



## Staff Report to GNSO Council: Experiences with Inter-Registrar Transfer Policy

14 April 2005

### Background

The [Inter-Registrar Transfer Policy](#) was created through ICANN's consensus-based, bottom-up policy development process and approved unanimously by both ICANN's Generic Names Supporting Organization (GNSO) and its Board of Directors. After consultation between ICANN staff and registry operators, registrars, and other knowledgeable parties, the policy went into effect on 12 November 2004. Beginning four months prior to the implementation date, all accredited registrars and unsponsored gTLD registry operators were notified of the implementation date, provided with copies of the policy, and reminded of their contractual obligations to comply with policies adopted through the consensus process.

The policy provides for enhanced domain name portability, resulting in greater consumer and business choice and enabling domain name registrants to select the registrar that offers the best services and price. The policy is designed to simplify and standardize the process, prevent abuses, and provide clear user information about the transfer process and options.

In order to provide strong protections against unauthorized transfers and to facilitate choice in domain name registration, all registrars are required to use a clear standardized form of authorization (FOA) that provides for the express consent of the domain name registrant prior to the initiation of any registrar transfer.

Additionally, the policy:

- Requires registrars to verify the identity of the registrant or administrative contact requesting the transfer by one of a number of approved methods to deter fraud;
- Preserves the ability of registrants to "lock" their domains so they may not be transferred from the registrar, but requiring registrars to provide a readily accessible way for registrants to have their current registrar remove this lock at their request;
- Enables registrants to transfer their domain names without having to "double-confirm" the transfer once the transfer has been reliably authenticated per the policy; and
- Provides a robust dispute resolution process for resolving disputes between registrars, including a registry "transfer undo" functionality to provide for efficiently reversing any transfer initiated in violation of the policy.

Consistent with the [policy recommendations](#) of the GNSO Council's Transfers Task Force, this report to the Council describes:

- i. How effectively and to what extent the policies have been implemented and adopted by Registrars, Registries and Registrants,
- ii. Whether or not modifications to these policies should be considered as a result of the experiences gained during the implementation and monitoring stages,
- iii. The effectiveness of the dispute resolution processes and a summary of the filings that have been resolved through the process.

This report is the first of the series and is presented to the GNSO Council in order to provide information on the early stages after implementation, and identify potential issues and problems that may remain to be addressed.

In preparing this report, ICANN staff has drawn on several sources of information, including: (i) public comments submitted during a three-week period, (ii) statistics provided in the registry operators' quarterly reports, and (iii) questions and complaints received by ICANN staff members individually. The complete archive of public comments received is posted and available at <http://www.icann.org/announcements/announcement-12jan05.htm>.

## **Policy Effectiveness and Suggested Considerations**

The following paragraphs describe key components of the Inter-Registrar Transfer Policy and issues that have developed concerning each area.

### **A. Standardized Forms of Authorization**

The policy requires that specific standardized Forms of Authorization, or FOAs, be used by registrars to [obtain](#) or [confirm](#) a registrant's intent to transfer a domain to a new registrar. The forms may not be modified or combined with any other information. The purpose of this requirement is to provide for clear, verifiable and uniform communications for all registrars, thus avoiding registrant confusion.

The FOA must be sent in at least English, and optionally in other languages.

#### *Transfer Contacts*

The policy provides that the FOA must be sent to either the Registrant or the Administrative Contact as shown in the Whois. These are the only parties who can legitimately authorize a transfer.

ICANN is aware of instances in which a registrar (or reseller) has listed itself in the Administrative Contact field, then in the case of a transfer request, does not respond to the FOA sent by the gaining registrar, thus defeating potential transfers. Under such circumstances, the Registrant can ask the potential gaining registrar to send the FOA to him/her and thereby start the process; however, Registrants frequently are not aware of this. Although the policy clearly states that it is the Registrant's intent that must prevail,

it has been noted that there could be more explicit guidelines for how conflicts between the Registrant and Administrative Contact should be handled.

### *Content of the FOAs*

Suggestions received by ICANN for improving the content of the FOAs included:

- a) the form should not be quite so standardized, but instead there could be a few mandatory elements;
- b) registrars should be able to choose freely how to perform registrant authorizations and confirmations, in order to distinguish themselves in the market;
- c) the FOA should be adaptable for special cases (for example, a registrant transfer occurring simultaneously with a registrar transfer, or performing different forms of identity validation for corporate clients);
- d) display of the full contact information for the domain name within the form would be helpful.

### *Security and the FOAs*

Suggestions received for improving the security of the process include:

- a) adding an individualized authorization code to the FOA;
- b) sending the FOA to both the Registrant and Admin Contact instead of one or the other;
- c) instituting a two-step confirmation process;
- d) instituting a capability for a temporary unlock mechanism (“soft/sticky unlock”) which would allow a transfer only to a specified registrar, within a specified time window;
- e) restricting registrant changes or instituting further confirmation procedures immediately following a transfer; and
- f) increasing/decreasing the time period of 5 days allowed for the losing registrar to reject the transfer.

In cases of spoofing, compromised account access, or other types of fraud, a gaining registrar may have complied with the policy and obtained an FOA from the right email address, but still have unknowingly initiated a fraudulent transaction. Such transactions were a problem prior to the implementation of the policy as well. Appropriate mechanisms for rolling back a transfer that has been determined to be fraudulent are provided by the Transfer Undo mechanism (section D below).

Many of the comments received relating to security and the transfer process referred to a fraudulent transfer incident involving the domain name <panix.com>, registered to an ISP located in New York. A brief review of this incident is contained in a separate section, below. A case study is also being undertaken by ICANN’s Security and Stability Advisory Committee (SSAC).

### *Summary*

Although the FOA requirements have brought about some of the desired improvements to the inter-registrar transfer process, it has not eliminated all potential problems. Although some problems continue to occur due to “bad actors” in the community and instances of noncompliance with various measures of the policy, many of these same problems and abuses could and did occur before the implementation of the policy. Staff experiences do not lead to a conclusion that “the old way was better.” Rather, staff recommends consideration by the GNSO of the following issues:

- Determining the efficacy of authorization/authentication for preventing security breaches.
- Providing greater latitude in content of the FOAs while still achieving the goals of accuracy and standardization.
- Improving the language of the FOA for clarity, and modifying it to fit special situations.
- Providing further development or clarification of the requirements regarding appropriate transfer contacts.

## **B. Dispute Resolution Processes**

The [Transfer Dispute Resolution Policy](#) incorporates mechanisms for resolution of disputes between registrars over alleged violations of the policy. Dispute proceedings may be initiated with the relevant registry operator or with an independent third-party [dispute resolution service provider](#).

Only a small number of disputes have been reported at the registry level, and none have been submitted to third-party dispute resolution service providers. While ICANN has received reports of satisfaction with the process and outcome of first-level disputes, in most cases registrars have opted to bring suspected registrar violations to the attention of ICANN instead of initiating a dispute under the policy.

While ICANN staff has been able to resolve a number of end customer complaints by working with registrars directly, substantial resources have been required to bring this about. Substantial staff time has been spent in researching the background information on individual transfer complaints, establishing contact with nonresponsive registrars, addressing compliance issues with registrars, or correcting misinformation that had been provided to customers by registrars. After this introductory period, ICANN has more actively directed parties with disputes to the dispute resolution options, while education on the policy has been ongoing. ICANN has also noted a gradual decrease in complaints after the first three months.

The dispute resolution process was intended to be a strong reinforcement to the policy. The registrar that is determined to have violated the policy is the one required to pay the fees for a dispute. A registrar that habitually violates the policy will be penalized for noncompliance through repeated payment of dispute resolution fees.

Although some registrars expressed strong concerns leading up to the implementation date that there might not be dispute resolution mechanisms readily in place, it appears that registrars have not yet fully availed themselves of this option. Many complaints have been voiced by registrars regarding other registrars allegedly violating the policy.

However, by and large, registrars have not taken full advantage of the means available to them for taking action.

#### *Access to Dispute Resolution Information and Services*

Some comments received on this topic requested that ICANN make information on dispute resolution services freely available, and that fees, providers, and decisions should be posted. Although links to dispute resolution providers are included in the transfer information area at <http://www.icann.org>, it may be helpful to issue a follow-up communication in this area.

Additionally, it appears that registrants sometimes file a UDRP complaint if they believe their domain has been hijacked by way of a transfer. Further education in the community on the most effective channels for resolving transfer complaints would also be useful.

Also, some registrars have indicated that it may be beneficial to consider making the dispute resolution process something that is directly accessible to registrants as an option for pursuing their complaints. Given that the process at the registry level is designed to be efficient and low-cost, this may be a practical option, and would help avoid situations in which a registrant is stuck when a registrar does not choose to pursue a dispute on his/her behalf against an alleged violating registrar.

#### *Summary*

Although there are reported instances of registrar violations that act to prevent transfers, the dispute resolution process has not yet been fully utilized as envisioned. ICANN staff recommends to the GNSO consideration of the following:

- Opening up the TDRP process to registrants to allow for better access to problem-solving

### **C. Grounds for Denying Transfer Requests**

The policy includes a list of 9 instances in which a transfer request may legitimately be denied by the Registrar of Record, as follows:

1. Evidence of fraud
2. UDRP action
3. Court order by a court of competent jurisdiction
4. Reasonable dispute over the identity of the Registered Name Holder or Administrative Contact
5. No payment for previous registration period (including credit card charge-backs) if the domain name is past its expiration date or for previous or current registration periods if the domain name has not yet expired. In all such cases, however, the domain name must be put into "Registrar Hold" status by the Registrar of Record prior to the denial of transfer.
6. Express written objection to the transfer from the Transfer Contact. (e.g. - email, fax, paper document or other processes by which the Transfer Contact has expressly and voluntarily objected through opt-in means)

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.
8. A domain name is in the first 60 days of an initial registration period.
9. 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).

An explicit list of allowable reasons for denial of a registrar transfer request is a key part of the policy. Problems relating to this list seem to center around ambiguities that allow registrars to interpret the reasons in different ways. Examples include:

- a) Lack of clarity about what can be considered as valid evidence of fraud (#1);
- b) Lack of clarity about what can be considered a reasonable dispute over identity of the registrant (#4);

[One way of encouraging further consistency in these definitions could be to include a “test of reasonableness” such as is included in the section of the policy dealing with the AuthInfo codes: “Registrars may not employ any mechanism for complying with a Registered Name Holder’s request to obtain the applicable “AuthInfo Code” that is more restrictive than the mechanisms used for changing any aspect of the Registered Name Holder’s contact or name server information.”]

- c) Lack of clarity about the definition of Lock status (#7). Registrars may unlock a domain only for an unreasonably short time and lock it again before a transfer takes place. Additionally, registrars may interpret the term “Lock status” to also include an internal or local “lock” mechanism which does not show up in the Whois record as a Registrar-Lock status, but is still used by the registrar to deny a transfer request;
- d) Lack of clarity about the definition of “initial registration period” (#8). This term can be interpreted to be only the 60 days after a party registers a domain name that was previously unregistered, or, alternatively, a new initial registration period triggered by a new registrant;
- e) Questions regarding denying transfers because they are within 60 days of a previous transfer (#9). This can be problematic because it may not always be possible for the registrar to tell whether a transfer has occurred in this time period. Also, there is nothing in the policy that *requires* registrars to deny transfer requests for this reason, but they *may* deny an incoming request for this reason should they choose to do so. ICANN has received a few complaints from registrants that the 60 day period was too long, when they had legitimately bought or taken over a previously-transferred domain name, but could not move it to their registrar of choice for nearly two months following the transaction. (Note that the policy says that a lesser period can be determined.).

### Summary

There do not appear to be major problems stemming from the list of valid transfer denial reasons that would recommend revision of the list. However, there can be improvement

in the clarification and definition of terms in the list, as described above. ICANN staff recommends consideration by the GNSO of the following:

- Inclusion of more precise guidelines in the policy in order to clarify terms and reduce confusion.
- Requirement, modification or elimination of the 60 day post-transfer period.

#### **D. Transfer Undo Mechanism**

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.

The [approach agreed on by the registries](#) was that a Transfer Undo mechanism would only undo the Registrar of Record change(s). No changes would occur to the expiration dates or registry transfer fees.

##### *Efficiency of the Transfer Undo Process*

Some comments indicated that the registry tool for reversing a transfer was inefficient and could take several days to complete even when registrars had agreed on the request. Suggestions included:

- a) putting a time limit on the response from the registry, in order to avoid unnecessary delays and inconvenience to the original domain name holder;
- b) providing a more precise definition for the Transfer-Undo mechanism at the protocol level;
- c) clarifying specifications regarding the payment of fees involved in the transfer and the effects of transfer and reversal on a domain name's expiration date.

The final description document developed by the registries regarding the Transfer Undo mechanism also stated:

It is recognized that this approach to a transfer undo mechanism could have lost revenue impact on registrars who have the registration returned to them. At least one year would have been added to the registration period and possibly multiple years if additional transfers or explicit renewals occurred and they would not have received any fees for the additional year(s).

...Moreover, it seems to be an issue that primarily impacts registrars and hence is one best worked by registrars. Therefore, since registrars believe that the issue of lost revenue impact is one for which a plan should be developed, registrars plan to pursue this separately from the initial implementation of the new registrar transfer policy. If they are successful in devising a plan that they can implement in time for the introduction of the new transfer policy, that would be fine. If they are not, any plan developed subsequently could be considered as part of the ongoing evaluation of the transfer policy.

ICANN would encourage continuing efforts by registrars to work with registries on these issues.

#### *Transfer Undo and Fraud Situations*

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 transactions 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 what they had been 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.

#### *Summary*

With regard to the Transfer-Undo mechanism and other measures for reversing transfers, ICANN recommends that the GNSO consider the following:

- Effectiveness of the current registry Transfer-Undo provisions.
- Sufficiency of the current Transfer-Undo provisions combined with the dispute resolution provisions as responses for situations involving fraud.

#### **E. Records**

The policy provides that registrars maintain copies of the forms of authorization and related documentation, and make these available upon request by the other registrar that is party to a transfer transaction, ICANN, the registry operator, a court or authority with jurisdiction over the matter, or a third party dispute resolution panel.



According to the policy, both registrars must be able to provide the evidence relied on for the transfer during and after the applicable inter-registrar transaction(s). Such information must be provided within 5 days when requested by any of the above parties.

Also, the Gaining Registrar must retain, and produce pursuant to a request by a Registrar of Record, a written or electronic copy of the FOA used for obtaining the registrant's intent to transfer. The Gaining Registrar must fulfill such a production request by a registrar within 5 calendar days. Failure to provide this documentation within the time period specified is grounds for reversal by the Registry Operator or the Dispute Resolution Panel in the event that a transfer complaint is filed in accordance with the requirements of this policy.

Cases have been reported to ICANN of registrars exercising their right to view the other registrar's documentation on every transfer request, creating an administrative burden on the other end. While a registrar cannot deny a transfer request because it does not receive such documentation from the gaining registrar, some have then taken the fact that the gaining registrar has not produced a valid FOA and used it to deny a transfer request, citing this as evidence of fraud. A proposed modification to the policy would allow a registrar to deny a transfer request if a requested confirmation from the gaining registrar is not responded to in the allowable time frame.

Finally, the policy provides that upon denying a transfer request for any reason, the registrar of record *must provide the registered name holder and the potential gaining registrar with the reason for denial*. In a number of cases which have been investigated by staff, it appears that many registrars are not currently providing this notification to one or both parties.

### *Summary*

With regard to the policy requirements relating to records, ICANN recommends that the GNSO consider:

- Further clarification or limitation with regard to appropriate use of a registrar's right to inspect the other's records.
- Addition to the list of allowable reasons for denying a transfer request: a gaining registrar's failure to provide evidence of authorization when requested to do so.

## **F. EPP – AuthInfo**

For domain names in EPP-based registries (.biz, .info, .name, .org, and .pro), registrars are required to provide registrants with a unique Auth-Info code, for purposes of validating the identity of the registrant. Registrars are required to provide this code to registrants within 5 days of a request.

An issue then is, in the cases of EPP registries, whether the Auth-Info code itself provides an adequate measure of security, and whether there would be any legitimate reason for a registrar to deny a transfer request if the potential gaining registrar had the Auth-Info code. Some comments also questioned whether the 5-day pending period was necessary when the Auth-Info code was being used.

Additionally, registrars have indicated that it can often be difficult for domain name holders to obtain AuthInfo codes from their existing registrar. Provisions exist in the policy requiring registrars to release this code to a name holder upon request; however, procedures for doing this vary across registrars. Along this same line, it has been proposed that registrants be permitted to obtain this code from the registry directly via a request on the registry website. Clearly there is a need for greater understanding in the community about management and use of the AuthInfo codes.

Existing policy clearly states that a registrar must provide the Registered Name Holder with the unique AuthInfo code for a domain name within 5 days of a request. ICANN has received very few complaints about registrars not releasing the AuthInfo code.

### *Summary*

The Auth-Info code is intended to help automate the authentication steps followed by registrars. ICANN recommends that the GNSO consider the following:

- Sufficiency of the AuthInfo code as an authentication tool in EPP registries.
- Further standardization with regard to procedures for communicating the AuthInfo code.

## **G. Other Issues**

### *Locking Mechanisms*

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.

Some comments suggested an opt-in means for higher security levels for high-profile domains. As a matter of policy, any service standard established for “high-profile” domains should also be available to any individual domain name holder.

### *Registrar Impact*

Successful implementation of the policy has required substantial effort on the part of ICANN’s accredited registrars, including modification of policies and publications, updating procedures, and time spent on internal and external education and problem-solving.

Aspects of the policy continue to represent a resource cost for registrars: disparity between registries (RRP versus EPP); disparity of Whois formats among 400+ registrars; limited access to Whois data; some common situations requiring some steps be carried out manually by the registrar (such as determining the actual registrant when a proxy shows in the Whois due to a privacy service offering). Because the Whois environment and the transfer policy implementation itself continue to evolve, registrars

are reluctant to invest in long-term systems or upgrades that could help automate the process.

Additionally, several registrars voiced concern over their potential liability as a Registrar of Record, stemming from the policy's requirement that they allow a domain transfer to go through without any knowledge of what process has been followed on the other end. It should be noted, however, that registrars are explicitly allowed to deny a transfer request if they have evidence of fraud. Some greater clarity surrounding these circumstances should be considered (discussed in section C, above).

### *Communications*

The transfer policy states that each registrar should establish and maintain a unique and private email address for use only by other registrars and the applicable registry, that is to be dedicated to inter-registrar transfer issues. Messages received at this address must be answered within 7 calendar days.

ICANN has not publicized these addresses, but maintains a registry of the email contacts and has periodically sent out confidential lists and updates to registries and registrars. In cases where a separate email address had not been set up, ICANN listed the registrars' public contact email, giving the option to change it to a specified email address for transfers. ICANN has received some complaints about contact information not being up to date, or lack of response from some registrars.

ICANN cannot now effectively follow up with registrars on this from a compliance standpoint. Such an email address is not a clear requirement in the policy. If a registrar does have such an email address; however, they are obligated to monitor it and respond within the stated time frame.

### *Fees*

ICANN has received several questions regarding the charging of fees involved in the transfer process. There is nothing in the policy which prevents a registrar from charging a fee to the registrant, and ICANN has received complaints concerning substantial fees being charged. However, it should be noted that when a transfer request is initiated by the gaining registrar, nonpayment of a transfer fee is not a valid reason for denial of the request by the Registrar of Record

### *Expiration Issues*

When a domain name registration expires, there is a 45-day auto-renewal grace period available to the registrar. ICANN has received a number of complaints from domain holders whose names are past the expiration date but within this period. Many registrars have told these customers that they must pay for a renewal of the domain before they can allow a transfer.

Expiration or nonrenewal of a domain registration is not currently a valid reason for denial of a transfer request.

### *Summary of Other Issues*

ICANN recommends that the GNSO consider the following:

- Greater standardization of locking and unlocking functions or more precise definitions of appropriate use of the lock status.
- Implementation and standardization of measures to make the transfer process easier to automate.
- Requiring a dedicated transfer email address for each registrar, with a required response time.
- Inclusion of explicit policy provisions regarding expired domain names.

## Conclusion

The policy as it currently exists strives to ease the process associated with legitimate transfer requests while continuing to provide strong protections for domain name holders against fraud. The requirements for periodic ongoing reviews of this policy area indicate an awareness that the implementation may need to be adjusted as conditions, practices, and standards evolve.

In reviewing the early experiences, ICANN concludes that a number of positive steps have been accomplished through implementation of the Inter-Registrar Transfer Policy. One key step is the availability of dispute resolution mechanisms and a clear basis for settling disputes over registrar transfers, which was not possible previously. It is hoped that over time these mechanisms will be more widely used and tested. Additionally, the policy contains significant contractual provisions allowing for enforcement. ICANN has taken a lead role in policy enforcement. Finally, the existence of an enumerated list of valid reasons for denial of a transfer has cut down on the capacity for registrars to make their own rules for registered name holders in order to prevent transfers out.

In this report ICANN has also described the key areas in which changes to the implementation may be considered. Some issues may result in changes in policy or small clarifications, while in some areas the parties involved may work out best practices.

ICANN will continue to maintain its [transfer-questions@icann.org](mailto:transfer-questions@icann.org) mailbox and respond to inquiries, and interface with registrars to ensure comprehensive understanding and compliance with the policy. ICANN will also devote further resources to formal logging and analysis of all complaints, so that staff resources can be directed to investigation of specific or frequent forms of complaints. In most cases, ICANN will attempt to refer complainants back to the registrars to better utilize existing dispute resolution procedures.

It is also evident that ongoing education and information regarding the transfer process is required. Answers to frequently-asked questions have been posted at <http://www.icann.org/transfers> and will continue to be updated periodically based on common questions.

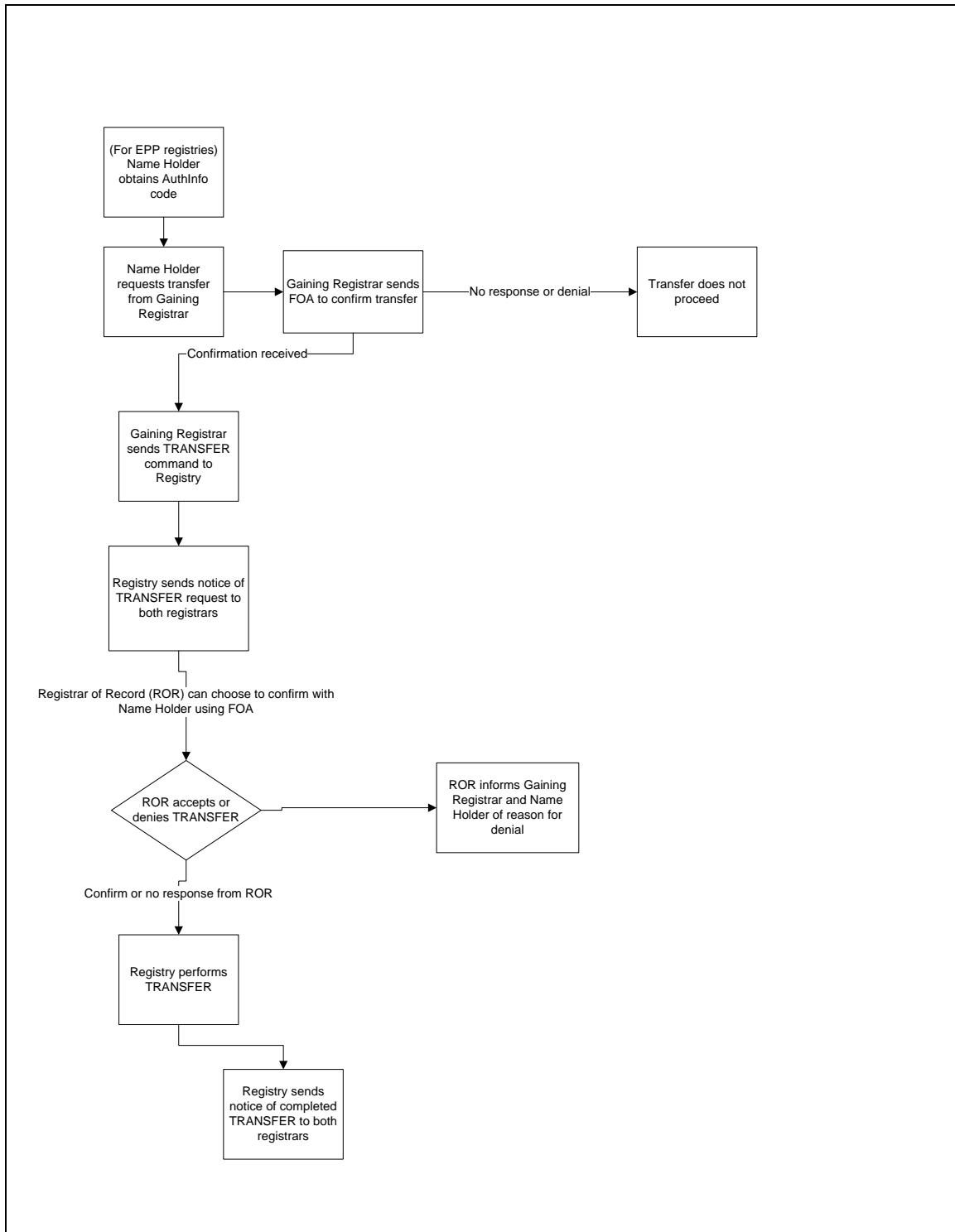
ICANN recognizes that many of the issues listed for consideration by the GNSO have already been topics of discussion during the policy development process. However,

these early experiences following the policy's implementation shed additional light on such issues and indicate they may need to be reconsidered and perhaps modified.

=

ICANN thanks all those who provided us their input in preparation for this report.

## Annex 1 - Flowchart of Transfer Process



## **Annex 2 – Panix Review**

The following correspondence contains ICANN's review of the <panix.com> case. This has been posted at <http://www.icann.org/correspondence/cole-to-tonkin-14mar05.htm>.

*14 March 2005 - Email from Tim Cole to Bruce Tonkin*

Dear Bruce:

We have completed our review of the unauthorized transfer of <panix.com>. ICANN considers this to have been one of the more serious breaches of its policies by an accredited registrar. We are also very concerned by Melbourne IT's explanation that the incident happened because Melbourne IT had purportedly “delegated” to a reseller the critical responsibility for obtaining the consent of the registrant prior to submitting a transfer request to the registry. While we appreciate Melbourne IT's report that it has withdrawn the offending reseller's ability to independently initiate transfers, Melbourne IT has indicated that it intends to continue to operate under agreements with other resellers that provide that Melbourne IT will not directly and independently verify the intent of registrants prior to initiating transfer requests. While we review the appropriateness of these arrangements under current policies and agreements, we will ask the SSAC to review this reseller/delegation issue in the context of the investigation it has launched into the security and stability concerns raised by the <panix.com> hijacking.

Also, while there is no indication that recent changes to the Transfer Policy had any bearing on this incident (the same abuse could have occurred under either the old or new policy), this issue will be referred to the upcoming GNSO review of the transfer policy for the consideration of changes that could be implemented to reduce the risks made apparent by this incident.

Based on documentation provided by Melbourne IT, Ltd. and Dotster, Inc., the <panix.com> incident occurred as a result of a failure of Melbourne IT to obtain express authorization from the registrant in accordance with ICANN's [Inter-Registrar Transfer Policy](#). The Transfer Policy is an ICANN Consensus Policy that went into effect on 12 November 2004. Both of the registrars were forthcoming with information about what took place concerning this transfer and the timeline below further details the events that took place. Correspondence detailing ICANN's questions and the registrars' responses can be found in the [Correspondence](#) section of the ICANN website including:

[Email from Tim Cole to Bruce Tonkin 18 January 2005](#)

[Email from Tim Cole to Clint Page 18 January 2005](#)

[Email from Bruce Tonkin to Tim Cole 27 January 2005](#)

[Email from Ravi Puri to Tim Cole 27 January 2005](#)

### **Timeline**

08 January 2005 (05:01 UTC) -Melbourne IT submitted a request to the registry to transfer the <panix.com> domain name. (Melbourne IT admits that this request was

submitted without proper authorization. Since <panix.com> was not on “lock” status, the registry accepted the transfer request and initiated the transfer process within the registry system. Had the domain name been on registry or registrar lock status, the attempt by Melbourne IT to initiate a transfer would have been automatically rejected by the registry software.)

09 January 2005 (01:40 UTC) - Dotster received notification from the registry of the transfer request. (The registry notifies losing registrars of pending transfer requests in two ways: via email and registrar-specific reports available for download. Following the transmission of the transfer request to the losing registrar, there is a standard five day Transfer Pending Period. During the Transfer Pending Period losing registrars may take steps to verify the registrant's intent to transfer, including attempting to contact the registrant. The Policy also permits the losing registrar to request a copy of the authorization for the transfer from the gaining registrar. In this case, Dotster has indicated that it did not take any action in response to the notification of the transfer request and allowed the transfer to be approved automatically at the end of the five day Transfer Pending Period.)

14 January 2005 (14:03 UTC) - Transfer completed to Melbourne IT.

15 January 2005 (05:56 UTC) - Domain re-delegated by Melbourne IT's customer to new nameservers. (At this point it became evident to the legitimate registrant that the domain name had been hijacked. This was around 01:00 Saturday morning in the location of the registrant. The registrant spent several hours attempting to reach someone at each of the registrars and the registry who could take action to reverse the transfer.)

16 January 2005 (18:55 UTC) - ICANN sent emails to both registrars requesting an explanation and an immediate fix as appropriate. (ICANN's inquiry to the registrars was prompted by a message to the public Registrars Constituency mailing list about the apparent hijacking.)

16 January 2005 (22:30 UTC) - Nameservers changed back by Melbourne IT Customer Service.

17 January 2005 (03:30 UTC) - Melbourne IT asked Dotster to initiate a transfer request in order to “undo” the transfer. (Registrars are encouraged to cooperate in this way to resolve disputes over transfers. The new Transfer Policy includes a formal dispute resolution process and a transfer undo mechanism, but it was not necessary to invoke either of those in this case.)

17 January 2005 (07:00 UTC) - Melbourne IT manually approved transfer requested by Dotster.

If you believe that further information would be helpful or corrections to the details above are warranted, please forward them to us and to SSAC for consideration in the review of this matter.

Sincerely,



Tim Cole  
Chief Registrar Liaison  
Internet Corporation for Assigned Names and Numbers

cc: Kurt Pritz  
John Jeffrey