial amount of time on developing the ETRP and recommends that the WG going forward 'focus more time on consideration of the other IRTP B issues'.

Charter Question A / Expedited Transfer Reversal Policy

PS acknowledges that domain name hijacking is problem that should be addressed but considers the proposed ETRP 'only a bandaid'. He notes that his main concern is that the current proposal 'does not require any due process' as it does not require the original registrant to demonstrate that the transfer was not authorized. Furthermore, he observes that the current proposal does not include any information on how to dispute an ETRP and suggests that 'a signed Domain Name Sale agreement, or evidence of payment of a purchase price into the original registrant's bank account' should provide sufficient evidence to dispute an ETRP. He also recommends that items such as indemnification and how to address potential abuse of the procedure are further fleshed out.

AA encourages the WG to undertake further research to 'scope out the size of the problem' and request disclosure from registrars on the number of domain names that are hijacked each month. If such disclosure finds that hijacking is 'a large enough problem', he recommends that the WG consider the following issues in relation to the ETRP and IRTP in general:

- Potential impact on the secondary domain name market;
- Security efforts should focus on problem and not become overly broad e.g. lock after change of email address;
- Consider limiting the number of transfers that can take place in a certain period as domains are sometimes transferred from one reputable to another reputable registrar before it is then transferred to a less reputable registrar;
- 30 days should be maximum time during which an ETRP can be initiated;
- There should be sufficient time for the new registrant to respond to an ETRP claim.

Several submissions, including those from GK, ICA, ON and RySG, take issue with the proposed 6-month time frame to submit a claim under the ERTP noting that it would 'create uncertainty in the secondary market' as a transfer can be contested up to six months following an initial transfer which often happens after transfer of ownership of a domain name registration (GK), 'a period of uncertainty that is far too long' (ICA), 'such a window of opportunity (…) would introduce instability in the transfer process, and in Internet usability in general' (ON), and, 'a more appropriate time period would be 7 days' (RySG).

GK notes that in the current proposal there are no safeguards that would prevent 'seller remorse'. He proposes that if the ETRP would go ahead, there should be a 'secure and predictable procedure for the irrevocable transfer of a domain name to a legitimate buyer'. Under such an Irrevocable Transfer Procedure (ITP), 'the transfer can't be reversed by the ETRP, because the ETRP would not apply to transfers done using the ITP'. Under the ITP, additional authentication could be carried out by the registrar for a premium to determine that it concerns a legitimate transfer request. In his view, the best approach to address domain name hijacking is to 'raise the level of security at all registrars, e.g. two-factor authentication, executive lock, verified WHOIS, having a WHOIS history archived as the registry level'. He also calls for further data on the incidence of domain name hijacking. In his submissions, GK provides several examples of the potential undesired effects the ETRP in its current form could have on the secondary market. Furthermore, he highlights the importance of registrant education and implementation of recommendations that were made by the Security and Stability Advisory Committee in relation to preventing hijacking several years ago. In addition, GK provided a copy of all the emails he contributed to the IRTP Part B WG during his membership, which can also be reviewed here: http://forum.icann.org/lists/gnso-irtp-b-jun09/.

ES also argues that the WG should focus on tightening up 'security procedures to prevent thefts from happening in the first place', instead of pursuing the ETRP which would create 'an imbalance of power between buyer and seller'.

The Chair of the Security and Stability Advisory Committee (SC) congratulates the WG 'on its progress towards defining a process and specifying standard requirements for the urgent return/resolution of a domain name registration' and notes that the proposed policy 'is consistent with the principles outlined in section 4.2. of SSAC Report SAC007, Domain Name Hijacking Report'.

The RrSG opposes the ETRP noting that it is 'overly complex, lacks focus and is probably unworkable in its current form', at the same time pointing out that 'the existing Transfer Dispute Resolution Policy ("TDRP") is a lengthy process that often does not serve the best interests of registrants'.

ICA objects to the proposed ETRP noting that 'it could be extremely disruptive to the secondary domain marketplace to the detriment of both sellers and purchasers', pointing out the potential for abuse and lack of due process and an appeal mechanism. ICA notes that 'absent a far shorter window for a reversal's initiation, effective sanctions of abusive ETRP users, and clearly delineated due process rights for purchasers, this proposal should not move forward'.

The RySG considers resolution of these types of disputes at the registrar level the most effective, but notes that 'to the extend there is community support for the proposed ETRP (…), the RySG is agreeable to supporting the implementation of this policy'.

Charter Question B

ICA does not support 'changing current practice and adopting a rule that only a registrant, and not its administrative contact, can initiate a domain name transfer that does not modify contact information'.

The RySG notes that requiring 'thick' WHOIS could have as a potential side effect that registrant contact information is 'more readily available for individuals with nefarious intent to obtain access to the information as well'. The RySG is of the view that if a confirmation of the transfer by using the FOA would be 'implemented consistently among losing registrars, [it] could help reduce the number of instances when a transfer dispute arises because a transfer has been requested by the administrative contact without the knowledge or consent of the registrant'. The RySG furthermore recommends that 'registrars implement a consistent policy regarding the proof required to undo a domain name transfer'.

Charter Question C

In relation to the 60-day lock applied by some registrars following a change of registrant, GK raises the question 'whether some registrars use a creative interpretation of 'opt-in' to a process which registrants can't opt-out of'. In this regard, GK also questions the interpretation of the term 'voluntarily' by ICANN as it is being used in the transfer policy in denial reason #6 ('Express written objection to the transfer from the Transfer Contact. (e.g. – email, fax, paper document or other processes by which the Transfer

Contact has expressly and voluntarily objected through opt-in means)'. He notes that it is also important to 'be careful about how one defines a registrant, because the "label" one attached to a certain registrant might change, but it's not considered a change of registrant'.

The RrSG recommends that in relation to charter question b as well as c, a first step should be for the WG to develop a definition of the term "change of registrant" as 'it is an important precursor to settling disputes between Registrant and Admin Contact, as well as understanding what might need to happen when contact information is changed just before a transfer request'. The RrSG also recommends the WG to further explore 'the existing processes in place for trying to prevent hijacking attempts' as these could be serve as best practices to be recommended for adoption by registrars.

ICA and the RySG support the WG recommendation in relation to this issue.

Charter Question D

GK is of the opinion that 'the "ad hoc" locks that are violating of existing transfers policy need to be eliminated'. In his view 'registrars should be proactive about security, rather than misusing the locks'. In his view, there would be no need for a 60-day lock after a registrant change if there would be 'properly authenticated registrant changes'.

ICA has the view that any changes in relation to locking of a domain name subject to UDRP proceedings should be considered as part of a policy development process on review of the UDRP.

The RySG is of the view that the use of Registrar Lock Status 'should be left up to the individual registrars'.

Charter Question E

In relation to charter question d and e, the RrSG 'supports the right of registrars to employ locks as a security measure as long as the process for their removal remains consistent with ICANN policy'.

ICA is of the opinion that a clarification could be helpful but wishes 'to review comments received from registrars on the question of whether administrative considerations, including determination that the RNH request is bona fide and not fraudulent, allow for compliance within a five day period'.

The RySG is supportive of a modification, but proposes a modification to 'reflect current terminology'.

Working Group Review of Public Comments

The Working Group reviewed and discussed the public comments received using a public comment review tool that details the Working Group's responses to the public comment received and the actions taken as a result.

6.5 Public Comment on the Proposed Final Report

Seven (7) community submissions from seven (7) different parties were made to the public comment forum on the proposed Final Report. The contributors are listed below in alphabetical order (with relevant initials noted in parentheses):

- At-Large Advisory Committee by Olivier Crepin-Leblond (ALAC)
- Commercial & Business Users Constituency by Steve DelBianco (BC)
- GoDaddy.com by James Bladel (GD)
- gTLD Registries Stakeholder Group by David Maher (RySG)
- Internet Commerce Association by Philip Corwin (ICA)
- Internet Committee of the International Trademark Association by Claudio Di Gangi (INTA)
- Registrar Stakeholder Group by Clarke Walton (RrSG)

Summary & Analysis of the Comments received

General Comments

ALAC and RrSG express their general support for all the recommendations in the Report, in addition to some specific comments that can be found below.

Charter Question A / Recommendation #1

In relation to recommendation #1, the RrSG, RySG, INTA, BC and GD note their general support for the concept and intent of requiring a Transfer Emergency Action Contact (TEAC). The RySG notes that a longer response time (up to 72 hours) 'may be necessary to accommodate smaller registrars that are not staffed 24X7'. The RySG also raises the point to what extend registries should be involved in an TEAC, as in sponsored registries the registrant may be known and the registry may be able to assist. INTA expresses its support for the development of a policy to accompany the TEAC which 'takes into account criteria including immediacy of harm to the registrant, magnitude of the harm to third parties, and escalating impact, if the transfer is not reversed'. ICA notes that 'many important elements […] remain to be worked out' and recommends that these should be developed consistent with 'true emergency situations and not to cause substantial potential disruption to the secondary domain marketplace'. The RrSG recommends that the IRTP Part B WG remains responsible for the 'design and implementation of a proposed Emergency Action Channel'.

In the public comment forum, the WG asked a number of specific questions in relation to the ECA:

Within what timeframe should a response be received after an issue has been raised through the Transfer Emergency Action Contact (for example, 24 hours – 3 days has been the range discussed by the WG)?

The RySG response to this question ranges from 24 hours (more than half of the registries, 48 hours (one registry) to 72 hours (one registry). INTA and GD would support a response time of 24 hour maximum. ALAC and the BC support a 'short a period as practical' with ALAC noting that this should be well under 24 hours and the BC recommending 6-12 hours.

What qualifies as a response?

'Most members of the RySG feel that at a minimum, a positive confirmation of receipt and initial human contact is appropriate'. The BC also notes that a non-automated response would be preferable but 'would defer to registrars and registries in determining what qualifies as "a response" (email, phone call, fax, etc.)'. ICA noted that the different responses 'must be clearly delineated and mechanisms must be set in place to prevent abuse of the TEAC in non-emergency situations'.

Is an auto-response sufficient?

ALAC as well as most registries are of the view that an auto-response is not sufficient. In addition, the RySG notes that 'the goal of the TEAC should be to resolve the issue not to merely advise the receiving registrar that an issue exists'. INTA also agrees that an auto-response is not sufficient, but does support 'auto-responses during the process to keep the parties informed of the progress of the complaint'. GD suggests that 'ICANN Compliance test this channel periodically to ensure a non-automated response'.

Should there be any consequences when a response is not received within the required timeframe?

ALAC, INTA and the RySG agree that there should be consequences when a response is not received. The RySG notes that such consequences might follow defined escalation paths, including warnings and could even include termination of the accreditation by ICANN in case of multiple violations. INTA proposes that consequences could range 'from requiring specific remedial actions by the registrar, composing monetary fines, to imposing liability on the registrar'. ALAC suggests that 'consequences should include a provision for the registry unilaterally reversing the transfer and possible fines'. The RySG suggests that in the first year of implementation, 'consequences should be more lenient'. GD suggests that ICANN Compliance 'issue reports or warnings' in case registrars do not provide non-automated responses. ICA furthermore recommends that 'effective sanctions must be established against a domain seller who initiates an illicit reversal action'. The BC notes its response for modifying the IRTP 'to mandate a transfer-undo in cases where the gaining registrar does not respond in a timely way to an emergency-action request regarding a suspected domain name hijacking'.

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

Responses varied to this question in the RySG, but the RySG recommends 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'. INTA recommends that action should be taken by the registrant 'within three days of discovering the transfer'. INTA notes that 'if a time limit was set based on the transfer date, hijackers would likely take advantage of this by waiting to inflict harm until just after the time limit expired'. ICA notes that 'the time period in which a domain transfer reversal can be sought must be far shorter than six months post transfer'. Both the ALAC and BC would support a reasonably long window, with the BC suggesting a range of 60-180 days.

Which issues may be raised through the Transfer Emergency Action Contact?

Registry responses also varied to this question, but the RySG notes that 'the criteria detailed in the SSAC report would be a good starting point'. ICA is of the view that the TEAC should only be used for 'true crisis situations under a clear and narrow definition of "emergency" that is based upon current and reliable metrics of actual, non-hypothetical instances of abuses, including those arising from fraud and deception'. The RrSG also agrees that 'the nature of emergencies to be handled via such channel must be precisely defined'. The BC and ALAC note that the TEAC might also be useful for issues outside the scope of this PDP, and although not in scope for consideration by this WG, should not be precluded.

How/who should document the exchanges of information on the Transfer Emergency Action Contact?

The BC 'defers to registries and registrars when it comes to documenting successful exchanges' as well as 'how those unsuccessful exchanges are documented and communicated to the registry'.

Who is entitled to make use of the Transfer Emergency Action Contact?

Again, opinions vary in the RySG; some registries are of the opinion that it should 'only be available to the registrant', others are of the view that 'it should be limited to an authorized list of registrar and registry contacts' and 'approved contacts of recognized security and stability oriented groups'. The RySG notes that 'more analysis / discussion is warranted'. INTA is of the opinion that the TEAC may be used by

'aggrieved registrants to raise the issues of hijacking or erroneous transfers'. GD recommends that 'use be reserved for inter-registrar and ICANN-registrar communications, and only in situations where a timely response is critical'. The RrSG assumes the TEAC can only be used by registrars and/or ICANN, and notes it only supports the TEAC if communication is limited between those parties to serious and urgent domain name related emergencies. The BC notes that it 'does not envision that registrants' would have access to the ECA.

Charter Question A / Recommendation #2

The RySG notes that **'**most of the registries agree with this recommendation'. ALAC recognizes the importance of registrant education and notes that 'ALAC and At-Large may be considered one of the possible channels' for the implementation of this recommendation. The BC also notes its support for a proactive approach and offers its support for 'developing and promoting best practices in this area'.

Charter Question B – Recommendation #3

The RySG notes that 'all but one registry agreed with this recommendation'. The one registry that did not agree with this recommendation noted that 'ICANN staff and GNSO volunteers are overloaded at this time'. INTA expresses its support for this recommendation. GD recognizes the benefits of thick WHOIS in the context of transfers, but recommends that 'unintended consequences of requiring this change, particularly with large incumbent registries' should also be considered. ICA notes no objection to this recommendation. The BC also notes its support for this recommendation, but also suggest that an alternative approach that could be explored would be direct conversations with incumbent "thin" registries about a possible change to "thick" WHOIS.

Charter Question B – Recommendation #4

The RySG notes that 'all but one registry agreed with this recommendation'. The one registry that did not agree with this recommendation noted that 'ICANN staff and GNSO volunteers are overloaded at this time'. INTA, the BC and GD express support for this recommendation. ICA notes no objection to this recommendation

Charter Question B – Recommendation #5

The RySG notes that again 'all but one registry agreed with this recommendation'. The registry that did not agree pointed out that 'notification would be a good thing but only if the registrant is not held hostage by the losing registrar presenting misleading information'. GD similarly supports the recommendation as long as 'the transfer is not delayed or dependent upon any action on the part of the "losing" registrar'. The BC also expresses its support for this recommendation.

Charter Question C

The BC notes its support for 'requiring a lock after WHOIS information is updated when that update effects a change of registrant', in addition to 'prohibiting a transfer of a domain name registration for 60-days following a transfer, which is currently an option under reason of denial #9 in the IRTP'.

Charter Question C – Recommendation #6

The RySG notes that 'most registries agree with this recommendation', although one registry did point out that the term "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'. In addition, a registry recommended that 'the clarification needs to accommodate court orders'. INTA expresses its support for this recommendation, noting that 'it would help with both preventing fraudulent transfer and allowing legitimate owners to recover domain names and place them with their registrar of choice within an acceptable period'. INTA does request that an exception should be considered for registrations acquired as part of a successful UDRP since 'if a change of registrant occurs after a UDRP or equivalent action, it is very likely that the domain name is being transferred back to the rightful owner and no limitations should exist as to how long the rightful owner should be required to keep the domain at a particular registrar'. GD and the BC also note their support for this recommendation.

Charter Question D – Recommendation #7

The RySG expresses its support for this recommendation. ICA notes no objection to this recommendation. The BC expresses its support for this recommendation, noting that it 'would also

support elevating this recommendation from an optional "best practice" to a policy change that makes this kind of lock mandatory'. Furthermore the BC 'would also support proceeding with this change as part of this PDP'.

Charter Question D – Recommendation #8

All but one member of the RySG support this recommendation. The one registry member that disagrees noted that 'it must be done in accordance with any existing ICANN/registry agreement requirements'. The BC also expresses its support for this recommendation.

Charter Question E – Recommendation #9

The BC and the RySG express support this recommendation. ICA notes no objection to this recommendation.

Working Group Review of Public Comments

The Working Group reviewed and discussed the public comments received using a public comment review tool that details the Working Group's responses to the public comment received and the actions taken as a result.

7. Conclusions and Next Steps

Taking into account the Working Group Deliberations (see Chapter 5) and the Public Comments received (see Chapter 6), the Working Group would like to put forward the following recommendations for consideration by the GNSO Council to address each of the Charter Questions. All the recommendations listed below have full consensus support from the Working Group.

a. **Whether a process for urgent return/resolution of a domain name should be developed, as discussed within the 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 – The WG recommends requiring registrars to provide a Transfer Emergency Action Contact (TEAC). To this end the WG recommends to update the language of section 4 (Registrar Coordination) and Section 6 (Registry Requirements of the Inter-Registrar Transfer Policy as follows:

  Transfer Emergency Action Contact (Append to Section 4)

  Registrars will establish a Transfer Emergency Action Contact (TEAC) for urgent communications relating to transfers. The goal of the TEAC is to quickly establish a real-time conversation between registrars (in a language that both parties can understand) in an emergency. Further actions can then be taken towards a resolution, including initiating existing (or future) transfer dispute or undo processes.

  Communications to TEACs will be reserved for use by ICANN-Accredited Registrars, gTLD Registry Operators and ICANN Staff. The TEAC point of contact may be designated as a telephone number or some other real-time communication channel and will be recorded in, and protected by, the ICANN RADAR system.

Communications to a TEAC must be requested in a timely manner, within a reasonable period of time following the alleged unauthorized loss of a domain.

Messages sent via the TEAC communication channel must generate a non-automated response by a human representative of the gaining Registrar. The person or team responding must be capable and authorized to investigate and address urgent transfer issues. Responses are required within 4 hours of the initial request, although final resolution of the incident may take longer.

The losing registrar will report failures to respond to a TEAC communication to ICANN Compliance and the registry operator. Failure to respond to a TEAC communication may result in a transfer-undo in accordance with Section 6 of this policy and may also result in further action by ICANN, up to and including non-renewal or termination of accreditation.

Both parties will retain correspondence in written or electronic form of any TEAC communication requests and responses, and share copies of this documentation with ICANN and the registry operator upon request. This documentation will be retained in accordance with Section 3.4 of the Registrar Accreditation Agreement (RAA). Users of the TEAC communication channel should report non-responsive Registrars to ICANN. Additionally, ICANN may conduct periodic tests of the Registrar TEAC communication channel in situations and a manner deemed appropriate to ensure that registrars are indeed responding to TEAC messages.

(Append to Section 6) 6 iv. Documentation provided by the Registrar of Record prior to transfer that the Gaining Registrar has not responded to a message initiated via the TEAC communication channel within the timeframe specified in Section 4.

In addition, update section 6 to reflect that the registry, in case of a transfer undo, will reverse the transfer and reset the registrar of record filed to its original state ('In such case, the transfer will be reversed and the Registrar of Record field ~~domain name~~ reset to its original state').

Implementation Recommendations for Recommendation #1

- In the first phase of implementation, the WG recommends that the ICANN Registrar Application and Database Access Resource (RADAR) system is used to record the TEAC point of contact.
- In order to avoid potential abuse of the TEAC for non-emergency issues or claims that TEAC messages did not receive a timely response, the WG recommends that the RADAR system is adapted, as part of a second phase implementation, so that registrars log in to send or respond to an TEAC, with both transactions time stamped with copy to ICANN and the Registry.
- The Working Group recommends that the GNSO perform a follow-up review of the TEAC 12 to 24 months after the policy is implemented to identify any issues that may have arisen and propose modifications to address them. This review should specifically address whether the TEAC is working as intended (to establish contact between registrars in case of emergency), whether the TEAC is not abused (used for issues that are not considered an emergency) and whether the option to 'undo' a transfer in case of failure to respond to a TEAC should be made mandatory.

- **Recommendation #2** - The WG notes that in addition to reactive measures such as outlined in recommendation #1, proactive measures to prevent hijacking are of the utmost importance. As such, the WG strongly recommends the promotion by ALAC and other ICANN structures of the measures outlined in the recent report of the Security and Stability Advisory Committee on A Registrant's Guide to Protecting Domain Name Registration Accounts (SAC 044). In particular, the IRTP WG recommends that registrants consider the measures to protect domain registrar accounts against compromise and misuse described in SAC044, Section 5. These include practical measures that registrants can implement "in house", such as ways to protect account credentials and how to incorporate domain name registrations into employee or resource management programs typically found in medium and large businesses. It suggests ways that registrants can use renewal and change notifications from registrars as part of an early warning or alerting system for possible account compromise.

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** - The WG recommends requesting an Issues Report on the requirement of 'thick' WHOIS for all incumbent gTLDs. The benefit would be that in a thick registry one could develop a secure method for a gaining registrar to gain access to the registrant contact information. Currently there is no standard means for the secure exchange of registrant details in a thin registry. In this scenario, disputes between the registrant and admin contact could be reduced, as the registrant would become the ultimate approver of a transfer. Such an Issue Report and possible subsequent Policy Development Process should not only consider a possible requirement of 'thick' WHOIS for all incumbent gTLDs in the context of IRTP, but should also consider any other positive and/or negative effects that are likely to occur outside of IRTP that would need to be taken into account when deciding whether a requirement of 'thick' WHOIS for all incumbent gTLDs would be desirable or not.

- **Recommendation #4**: The WG notes that the primary function of IRTP is to permit Registered Name Holders to move registrations to the Registrar of their choice, with all contact information intact. The WG also notes that IRTP is widely used to affect a "change of control," moving the domain name to a new Registered Name Holder. The IRTP Part B WG recommends requesting an Issue Report to examine this issue, including an investigation of how this function is currently achieved, if there are any applicable models in the country-code name space that can be used as a best practice for the gTLD space, and any associated security concerns. The policy recommendations should include a review of locking procedures, as described in Reasons for Denial #8 and #9, with an aim to balance legitimate transfer activity and security. Recommendations should be made based on the data needs identified in the IRTP Part B workgroup discussions and should be brought to the community for public comment. The WG would like to strongly encourage the GNSO Council to include these issues (change of control and 60-day post-transfer lock) as part of the next IRTP PDP and ask the new working group to find ways to quantify their recommendations with data.

- **Recommendation #5**: 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. The Registrar of Record has access to the contact information for the Registrant

and could modify their systems to automatically send out the Standardized Form for Losing Registrars ("Confirmation FOA") to the Registrant.

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 in hijacking cases;**

- **Recommendation #6**: The WG does recognize that the current language of denial reason #6 is not clear and leaves room for interpretation especially in relation to the term 'voluntarily' and recommends therefore that this 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 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. The WG recommends to modify denial reason #6 as follows:

  Express objection to the transfer by the authorized Transfer Contact. Objection could take the form of specific request (either by paper or electronic means) by the authorized Transfer Contact to deny a particular transfer request, or a general objection to all transfer requests received by the Registrar, either temporarily or indefinitely. In all cases, the objection must be provided with the express and informed consent of the authorized Transfer Contact on an opt-in basis and upon request by the authorized Transfer Contact, the Registrar must remove the lock or provide a reasonably accessible method for the authorized Transfer Contact to remove the lock within five (5) calendar days.

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

- **Recommendation #7**: The WG recommends that 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.

- **Recommendation #8**: The WG recommends standardizing and clarifying WHOIS status messages regarding Registrar Lock status. The goal of these changes is to clarify why the Lock has been applied and how it can be changed. Based on discussions with technical experts, the WG does not expect that such a standardization and clarification of WHOIS status messages would require significant

investment or changes at the registry/registrar level. The WG recommends that ICANN staff is asked to develop an implementation plan for community consideration which ensures that a technically feasible approach is developed to implement this recommendation.

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**: 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. The WG recommends that ICANN staff is asked to develop an implementation plan for community consideration including proposed changes to the IRTP to reflect this recommendation.

Annex A – Background

1.1 Process background

- Consistent with ICANN's obligation to promote and encourage robust competition in the domain name space, the Inter-Registrar Transfer Policy (IRTP) aims to provide a straightforward procedure for domain name holders to transfer their names from one ICANN-accredited registrar to another should they wish to do so. The policy also provides standardized requirements for registrar handling of such transfer requests from domain name holders. The policy is an existing community consensus policy that was implemented in late 2004 and is now being reviewed by the GNSO.
- As part of that review, the GNSO Council formed a Transfers Working Group (TWG) to examine and recommend possible areas for improvements in the existing transfer policy. The TWG identified a broad list of over 20 potential areas for clarification and improvement (see http://www.icann.org/en/gnso/transfers-tf/report-12feb03.htm).
- The Council tasked a short term planning group to evaluate and prioritize the policy issues identified by the Transfers Working Group. In March 2008, the group delivered a report to the Council that suggested combining the consideration of related issues into five new PDPs (A – E) (see http://gnso.icann.org/drafts/transfer-wg-recommendations-pdp-groupings-19mar08.pdf).
- On 8 May 2008, the Council adopted the structuring of five additional inter-registrar transfers PDPs as suggested by the planning group (in addition to a recently concluded Transfer PDP 1 on four reasons for denying a transfer). It was decided that the five new PDPs would be addressed in a largely consecutive manner, with the possibility of overlap as resources would permit.
- The first PDP of the series of five, IRTP Part A PDP, was concluded in March 2009 with the publication of the final report.
- In its meeting on April 16 2009, the GNSO Council requested an Issues Report from Staff on the second of the PDP issue sets, and on the recommendation of the IRTP Part A WG, also added a number of issues from the third PDP issue set to this IRTP Part B. The Issues Report was delivered to the Council on 15 May 2009.
- The issues that IRTP Part B addresses are:

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

g. 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;

h. 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 in hijacking cases;

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

j. 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.

- The GNSO Council resolved at its meeting on 24 June 2009 to launch a PDP on these five issues and adopted a charter for a Working Group on 23 July 2009 (see Annex A for the Working Group Charter).

1.2 Issue Background (excerpt from Issues Report)

- Please note that the following text has been excerpted from the issues report and does not contain any new input from the Working Group.

Issue A: Urgent return/resolution of a domain name

Issue A: Whether a process for urgent return/resolution of a domain name should be developed, as discussed within the SSAC hijacking report (http://www.icann.org/announcements/hijacking-report-12jul05.pdf); see also http://www.icann.org/correspondence/cole-to-tonkin-14mar05.htm) (Issue #2).

In response to the ICANN request for public comments on the experiences with the Inter-Registrar Transfer, the Go Daddy Group noted that:

> "If a Registered Name Holder feels that a third party has illegally hijacked his or her domain name through a transfer, they may lodge a UDRP dispute. This complicates the issue since the registrars involved may be willing to work to correct the situation but now have their hands tied since they are obligated to lock down the domain name. This also conflicts with the TDRP, which should be the recommended and preferred method for a dispute regarding a transfer. It may be appropriate if the UDRP provider was required to refer the Registered Name Holder to the TDRP in cases that involve a transfer if that dispute mechanism has not already been tried, or to the registrars involved if they have not yet been consulted or yet allowed to work it out between themselves".

The Staff Report to the GNSO Council: Experiences with the Inter-Registrar Transfer Policy (14 April 2005) noted that "many of the comments related to security and the transfer process referred to a fraudulent transfer incident involving the domain name <panix.com>". In addition, in a section on transfer undo and fraud situations, it is stated that: "Although a transfer that has been determined to be fraudulent can be reversed by agreement between registrars, or by the registry using the Transfer-Undo mechanism, it has been suggested that such methods may not always allow sufficient responsiveness to fraud situations. The time period needed for adequate fact-finding and registrar coordination, or for the outcome of a fair dispute proceeding, may prolong problems including downtime, disruption of email services, or loss of business, especially if a domain name is one on which other services or financial services depend.

Suggestions on handling or reversing disputed transfers included:

(a) developing an expedited handling process for fraud situations;

(b) automatically returning names that are subject to a dispute to be returned to the original registrar until the dispute has been resolved;
(c) automatically rolling back the nameservers to [reflect the data contained therein] prior to the transfer.

It should be noted, however, that not every transfer that appears fraudulent may end up actually being a fraud case. Therefore, any measures should allow for flexibility in handling various outcomes." It is important to emphasize this last point as determinations of fraudulent activity must be made with caution and a number of questions would need to be addressed including; who has the authority to make such a determination and what qualifies an activity as fraudulent?

The SSAC report on Domain Name Hijacking: Incidents, threats risks and remedial actions (July 2005) recommends that "Registrars should identify evaluation criteria a registrant must provide to obtain immediate intervention and restoration of domain name registration information and DNS configuration. Registrars should define emergency procedures and policy based on these criteria. This policy would complement the Transfer Dispute Resolution Policy (TDRP) and must not undermine or conflict with those policies." The report notes that "The Inter-Registrar Transfer Policy incorporates formal dispute mechanisms (the Transfer Dispute Resolution Policy) intended for handling disputes between registrars associated with a transfer that cannot be solved directly between the two parties. These business-oriented processes are appropriate when the DNS information of a domain name is unaffected, when there is no issue of service denial or interruption, and when there is less immediate urgency to restore service. While the processes may be satisfactory for resolving a transfer-related dispute in a matter of days, another mechanism may be necessary to allow restoration of service in the timely manner real-time communications networks demand".

In relation to the current dispute resolution mechanisms, the report notes that "the UDRP is available for cases of abusive registrations or cybersquatting, particularly with regard to

trademarked names. A UDRP involves a cost of approximately USD $2,000, and takes at least two months to reach a decision.

The Transfer Dispute Resolution Policy (TDRP) is available to registrars to address disputes involving a transfer that has occurred. A TDRP dispute can be brought to the registry for a decision or to a third-party dispute resolution service provider. Both dispute resolution policies are designed to provide an impartial assessment of the factual circumstances of a case in order t[o] determine the appropriate outcome of a dispute. However, neither of these provides an immediate fix to cases of interrupted service or suspected hijacking".

Furthermore, the report states that "although registrars have worked together and agreed on a solution in several specific hijacking or fraud incidents, registrars may need a new communications channel and corresponding procedures to respond quickly to an operational loss of use of a domain name resulting from a transfer or DNS configuration error or hijacking. Possible elements of an urgent restoration of domain name registration information and DNS configuration include:

An emergency action channel – to provide 24 x 7 access to registrar technical support staff who are authorized to assess the situation, establish the magnitude and immediacy of harm, and take measures to restore registration records and DNS configuration to what is often described as "the last working configuration". An urgent restoration of a hijacked domain may require the coordinated efforts of geographically dispersed registrars, operating in different time zones. The emergency action channel requires a contact directory of parties who can be reached during non-business hours and weekends. It may be useful to make support staff contacts available online, so a third party is not required to maintain and distribute the contact details.

A companion policy to the emergency action channel – to identify evaluation criteria a registrant must provide to obtain immediate intervention (e.g., circumstances and evidence). From these, registrars can define emergency UNDO procedures. This policy would complement the TDRP and must not undermine or conflict with policies defined therein. The circumstances which distinguish when an urgent recovery policy may be a more appropriate action than the TDRP include:

2) Immediacy of the harm to the registrant if the transfer is not reversed (e.g., business interruption, security incidents).
3) Magnitude of the harm, or the extent to which the incident threatens the security and stability of parties other than the registrant, including but not limited to users, business partners, customers, and subscribers of a registrant's services.
4) Escalating impact, or the extent to which a delay in reversing the transfer (and DNS configuration) would cause more serious and widespread incidents.

The emergency action procedures should be tested to verify they are resilient to tampering and difficult to exploit. In particular, it should be difficult or impossible for an attacker to effect a hijack or interfere with a transfer under the guise of requesting urgent restoration of a domain. **A public awareness campaign** should be conducted to provide clear and unambiguous documentation that describes the policy and processes to registrars and registrants. This documentation should identify the criteria and the procedures registrants must follow to request intervention and immediate restoration."

Some of the questions that might need further consideration in a potential policy development process include determining the extent of the problem and whether it warrants a new policy or policy change; how to ensure that a process for urgent return does not interfere with the potential outcome of a dispute resolution process; who would be the ultimate decision-maker in such a process; and, which market solutions or best practices currently exist for dealing with this issue.

ICANN staff is aware that some registrars have dealt with the issue of urgent return of a domain name in the case of a suspected hijacking by indemnifying the gaining registrar, which appears to be a mechanism that ensures that the registrar of record will only pursue this avenue if it is absolutely sure that the domain name has been hijacked as it could otherwise incur substantial costs.

Issue B: Additional provisions for undoing inappropriate transfers

Issue B: Whether additional provisions on undoing inappropriate transfers are needed, especially with regard to disputes between a Registrant and Admin Contact (AC). The policy is clear that the Registrant can overrule the AC, but how this is implemented is currently at the discretion of the registrar (Issue #7).

In response to the ICANN request for public comments on the experiences with the Inter-Registrar Transfer, the Go Daddy Group submitted the following comment in relation to this issue:

"We have seen more than a few cases where the gaining registrar has received appropriate confirmation of a transfer request from the current Administrative Contact of record for the domain name. After the transfer completed, the Registered Name Holder of record at the time of the transfer claims that they did NOT approve the transfer and want it reversed. The Policy states that the Registered Name Holder's authority supersedes that of the Administrative Contact. Although the transfer was valid based on the current Policy the registrars are left to work together to reverse the transfer or face a formal dispute or legal action.

Is this the intent of the Policy? It opens up the potential for fraud, for example, in the event of a domain name sale and transfer. It also puts a burden on the registrar to attempt to verify the identity of the Registered Name Holder. Since most Whois records do not list the Registered Name Holder's email address, we need to rely on other documentation. However, given the international nature of our businesses, if we rely on photo identifications and business licenses from the Registered Name Holder we could easily be defrauded.

In addition, apparently due to the situation noted above, some registrars have adopted a hard copy transfer process centered on getting confirmation only from Registered Name Holders. This not only slows down the process for the Registered Name Holders, but puts registrars at increased risk and expense as they attempt to verify identification information from an international user base."

The Staff Report to the GNSO Council: Experiences with the Inter-Registrar Transfer Policy (14 April 2005) noted that "the policy provides that registry operators implement and make available a Transfer-Undo mechanism, to be used in cases where a transfer is determined to have been processed in contravention of the policy. This capability can be used either: a) when both registrars agree that a transfer should not have occurred and request the registry to reverse it, or b) as a result of a dispute proceeding which determines that a transfer should not

have occurred. The policy recommendations only required that registries develop such a mechanism. ICANN encouraged coordination among registries but determined that registries could be individually responsible for their own implementation of this mechanism".

In a document titled 'Review of Issues for Transfers Working Group' (19 January 2006), a working document developed by the Transfers Working Group, it is noted that "repatriation of inappropriately transferred names is difficult and processes are still unclear. This is mostly evident in incidences where a registrant has objected to a transfer despite the approval of the admin contact. The transfer policy is quite clear that the registrant 'trumps' the admin contact, but it is not clear how these types of veto situations should be handled. The result is an inconsistent application of policy and increased risk of domain theft." The document notes that potential next steps to be considered include a clarification, "restate intent of existing policy", as well as "additional policy provisions for handling inappropriate transfers".

In its Final Report, the IRTP Part A PDP Working Group recommended that "in the absence of a simple and secure solution for providing the gaining registrar access to the registrant email address, future IRTP working groups should consider the appropriateness of a policy change that would prevent a registrant from reversing a transfer after it has been completed and authorized by the admin contact. This option would not change the current situation whereby a losing registrar can choose to notify the registrant and provide an opportunity to cancel a transfer before the process is completed".

Issue C: Special provisions for a change of registrant near a change of registrar

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 in hijacking cases (Issue #9).

As stated in the description of the issue, a change of registrar near a change of registrant is a common feature in hijacking cases. In the opinion of Registrar.com as noted in one of the

comments submitted in response to the ICANN request for public comments on the experiences with the Inter-Registrar Transfer:

> "the Inter-Registrar Transfer Policy exposes losing registrars to an unacceptable level of liability when names are fraudulently transferred. Ultimately, the liability for a fraudulent transfer rests with the losing registrar since it has allowed a transfer-away to be processed while it is the current service provider for the registrant. The registrant will almost always look to the losing registrar in the event an unauthorized or fraudulent transfer is completed."

As a result, a number of registrars have taken preventative measures such as Go Daddy, which introduced a 60-day transfer prohibition period[11] following a change of registrant. However, some registrants seem to view such measures unnecessarily restrictive and not in compliance with the transfer policy, see e.g.:

> "GoDaddy has been treating a Registrant change as something major and is denying transfers for 60 days based on this [...] I wish ICANN puts a stop to all this ASAP." (From http://forum.icann.org/lists/transfer-comments-a/msg00012.html),

and

> "Also there are some registrars that in case of change of ownership, avoid ack transfers request send by other registrar, saying that "the domain registrant has recently changed". That is NOT one of the instances in which a transfer request may legitimately be denied by the Registrar of Record" (From http://forum.icann.org/lists/transfer-comments-g/msg00023.html).

ICANN issued an advisory in April 2008 to clarify that "a registrant change to Whois information is not a valid basis for denying a transfer request". It should be pointed out that Go Daddy since then has changed the "transfer prohibition period" to a voluntary opt-in provision that is offered to the registrant to prevent any transfers for 60 days after their domain name ownership change for security reasons. If a registrant has opted for this provision but still tries to transfer the domain name before the expiration of the 60 days, the transfer is denied under section A3(6) of the Inter-Registrar Transfer Policy (http://www.icann.org/en/transfers/policy-en.htm).

[11] From Go Daddy agreement: 'The domain name may not be transferred to another registrar within sixty (60) days of the completion of the change of Registrant transaction (the "Transfer Prohibition Period"). In the event the domain name is subject to another change of Registrant within the Transfer Prohibition Period, the 60-day Transfer Prohibition Period will begin again upon completion of the subsequent change of Registrant transaction'.

In a document titled 'Review of Issues for Transfers Working Group' (19 January 2006), a working document developed by the Transfers Working Group, it is stated that "transfers immediately following a Registrant transfer (change of ownership or license) should not be allowed, or at least the registrar should have the option of not allowing it for some period of time, 30-60 days perhaps. This was an explicit requirement in the old transfer policy, not sure why it was removed". Potential next steps referred to include "clarify intentions of existing policy related to how change of registrant fits into definitions in policy and whether [the] intent was to allow for Registrar implementation of special provisions needed for change of registrant simultaneous to transfer or within a period after transfer" and "possible PDP to create policy related to change of registrant".

Issue D: Standards or best practices regarding use of Registrar Lock Status

Issue D: Whether standards or best practices should be implemented regarding use of Registrar Lock status (e.g., when it may/may not, should/should not be applied) (Issue #5).

Registrar-Lock is described in RFC 2832 as:

> "REGISTRAR-LOCK: The registrar of the domain sets the domain to this status. The domain cannot be modified or deleted when in this status. The registrar MUST remove REGISTRAR-LOCK status to modify the domain. The domain can be renewed. The domain SHALL be included in the zone file when in this status".

Registrar-Lock does not refer to any internal flag or status termed 'lock' which a registrar may be using. As outlined in an ICANN Inter-Registrar Transfer Policy: Implementation Update "Registrars will […] be able to use "registrar-lock" to give registrants added assurance that their domains will not be transferred or modified without their consent, but only if the registrar provides a readily accessible and reasonable means for registrants to remove the lock if and when the registrant decides to transfer".

The Staff Report to the GNSO Council: Experiences with the Inter-Registrar Transfer Policy (14 April 2005) noted that "many comments raised issues concerning locking mechanisms which are currently used by registrars. Variations in the use of lock statuses and their variability across

registrars has added a level of complexity to the transfer process that in some cases has the effect of obstructing the desired ease of inter-registrar transfers. Additionally, such mechanisms impose a further burden on policy implementation because many registrants do not understand locking mechanisms. This is especially complicated in cases involving multiple languages". As a result, the report recommends considering "greater standardization of locking and unlocking functions or more precise definitions of appropriate use of the lock status".

In a document titled 'Review of Issues for Transfers Working Group' (19 January 2006), a working document developed by the Transfers Working Group, it is noted that "there seems to be ambiguity about what can be considered as registrar lock". Potential next steps mentioned include a clarification by defining registrar lock within the policy. In addition, the document notes that "best practices regarding registrar lock need to be drawn out from current practices. Standards may need to be set regarding when use of lock is appropriate and not appropriate".

Issue E: Clarification of denial reason #7

Issue E: Whether, and if so, how to best 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 from the IRTP Denials WG).

From the Issues Report on Specified Inter-Registrar Transfer Policy Issues:
"The current language (describing a reason for which a registrar of record may deny a transfer request) reads: 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. Referring to the Task Force's Report (http://www.icann.org/gnso/transfers-tf/report-exhd-12feb03.htm) for the intention behind the policy language, the following Q/A occurs:

9. "Some Registrars liberally employ the 'Registrar lock' function as it relates to the domain names they register for Registrants. This often means that Registrants *can't* transfer their

domain name in a predictable way. Do the Task Force recommendations consider this?"

A. Through extensive discussion within the Task Force and further consultation with the community after the Interim Report, the Task Force formed a minor series of amended recommendations that simply requires Registrars to provide Registrants with simple and transparent mechanisms by which Registrants can simply unlock or lock their domain name using accessible processes established by the Registrar.

Analysis: The Task Force heard this concern from several user groups. Earlier versions of this report contained substantially more stringent recommendations, however further discussion within the Task Force and outreach to various stakeholders within the DNSO only drew the lack of consensus on the older recommendations into focus. Accordingly the Task Force re-crafted its recommendations in order to support the principles that were supported by consensus.

In the current environment, registrar policies and practices vary with regard to means available to registrants for removing a Registrar Lock status. As a prerequisite to a registrar's denial of a transfer request for this reason, the policy requires that registrars provide a "readily accessible and reasonable means for the Registered Name Holder to remove the lock status." In staff's investigation of complaints about an inability to unlock a name, it is necessary to review the circumstances on a case by case basis, and apply an interpretation as to whether the registrar's practice is reasonable.

ICANN continues to receive complaints from registrants noting difficulty in unlocking names (see data from 2006 at http://www.icann.org/compliance/pie-problem-reports-2006.html).

ICANN could more efficiently enforce this provision if there were a test available for what is "reasonable or readily accessible." Adoption of a common test or standard would also facilitate

uniform enforcement of this provision[12].

In instances where a domain name is in Registrar Lock status, a transfer that is initiated by a potential gaining registrar will be automatically rejected at the registry level, without an explicit denial by the registrar of record. This makes it difficult for a registrar of record to comply with the requirement to provide the registrant and potential gaining registrar with the reason that the transfer was denied. It may be helpful for the policy language to reflect the process that occurs in the case of this type of denial."

Clarification of denial reason #7 was discussed in a previous PDP on Clarification of Denial Reasons, but the drafting group recommended dealing with this issue in conjunction with the question of standards or best practices regarding use of Registrar Lock Status which has been outlined in the previous section. The drafting group noted in its report the following concerns:

- "Discussions focused on clarification of the meaning of "readily accessible and reasonable means", but in the attempts to clarify this by comparison and by increased specificity potential undesired consequences were identified, see below
- The proposed texts raise deeper issues and more complexity than we are prepared to deal with within the scope and timeframe allotted to this drafting group
- We want to avoid a situation where registrars increase difficulty on contact/DNS changes in order to prevent transfers
- Some registrars have offered higher levels of security, and don't want to lose the flexibility of offering those add-on opt-in services
- The trade-off between security and convenience is one that must be made by registrants and this policy needs to provide the ability to make that choice
- Issue 5 under PDP C of the IRTP Issues PDP Recommendations of 19 March 2008 and the reason for wanting to clarify reason for denial number 7 are very closely related:
    - Issue 5 of PDP C on IRTP Operational Rule Enhancements states: "Whether standards

[12] As an example of such a test or standard, Section 5 of the policy includes the following in regard to provision of the authInfo code: "Registrars may not employ any mechanism for complying with a Registered Name Holder's request to remove the lock status that is more restrictive than the mechanisms used for changing any aspect of the Registered Name Holder's contact or name server information."

or best practices should be implemented regarding use of Registrar Lock status (e.g., when it may/may not, should/should not be applied). (CR 8.0)"

- The IRTP Policy Clarification of Reasons for Denial final report of 9 April 2008 says in the first sentence of the second paragraph on page 5: "Regarding "lock status", there is support for clarification, with a clear focus on the meaning of "readily accessible and reasonable means" for removing the lock."

As a result, the GNSO Council resolved 'that the work on denial reason #7 […] be suspended until such time as PDP C of the IRTP Issues PDP is initiated'.

Annex B - IRTP Part B PDP WG Charter

The Working Group shall consider the following questions as outlined in the issues report and make recommendations to the GNSO Council:

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

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

c) Whether special provisions are needed for a change of registrant when it occurs near the time of a change of registrar. The policy does not currently deal with change of registrant, which often figures in hijacking cases;

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

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.

To inform its work, the WG should pursue the availability of further information from ICANN compliance Staff to understand how elements of the existing Inter-Registrar Transfer Policy that are applicable to the above questions are enforced. The WG should also request compliance Staff to review any policy recommendations it develops and provide advice on how the recommendations may best be structured to ensure clarity and enforceability.

Working Group processes:

While the development of Guidelines for Working Group operations are still to be developed the guidelines at the following link will apply to this WG: working group process https://st.icann.org/gnso-council/index.cgi?24_june_09_motions

Milestones

WG formed, chair & Council liaison & staff coordinator identified = T

Initial Report: T + 170 days

First comment period ends: T + 190 days

Preliminary Final Report: T + 220 days.

Note: If the WG decides that a change is needed to the milestone dates, it should submit a revised time line to the GNSO council for approval

Annex C – TEAC FAQ

What is the TEAC and what is it for?

The Transfer Emergency Action Contact (TEAC) is a mechanism to facilitate urgent communications relating to transfers. The goal of the TEAC is to quickly establish real time communication between registrar representatives who can take steps to resolving the issue, but this policy only addresses establishing that communication not resolving any disputes that may arise.

What's the scope of the TEAC?

The TEAC only addresses the need to establish communications between registrars in emergency situations. The TEAC requirements outlined in this policy consciously exclude all aspects of resolving any disputes that may arise between parties in order not to disrupt processes that already exist to do that. The TEAC is limited to domain-transfer emergencies at this time, such as an unauthorized transfer following a hijacking, although other PDPs may expand this scope in the future.

What happens when the gaining registrar does not respond to a TEAC request?

The losing registrar may inform the registry that they have not received a response to their TEAC request after which the registry performs a "transfer-undo" in accordance with Section 6 of the existing IRTP.

How can a gaining Registrar eliminate the threat of a transfer undo?

The gaining registrar simply responds to the request. They do not need to return the domain, they do not need to resolve any disputes, they just need to respond to the TEAC request of the losing registrar and initiate communication between the two registrars. As soon as the gaining registrar responds to the losing registrar, the threat of transfer-undo vanishes. The whole aim of this policy is to get decision-makers talking to each other.

The policy requires a four-hour response time. Isn't that going to be hard for smaller registrars to cover, especially at night or on the weekends?

No. Even the smallest of registrars can simply rotate this function among operational staff, just as they rotate other "emergency" aspects of their business. The number of TEAC requests is likely to be very small and quite infrequent, but when they occur there is a genuine emergency that needs to be dealt with quickly.

Who can use the TEAC?

The TEAC is reserved for registrars, registries and ICANN staff.

Can the TEAC be used to initiate urgent, but not emergency, communications?

No, the TEAC is only for emergency communications relating to domain-transfer situations (primarily domain hijacking). It is not to be used for non-emergencies. It is not to be used for situations outside of domain transfers.

Can Registrants use the TEAC?

No, the TEAC is only available to registrars, registries and ICANN staff.

How is the TEAC protected from abuse by registrants or registrars that want to game the system or claw back a domain name?

The TEAC is not available to registrants, only their registrars so a registrant would need to request their registrar to start a TEAC. The TEAC only initiates communication, so as soon as the gaining registrar responds to the request, the TEAC request is fulfilled and the threat of transfer-undo is eliminated.

What is the definition of "emergency" in this context?

In order to qualify as a TEAC emergency, the issue has to be a serious, unexpected, time sensitive and harmful situation related to a domain-transfer.

What happens if a Registrar abuses the TEAC?

The same thing that happens if a registrar violates any ICANN consensus policy. This is a question that is outside the scope of the IRTP working group.

What escalation options does a Registrant have with regard to hijacking and where does the TEAC fit in?

The first, and best, source of help for a registrant whose domain has been hijacked is their registrar. The TEAC is aimed at helping that registrar quickly get in touch with the gaining registrar so that they can resolve the issue quickly (or quickly discover that there is a dispute that needs to be escalated to a higher level for resolution). In the event that the registrars cannot resolve the situation, the registrant can then move on to the other existing dispute-resolution processes (through the courts, ICANN Compliance and/or the Transfer Dispute Resolution Policy).

How long is the timeframe that the TEAC is available, after an incident or problem is identified?

This timeframe is consciously not defined, for several reasons. The primary reason is that by not specifying availability we avoid providing a roadmap for hijackers to time their activities. But another reason why this is not defined in the policy is the ease with which the threat of a transfer-undo can be avoided by the gaining registrar – they simply get in contact with the losing registrar and the requirements of the TEAC are fulfilled.

Annex D - Template for Constituency Statements

The GNSO Council has formed a Working Group of interested stakeholders and Constituency representatives, to collaborate broadly with knowledgeable individuals and organizations, in order to consider recommendations for a number of issues related to the Inter-Registrar Transfer Policy (IRTP).

Part of the working group's effort will be to incorporate ideas and suggestions gathered from Constituencies through this Constituency Statement. Inserting your Constituency's response in this form will make it much easier for the Working Group to summarize the Constituency responses. This information is helpful to the community in understanding the points of view of various stakeholders. However, you should feel free to add any information you deem important to inform the working group's deliberations, even if this does not fit into any of the questions listed below.

For further background information on this issue, please review the GNSO Issues Report on IRTP Part B.

Process

- Please identify the members of your constituency who participated in developing the perspective(s) set forth below.
- Please describe the process by which your constituency arrived at the perspective(s) set forth below.

Questions

Please provide your constituency's views on:

a) 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);

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

registrar;

c) Whether special provisions are needed for a change of registrant when it occurs near the time of a change of registrar. The policy does not currently deal with change of registrant, which often figures in hijacking cases;

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

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.

Annex E – Charter Question B – Standard Use Cases

Registrant	Admin Contact	Description	Comment
Company Ltd	**Employee ex-employee**	Company director (providing company documentation demonstrating his authority and personal documentation demonstrating identity) claims authority over admin contact requests return to original registrar (and changes to record)	Within scope. Original registrar talks to new registrar or ERTP evoked.
Company Ltd	**Director A**	Company director B claiming higher authority	How can registrar make judgemnet?
Company Ltd	**Service Provider (WG definition) Webmaster or other third party**	Company director (providing company documentation demonstrating his authority and personal documentation demonstrating identity) claims authority over admin contact requests return to original registrar (and changes to record)	Within scope. Original registrar talks to new registrar or ERTP evoked.
Marketing Name (non legal entity)	**An individual**	Another individual tries to demonstrate authority within the non legal entity (by showing name on marketing material.	How can registrar be sure? Is it correct to allow such loose registrant names?
Family Member A	**Family member B, parent of minor,**	Family member C tries to demonstrate authority.	Registrar only takes authority from Registrant or Admin Contact.
Service Provider Proxy name service or Webmaster or other third party	**Any individual from service provider**	"Owner" claims or demonstrates equity authority and requests return to original registrar	Registrar only takes authority from Registrant or Admin Contact. This is classic case outside ICANN or policy. Case of incorrect registration is not

			considered fraud?.
Service Provider Proxy name service or Webmaster or other third party	**Any individual from service provider**	"Owner" claims or demonstrates that registrant WHOIS has changes and he was previous registrant.	Change of registrant to a service provider could be fraud?
Registrant A	**Individual B**	Registrar Account holder C	Registrar only takes authority from Registrant or Admin Contact.

ANNEX F - EPP Status Codes: What do they mean, and why should I know?

Extensible Provisioning Protocol (EPP) domain status codes, also called domain name status codes, indicate the status of a domain name registration. Every domain has at least one status code, but they can also have more than one.

Is your domain name registration about to be dropped? Is it safely locked to prevent unauthorized transfers, updates or deletions? Does it have any restrictions or pending actions that you need to address? Finding and understanding your domain's EPP status codes will answer all of these questions and more.

It is important for registrants (that means you!) to understand EPP status codes because they can explain why your domain may have stopped working, if it is protected from domain name hijacking, and when and if your domain name registration will expire and become available to the public for registration.

You can find out your domain's status codes by running a Whois lookup, which you can do by visiting http://www.internic.net/whois.html or your registrar's website. Your domain's EPP status codes will be included in the search results.

There are two different types of EPP status codes: **client** and **server** codes. Client status codes are set by registrars. Some registrars automatically enact certain status codes when you register a domain name, while others do so when you request it. Server status codes are set by registries, and they take precedence over client codes. Both kinds of status codes appear when you run a Whois lookup for your domain.

The following are two tables containing the 17 official EPP domain status codes. The first table lists the server status codes; the second table lists the client status codes. These tables will explain what each status means, why you should care what it means, and what kind of action you might want to take to respond to a status.

Server Status Codes are Set by Your Domain's Registry

Status Code	What does it mean?	Should you do something?
OK	This is the standard status for a domain, meaning it has no holds or restrictions.	Asking your registrar to enact status restrictions, like clientTransferProhibited, clientDeleteProhibited, and clientUpdateProhibited, can help to prevent unauthorized transfers, deletions, or updates to your domain.
serverTransferProhibited	This status code prevents your domain from being transferred from your current registrar to another. It is an uncommon status that is usually enacted during legal or other disputes, at your request, or when a redemptionPeriod status is in place.	This status may indicate an issue with your domain that needs to be addressed promptly. You should contact your registrar to request more information and resolve the issue. If your domain does not have any issues, and you simply want to transfer it to another registrar, you must first contact your registrar and request that they work with the Registry Operator to remove this status code. Alternatively, some Registry Operators offer a Registry Lock Service that allows registrants, thought their registrars to set this status as an extra protection against unauthorized transfers. Removing this status can take longer than it does for clientTransferProhibited because your registrar has to forward your request to your domain's registry and wait for them to lift the restriction.
serverRenewProhibited	This status code indicates your domain's Registry Operator will not allow your registrar to renew your domain. It is an uncommon status that is usually enacted during legal disputes or when your	Often, this status indicates an issue with your domain that needs to be addressed promptly. You should contact your registrar to request more information and resolve the issue. If your domain does not have any issues, and you simply want to renew it, you must first contact your registrar and request that they work with

	domain is subject to deletion.	the Registry Operator to remove this status code. This process can take longer than it does for clientRenewProhibited because your registrar has to forward your request to your domain's registry and wait for them to lift the restriction.
pendingTransfer	This status code indicates that a request to transfer your domain to a new registrar has been received and is being processed.	If you did not request to transfer your domain, you should contact your registrar immediately to request that they deny the transfer request on your behalf.
pendingUpdate	This status code indicates that a request to update your domain has been received and is being processed.	If you did not request to update your domain, you should contact your registrar immediately to resolve the issue.
pendingRenew	This status code indicates that a request to renew your domain has been received and is being processed.	If you did not request to renew your domain and do not want to keep it (i.e., pay the renewal fee) anymore, you should contact your registrar immediately to discuss what options are available.
pendingCreate	This status code indicates that a request to create your domain has been received and is being processed.	If you are NOT the listed Registrant, you should contact your registrar immediately to resolve the issue. If your domain has remained in this status for several days, you may want to contact your registrar to request information about the delay in processing.
inactive	This status code indicates that delegation information (DNS or name servers) has not been associated with your domain. Your domain is not included in the zone file and will not resolve.	This status may indicate an issue with your domain that needs resolution. If so, you should contact your registrar to request more information. If your domain does not have any issues, but you need it to resolve, you must first contact your registrar and request that they work with the Registry Operator to include the missing information and remove this status code.
serverHold	This status code is set by your domain's Registry Operator. Your domain is not included in the zone file and will not resolve. It is an uncommon status that is usually enacted during legal	Often, this status indicates an issue with your domain that needs resolution. If so, you should contact your registrar to request more information. If your domain does not have any issues, but you need it to resolve, you must first contact your registrar and request that they work with

	disputes or when your domain is subject to deletion.	the Registry Operator to remove this status code. This process can take longer than it does for clientHold because your registrar has to forward your request to your domain's registry and wait for them to lift the restriction.
serverDeleteProhibited	This status code prevents your domain from being deleted. It is an uncommon status that is usually enacted during legal disputes, at your request, or when a redemptionPeriod status is in place.	This status may indicate an issue with your domain that needs resolution. If so, you should contact your registrar to request more information and to resolve the issue. If your domain does not have any issues, and you simply want to delete it, you must first contact your registrar and request that they work with the Registry Operator to remove this status code. Alternatively, some Registry Operators offer a Registry Lock Service that allows registrants, thought their registrars to set this status as an extra protection against unauthorized deletions. Removing this status can take longer than it does for clientDeleteProhibited because your registrar has to forward your request to your domain's registry and wait for them to lift the restriction.
serverUpdateProhibited	This status code locks your domain preventing it from being updated. It is an uncommon status that is usually enacted during legal disputes, at your request, or when a redemptionPeriod status is in place.	This status may indicate an issue with your domain that needs resolution. If so, you should contact your registrar for more information or to resolve the issue. If your domain does not have any issues, and you simply want to update it, you must first contact your registrar and request that they work with the Registry Operator to remove this status code. Alternatively, some Registry Operators offer a Registry Lock Service that allows registrants, thought their registrars to set this status as an extra protection against unauthorized updates. Removing this status can take longer than it does for clientUpdateProhibited because your registrar has to forward your request to your domain's registry and wait for them to lift the restriction.

addPeriod	This grace period is provided after the initial registration of a domain name. If the registrar deletes the domain name during this period, the registry provides a credit to the registrar for the cost of the registration.	This is an informative status set for the first 5 days or your domain's registration. There is no issue with your domain name.
autoRenewPeriod	This grace period is provided after a domain name registration period expires and is extended (renewed) automatically by the registry. If the registrar deletes the domain name during this period, the registry provides a credit to the registrar for the cost of the renewal.	This is an informative status set for the first 5 days or your domain's auto-renewal by the registry. If you did not request to renew your domain and do not want to keep it (i.e., pay the renewal fee) anymore, you should contact your registrar immediately to discuss what options are available.
renewPeriod	This grace period is provided after a domain name registration period is explicitly extended (renewed) by the registrar. If the registrar deletes the domain name during this period, the registry provides a credit to the registrar for the cost of the renewal.	This is an informative status set for the first 5 days or your domain's renewal by your registrar. If you did not request to renew your domain and do not want to keep it (i.e., pay the renewal fee) anymore, you should contact your registrar immediately to discuss what options are available.
transferPeriod	This grace period is provided after the successful transfer of a domain name from one registrar to another. If the new registrar deletes the domain name during this period, the registry provides a credit to the registrar for the cost of the transfer.	This is an informative status set for the first 5 days or your domain's transfer to a new registrar. If you did not request to transfer your domain, you should contact your original registrar.
redemptionPeriod	This status code indicates that your registrar has asked the registry to delete your domain. Your domain will be held in this status for a maximum of 30 days. After	If you want to keep your domain, you must immediately contact your registrar to resolve whatever issues resulted in your registrar requesting that your domain be deleted, which resulted in the redemptionPeriod status for your domain.

	then, it will be updated with the pendingDelete status for five calendar days after which time, your domain is purged from the registry database and becomes available for anyone to register on a first come, first served basis.	Once any outstanding issues are resolved and for the appropriate fee has been paid, your registrar should restore the domain on your behalf.
pendingRestore	This status code indicates that your registrar has asked the registry to restore your domain that was in redemptionPeriod status. Your registry will hold the domain in this status while waiting for your registrar to provide required restoration documentation. If your registrar fails to provide documentation to the Registry Operator within seven calendar days to confirm the restoration request, the domain will revert to redemptionPeriod status.	Watch your domain's status codes within this seven-day period to ensure that your registrar has submitted the correct restoration documentation within the seven-day time window. If seven days pass and your domain has reverted back to a redemptionPeriod status, contact your registrar to resolve whatever issues that may have halted the delivery of your domain's required restoration documentation.
pendingDelete	This status code is automatically set after your domain has been in redemptionPeriod status AND if you have not restored it within that maximum 30-day period. Your domain will remain in the pendingDelete status for five calendar days, after which time your domain will be purged and dropped from the registry database. Once deletion occurs, the domain is available for anyone to register on a first come, first served basis.	If you want to keep your domain name, you must immediately contact your registrar to discuss what options are available.

Client Status Codes are Set by Your Domain's Registrar

Status Code	What does it mean?	Should you do something?
clientTransferProhibited	This status code tells your domain's registry to reject requests to transfer the domain from your current registrar to another.	This status indicates that it is not possible to transfer the domain name registration, which will help prevent unauthorized transfers resulting from hijacking and/or fraud. If you do want to transfer your domain, you must first contact your registrar and request that they remove this status code.
clientRenewProhibited	This status code tells your domain's registry to reject requests to renew your domain. It is an uncommon status that is usually enacted during legal disputes or when your domain is subject to deletion.	Often, this status indicates an issue with your domain that needs resolution. If so, you should contact your registrar to resolve the issue. If your domain does not have any issues, and you simply want to renew it, you must first contact your registrar and request that they remove this status code.
clientHold	This status code tells your domain's registry to not include your domain in the zone file and as a consequence, it will not resolve. It is an uncommon status that is usually enacted during legal disputes, non-payment, or when your domain is subject to deletion.	Often, this status indicates an issue with your domain that needs resolution. If so, you should contact your registrar to resolve the issue. If your domain does not have any issues, but you need it to resolve, you must first contact your registrar and request that they remove this status code.
clientDeleteProhibited	This status code tells your domain's registry to reject requests to delete the domain.	This status indicates that it is not possible to delete the domain name registration, which can prevent unauthorized deletions resulting from hijacking and/or fraud. If you do want to delete your domain, you must first contact your registrar and

		request that they remove this status code.
clientUpdateProhibited	This status code tells your domain's registry to reject requests to update the domain.	This domain name status indicates that it is not possible to update the domain, which can help prevent unauthorized updates resulting from fraud. If you do want to update your domain, you must first contact your registrar and request that they remove this status code.