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

STATUS OF THIS DOCUMENT

This is the Initial Report on IRTP Part B PDP, prepared by ICANN staff for submission to the GNSO Council on 29 May 1020. A Final Report will be prepared by ICANN staff following public comment.

SUMMARY

This report is submitted to the GNSO Council and posted for public comment as a required step in this GNSO Policy Development Process on Inter-Registrar Transfer Policy.

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.

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.
- Chapter 5 provides an overview of the deliberations of the Working Group conducted both by conference call as well as e-mail threads. It should be noted that the Working Group will not make a final decision on which solution(s), if any, to recommend to the GNSO Council before a thorough review of the comments received during the public comment period on the Initial Report.

1.3 Preliminary Conclusions of the Working Group

- **Preliminary Conclusion for Issue A**

  The WG recognizes the need for a process for the urgent return / resolution of a domain name registration and would like to put forward an 'Expedited Transfer Reverse Policy' (ETRP) for community consideration. The ETRP should be seen as an escalation process that can be invoked by the registrar of record if the situation cannot be resolved amicably, with registrar co-operation still being the preferred avenue for resolving disputes. The main elements of the proposed ETRP are as follows:

  - The ETRP will be mandatory for all gTLD Registries and Registrars that are subject to IRTP.
  - Registrants claiming to be victims of a hijack must work through their original sponsoring Registrar (i.e., the PTRa), as they possess all necessary pre-transfer information.
  - The ETRP must be initiated within 60 days of the completion of a transfer under the IRTP
  - The PTRa must obtain an ETRP authorization from the Registrant to initiate the ETRP. An ETRP Authorization from any of the other contacts noted in the associated WHOIS records, including the Administrative Contact, is not eligible for ETRP.
  - Elements of the ETRP Authorization should include:

    - An authorization from the pre-transfer Registrant, affirming or declaring that the transfer was unauthorized, and that they desire to restore the registration to its pre-transfer state, and that the PTRa is initiating the ETRP on their behalf;
    - Documentation that the PTRa has verified the identity of the pre-transfer registrant in a manner conforming to local law and practices;
    - Indemnification of the PTRa and Registry Operator by the pre-transfer Registrant;
    - These materials, along with any supporting documentation, will be bundled into an "ETRP packet"
- The PTRa may, at their discretion, charge the Registrant a fee for these services. Any registrar that operates a website for domain registration or renewal must state, both at the time of registration and in a clear place on its website, any additional fee charged for the recovery of a domain name via ETRP. Upon receipt of a valid ETRP Packet, the Registry Operator for the Top Level Domain of the name in dispute ("Registry") will, within their best reasonable efforts not to exceed 48 hours, restore the domain name to its pre-transfer state. This will include:
    - Reinstating in the Registry database the PTRa as the Registrar of Record.
    - Notifying the PTRa that the transfer was reversed via ETRP;
    - Refunding the original transfer transaction fee charged to the gaining Registrar, if any;
    - Assessing any ETRP processing fee, not to exceed the then current TDRP processing fee to the PTRa;
    - Maintaining the domain name expiration as extended by one year (not to exceed the maximum registration term) when the original transfer was processed.
- The ETRP is intended to correct fraudulent or erroneous transfers, not to address or resolve disputes arising over domain control or use.
- Upon notice from the PTRa, the gaining Registrar will, within their best reasonable efforts not to exceed 48 hours, notify the post-transfer registrant of the ETRP transfer reversal.
- The WG agrees that there should be a mechanism to dispute an ETRP but has not reached agreement on how such a mechanism might work. The WG hopes to receive further input during the public comment period on the elements an ETRP dispute

mechanism should contain and whether it should be an integral part of the ETRP or another existing dispute resolution mechanism e.g. the TDRP.

- Minority viewpoint – one member of the WG supported adding the following provision to section 3.1 of the proposed ETRP: The PTRa shall distribute a Registrant's Title to each Registrant in a communication directly to the Registrant without notice to any of the other contacts noted in the associated WHOIS records, including the Administrative Contact. Such a Registrant's Title shall include a unique identifier as determined by the Registrar for the purpose of providing the Registrant with a mechanism for identification as the Registrant.

Members of the ICANN Community are encouraged to provide their feedback on the proposed ETRP, including the timeframes currently proposed.

The complete language of the proposed ETRP can be found in Annex C.

- **Preliminary Conclusion for Issue B**

  The WG is considering a recommendation to request an Issues Report on the requirement of 'thick' Whois for all 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 means for the secure exchange of registrant details in a thin registry. In this scenario, disputes between the registrant and admin contact could be avoided, as the registrant would become the ultimate approver of a transfer. The WG is interested to receive input from the community on why it should or why it should not consider this recommendation for a PDP to require 'thick' Whois for all gTLDs.

  The WG notes that the IRTP is widely used to effect a change of "control" over a given registration, as opposed to simply moving the registration to a new sponsoring registrar with all contacts unchanged. While the IRTP lists both the registrant and the admin contact as authorized "transfer contacts" to change registrars, the change of control function is not defined. Therefore, the WG recommends that only the registrant can effect a change of control, while both the registrant and admin contact remain eligible to authorize a transfer that does not modify any contact information. This could be achieved by either (a) restricting the admin contact's ability to modify any contact information associated with the domain name, or (b) ensuring that any transfer reversal or change of control features are explicitly limited for use by the registrant only. The WG seeks input from the community on this proposed recommendation.

- **Preliminary Conclusion for Issue C**

  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-Daddys solution 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.

  Therefore the WG concludes that whilst it recognises the symptom of this question as one of several indicators, there is no plausible outcome that would make any change effective for the purpose.

- **Preliminary Conclusions Issue D**

  The WG is considering recommending 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.

The WG is considering a recommendation to standardize and clarify 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.

- **Preliminary Conclusions Issue E**

  The WG is considering recommending the following modification of 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.

1.4 Stakeholder Group / Constituency Statements & 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.
- A 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.
- Chapter 6 features an overview of the issues reflected in the statements from the GNSO stakeholder groups / constituencies and comments received during the public comment period.

1.5 Conclusions and Next Steps

- The Working Group aims to complete this section of the report in the second phase of the PDP, following a second public comment period.

2. Objective and Next Steps

This Initial Report on the Inter-Registrar Transfer Policy (IRTP) Part B PDP is prepared as required by the GNSO Policy Development Process as stated in the ICANN Bylaws, Annex A (see http://www.icann.org/general/bylaws.htm#AnnexA). The Initial Report will be posted for public comment for 20 days. The comments received will be analyzed and used for redrafting of the Initial Report into a Final Report to be considered by the GNSO Council for further action.

3. Background

3.1 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:
  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 A for the Working Group Charter).

3.2 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:

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

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[1] 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).

[1] 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'.

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).

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[2].
>
> 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:

[2] 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."

- “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 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’.

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
James Bladel	RrSG	24
Eric Brown	RySG	6
Berry Cobb	CBUC	23
Michael Collins	Individual	20
Chris Chaplow	CBUC	23
Graham Chynoweth	RrSG	2
Paul Diaz	RrSG	25
Kevin Erdman	IPC	21
Anil George	IPC	20
Mark Klein	RrSG	0
Matt Mansell[3]	RrSG	3
Bob Mountain[4]	RrSG	3
Michele Neylon (WG Chair)	RrSG	24
Mike O'Connor	CBUC	23
Mike Rodenbaugh	CBUC	1
Tim Ruiz (Council Liaison)	RrSG	6
Boudouin Schombe	NCUC	8

[3] Joined the WG on 22 March 2010

[4] Joined the WG on 30 April 2010

Matt Serlin	RrSG	15
Barbara Steele	RySG	20
Rudi van Snick	At Large	3
Miriam Trudell	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

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. It should be noted that the Working Group will not make a final decision on which solution(s), if any, to recommend to the GNSO Council before a thorough review of the comments received during the public comment period on the Initial Report.

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 (see further details below).

Preliminary Conclusion for Issue A

The WG recognizes the need for a process for the urgent return / resolution of a domain name registration and would like to put forward an 'Expedited Transfer Reverse Policy' (ETRP) for community consideration. The ETRP should be seen as an escalation process that can be invoked by the former registrar of record if the situation cannot be resolved amicably, with registrar co-operation still being the preferred avenue for resolving disputes. The main elements of the proposed ETRP are as follows:

- The ETRP will be mandatory for all gTLD Registries and Registrars that are subject to IRTP.
- Registrants claiming to be victims of a hijack must work through their original sponsoring Registrar (the "PTRa"), as they possess all necessary pre-transfer information.
- The ETRP must be initiated within 60 days of the completion of a transfer under the IRTP.
- The PTRa must obtain an ETRP authorization from the Registrant to initiate the ETRP. An ETRP Authorization from any of the other contacts noted in the associated WHOIS records, including the Administrative Contact, is not eligible for ETRP.
- Elements of the ETRP Authorization should include:
    - An authorization from the pre-transfer Registrant, affirming or declaring that the transfer was unauthorized, and that they desire to restore the registration to its pre-transfer state, and that the PTRa is initiating the ETRP on their behalf;
    - Documentation that the PTRa has verified the identity of the pre-transfer registrant in a manner conforming to local law and practices;
    - Indemnification of the PTRa and Registry Operator by the pre-transfer Registrant;
    - These materials, along with any supporting documentation, will be bundled into an "ETRP packet"
- The PTRa may, at their discretion, charge the Registrant a fee for these services. Any registrar that operates a website for domain registration or renewal must state, both at the

time of registration and in a clear place on its website, any additional fee charged for the recovery of a domain name via ETRP. Upon receipt of a valid ETRP Packet, the Registry Operator for the Top Level Domain of the name in dispute ("Registry") will, within their best reasonable efforts not to exceed 48 hours, restore the domain name to its pre-transfer state. This will include:

  - Reinstating in the Registry database the PTRa as the Registrar of Record.
  - Notifying the PTRa that the transfer was reversed via ETRP;
  - Refunding the original transfer transaction fee charged to the gaining Registrar, if any;
  - Assessing any ETRP processing fee, not to exceed the then current TDRP processing fee, to the PTRa;
  - Maintaining the domain name expiration as extended by one year (not to exceed the maximum registration term) when the original transfer was processed.

- The ETRP is intended to correct fraudulent or erroneous transfers, not to address or resolve disputes arising over domain control or use.
- Upon notice from the PTRa, the gaining Registrar will, within their best reasonable efforts not to exceed 48 hours, notify the post-transfer registrant of the ETRP transfer reversal.
- The WG agrees that there should be a mechanism to dispute an ETRP but has not reached agreement on how such a mechanism might work. The WG hopes to receive further input during the public comment period on the elements an ETRP dispute mechanism should contain and whether it should be an integral part of the ETRP or another existing dispute resolution mechanism e.g. the TDRP.
- Minority viewpoint – one member of the WG supported adding the following provision to section 3.1 of the proposed ETRP: The PTRa shall distribute a Registrant's Title to each Registrant in a communication directly to the Registrant without notice to any of the other contacts noted in the associated WHOIS records, including the Administrative Contact. Such a Registrant's Title shall include a unique identifier as determined by the Registrar for the purpose of providing the Registrant with a mechanism for identification as the Registrant.

Members of the ICANN Community are encouraged to provide their feedback on the proposed ETRP, including the timeframes currently proposed.

The complete language of the proposed ETRP can be found in Annex C.

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'[5] 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, as the registrant email address would be public. It was pointed out that the current proposals in the new gTLD process require all new gTLD registries to run a 'thick[6]' 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.

[5] 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.

[6] Thick Whois output includes a broader set of data elements including contact information for the registrant and designated administrative and technical contacts.

Preliminary Conclusion for Issue B

The WG is considering a recommendation to request an Issues Report on the requirement of 'thick' Whois for all 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 means for the secure exchange of registrant details in a thin registry. In this scenario, disputes between the registrant and admin contact could be avoided, as the registrant would become the ultimate approver of a transfer. The WG is interested to receive input from the community on why it should or why it should not consider this recommendation for a PDP to require 'thick' Whois for all gTLDs.

The WG notes that the IRTP is widely used to effect a change of "control" over a given registration, as opposed to simply moving the registration to a new sponsoring registrar with all contacts unchanged. While the IRTP lists both the registrant and the admin contact as authorized "transfer contacts" to change registrars, the change of control function is not defined. Therefore, the WG recommends that only the registrant can effect a change of control, while both the registrant and admin contact remain eligible to authorize a transfer that does not modify any contact information. This could be achieved by either (a) restricting the admin contact's ability to modify any contact information associated with the domain name, or (b) ensuring that any transfer reversal or change of control features are explicitly limited for use by the registrant only. The WG seeks input from the community on this proposed recommendation.

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. Currently some registrars do allow for unlocking when appropriate credentials are provided, while others do not.

- 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.

Preliminary Conclusion for Issue C

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 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.

Therefore the WG concludes that whilst it recognises the symptom of this question as one of several indicators, there is no plausible outcome that would make any change effective for the purpose.

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 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.

Preliminary Conclusions Issue D

The WG is considering recommending 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.

The WG is considering a recommendation to standardize and clarify 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.

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.

Preliminary Conclusions Issue E

The WG is considering recommending the following modification of 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 WG seeks input of the community on this proposed modification.

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 Period

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.

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.

7. Conclusions and Next Steps

The Working Group aims to complete this section of the report in the second phase of the PDP, following a public comment period on this Initial Report.

Annex A – 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 B – 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 C – Expedited Transfer Reverse Policy (ETRP)

1. Objective

1.1 This document describes a policy recommendation for the timely, cost-effective reversal of an Inter-Registrar domain name transfer, restoring the registration to its pre-transfer state.

1.2 This policy recommendation is intended to augment, rather than replace, existing policy and services currently in use. These include the Transfer Dispute Resolution Procedure (TDRP), various Registry-specific reassignment services, and ad hoc Registrar cooperation.

2. Background

2.1 The Inter-Registrar Transfer Policy (IRTP) aims to provide a straightforward procedure for a domain name holder (i.e. the duly contracted entity with registration rights to the domain name, hereafter referred to as the "Registrant") 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 the Registrant. The policy is an existing GNSO consensus policy that was implemented in late 2004.

2.2 In its current form, the IRTP represents a vulnerability to the unauthorized transfer of a domain name to a new Registrar. This is commonly referred to as domain name "hijacking."

2.3 Hijacking results in significant harms to Registrants, and undermines public trust in the domain name system.

2.4 In their efforts to detect and remedy incidents of hijacking, Registrars will employ a variety of tools, including the TDRP, Registry-specific reassignment services, and informally cooperating with other Registrars to reverse a recent transfer.

2.5 No single method provides a general procedure to address hijacked domain names, however, as they are perceived as expensive, slow, and requiring the cooperation of multiple parties.

2.6 The IRTP-B PDP working group has produced this draft policy recommendation to address the need for an urgent return mechanism.

3. Procedure

3.1 The Expedited Transfer Reverse Policy (ETRP) will be mandatory for all gTLD Registries and Registrars that are subject to the IRTP. Registrants claiming to be victims of a hijack must work through their original sponsoring Registrar, as they possess all necessary pre-transfer information including the Registrant's Title. Throughout the remainder of this document, the original sponsoring registrar is termed the Pre-Transfer Registrar (PTRa).

> *Minority viewpoint – one member of the WG supported adding the following provision to section 3.1 of the proposed ETRP:*
> *The PTRa shall distribute a Registrant's Title to each Registrant in a communication directly to the Registrant without notice to any of the other contacts noted in the associated WHOIS records, including the Administrative Contact. Such a Registrant's Title shall include a unique identifier as determined by the Registrar for the purpose of providing the Registrant with a mechanism for identification as the Registrant.*

3.2 ETRP must be initiated by the PTRa within 60 days of the completion of an Inter-Registrar domain name transfer, corresponding to the 60-day Transfer Lock / Reason For Denial period that is implemented by most Registries and Registrars, or within 60 days of the Registrant becoming aware of the transfer (but in no event more than six (6) months after the Inter-Registrar domain name transfer).

> 3.2.1 While widely implemented by many Registrars, this Transfer Lock is currently described as "optional" in the existing IRTP. We recommend that this practice be required, to guard against serial transfers following an initial unauthorized transfer.

3.3 PTRa must obtain an ETRP Authorization from the Registrant to initiate a ETRP. ETRP Authorization from any of the other contacts noted in the associated WHOIS records, including the Administrative Contact, is not eligible for ETRP.

3.4 Staff is asked to develop, in collaboration with the Working Group, an appropriate ETRP Authorization. Elements of the ETRP Authorization should include:

3.4.1 An Authorization from the pre-transfer Registrant, affirming or declaring that the transfer was unauthorized, and that they desire to restore the registration to its pre- transfer status, and that the PTRa is initiating the ETRP on their behalf. If the ETRP is initiated outside of the 60-day Transfer Lock period, the Registrant must additionally provide an explanation of when and how the Registrant became aware of the transfer.

3.4.2 Documentation that the PTRa has verified the identity of the pre-transfer Registrant by including information on the Registrant Title.

3.4.3 Indemnification of the PTRa and Registry Operator by the pre-transfer Registrant.

3.4.4. These materials, along with any supporting documentation, will be bundled into an "ETRP Packet".

3.5 PTRa may, at their discretion, charge the Registrant a fee for these services. Any Registrar that operates a website for domain registration or renewal must state, both at the time of registration and in a clear place on its website, any additional fee charged for the recovery of a domain name via ETRP.

3.6 Upon receipt of a valid ETRP Packet, the Registry Operator for the Top Level Domain of the name in dispute (“Registry”) will, within their best reasonable efforts not to exceed 48 hours:

3.6.1. Restore the domain name to its pre- transfer stateby reinstating in the Registry database the PTRa as the Registrar of Record.

3.6.2 Notify the PTRa that the transfer was reversed via ETRP, using the appropriate "urgent" communication method (email, poll message, etc.)

3.6.3 Refund the original transfer transaction fee charged to the gaining Registrar, if any.

3,6.4Assess an ETRP transaction fee, not to exceed the then current TDRP processing fee, to the PTRa.

3.6.5Retain the then effective expiration date of the domain name to ensure that the name does not expire or enter any grace periods.

3.7 Upon notice from the PTRa, the gaining Registrar will, within their best reasonable efforts not to exceed 48 hours, notify the post-transfer registrant of the ETRP transfer reversal.

4. Restrictions

4.1 The ETRP may -not- be used for transfers that:

4.1.1 Are the result of implementing a UDRP decision, or for names subject to UDRP complaints in which a decision is pending.

4.1.2 Are part of a bulk transfer.

4.1.3 Are part of an ICANN-sponsored reallocation associated with the termination or non-renewal of a Registrar Accreditation.

4.1.4 Are involved in pending litigation.

4.2 PTRa must deny future transfer requests for a period of 60 days following a successful ETRP.

4.3 ETRP is intended to correct fraudulent or erroneous transfers, not to address or resolve disputes arising over domain control or use. In these scenarios, the appropriate remedies include, but are not limited to, one or more of the following:

4.3.1 Registry-Specific reassignment service

4.3.2 Uniform Dispute Resolution Policy (UDRP)

4.3.3 Court of competent jurisdiction

4.4 PTRa may block ETRP use in cases of repeated hijack claims, abuse of the procedure, or in suspected cases of "reverse hijacking," and refer the Registrant to alternative mechanisms (Sec. 4.3) where appropriate.

5. Disputed ETRP Claim

[The WG agrees that there should be a mechanism to dispute an ETRP but has not reached agreement on how such a mechanism might work. The WG hopes to receive further input during the public comment period on the elements an ETRP dispute mechanism should contain and whether it should be an integral part of the ETRP or another existing dispute resolution mechanism e.g. the TDRP.]

6. Role of ICANN

6.1 ICANN shall engage in community outreach to build awareness of the ETRP among Registrars and Registrants.

6.2 ICANN Compliance shall collect and investigate complaints of Registrars who employ the ETRP in bad faith, or are unresponsive to Registrant claims of domain hijacking.

6.3 ICANN may include reporting of ETRP use as a component of Registry Monthly Reports, but in no event shall the reporting requirements be more extensive than those currently required under the TDRP.

.