Staff Report of Public Comment Proceeding

Policy Status Report: Inter-Registrar Transfer Policy (IRTP)	
Publication Date:	1 February 2019
Prepared By:	Brian Aitchison, Lead Researcher, ICANN Operations and Policy Research

Public Comment Proceeding	
Open Date:	14 November 2018
Close Date:	7 January 2019 (extended from 24 December 2018)
Staff Report Due Date:	1 February 2019

Important Information Links
Announcement
Public Comment Proceeding
View Comments Submitted

Staff Contact:	Brian Aitchison	**Email:**	brian.aitchison@icann.org

Section I: General Overview and Next Steps

General Overview

The IRTP Policy Status Report (PSR) is intended to provide an overview of the Inter-Registrar Transfer Policy. It includes readily available and general data on domain transfers, brief analyses, and a history of the Policy Development Process (PDP) for the consideration of the GNSO Council and ICANN community. It may serve as a basis for further review activities or, at the discretion of the GNSO Council, it may provide sufficient information as a standalone report for assessment of the policy.

The mandate for the IRTP PSR stems from two sources:

1. IRTP-D Working Group Final Report, Recommendation 17: "The WG recommends that, once all IRTP recommendations are implemented (incl. IRTP-D, and remaining elements from IRTP-C), the GNSO Council, together with ICANN staff, should convene a panel to collect, discuss, and analyze relevant data to determine whether these enhancements have improved the IRTP process and dispute mechanisms, and identify possible remaining shortcomings."

2. Consensus Policy Implementation Framework, Stage 5 "Support and Review: Policy Status Report": "Compliance and GNSO Policy Staff should provide a report to the GNSO Council when there is sufficient data and there has been adequate time to highlight the impact of the policy recommendations, which could serve as the basis for further review and/or revisions to the policy recommendations if deemed appropriate."

Next Steps

ICANN Org will update the Policy Status Report to include relevant information from public comments and the associated survey. The updated report will then be returned to the GNSO Council, who may then consider whether the report, public comments, and survey responses provide sufficient information as a standalone report for assessment of the policy, or if further work on the IRTP should be undertaken.

Section II: Contributors

*At the time this report was prepared, a total of **2 public comments had been posted to the forum, and 38 responses to the associated survey were received**. The public comment contributors, both individuals and organizations/groups, are listed below in chronological order by posting date with initials noted. To the extent that quotations are used in the foregoing narrative (Section III and IV), such citations will reference the contributor's initials.*

Organizations and Groups:

Name	Submitted by	Initials
World Intellectual Property Organization (WIPO) Arbitration and Mediation Center	Leena Ballard, Senior Legal Officer Ty Gray, Legal Officer	WIPO
Registrar Stakeholder Group – Tech Ops	Zoe Bonython	RrSG

In addition to the public comment proceeding, ICANN org created an online survey to gather input on general and specific aspects of the IRTP. The survey included 29 questions divided into two sets: one targeted at registrars, the other at registrants. The majority of questions—24—were registrar-specific.

The survey was provided via a link on the public comment page. It was not intended to provide a statistically representative sample of these communities, but rather to gather qualitative insight into issues surrounding the IRTP. The results of the survey can be viewed here: https://www.surveymonkey.com/results/SM-Q2J8JZRQV/

The survey instructions provided for respondents to submit their answers to the survey questions in the public comment forum rather than within the survey itself if they wanted to identify as a particular group (survey responses were anonymous). The RrSG submitted a public comment in this way. The other public comment received, from WIPO, was drafted independently of the survey questions, addressing issues surrounding the IRTP and Uniform Domain Name Dispute Resolution Policy (UDRP).

A summary of responses received via survey and public comment is provided in Section III: "Summary of Comments." Given it was provided independently of the survey, WIPO's comment is assessed separately from the others. The rest of the summary is organized according to the questions in the survey. As much as possible, the answers conveyed are intended to be representative of the general thrust of comments on a particular issue, but are not necessarily representative of the wider registrar or registrant communities.

An analysis of the survey responses and public comments is provided in Section IV: "Analysis of Comments." This section contains a brief, high-level summary of the major themes identified in the survey and public comments.

Section III: Summary of Comments

General Disclaimer: This section intends to summarize broadly and comprehensively the comments submitted to this public comment proceeding but does not address every specific position stated by each contributor. The preparer recommends that readers interested in specific aspects of any of the summarized comments, or the full context of others, refer directly to the specific contributions at the link referenced above (View Comments Submitted).

WIPO's public comment focuses on the IRTP's relationship with the Uniform Domain Name Dispute Resolution Policy (UDRP), in particular domain (un)locking, UDRP decision implementation (i.e. case suspension and settlement), and cyberflight (a form of unauthorized domain transfer carried out during a pending UDRP case).

WIPO posits that an ambiguity exists in the definition of a domain name "lock" and the responsibilities of gaining and losing registrars to "lock," or otherwise prevent transfer of, a domain subject to a UDRP proceeding. WIPO notes that inter-registrar transfers of domains subject to UDRP proceedings are still carried out, despite this being a violation of the IRTP (in most cases). While the losing registrar holds the responsibility of preventing a domain from being transferred if it's subject to a UDRP proceeding (usually via locking the domain), the ambiguity noted above results in losing registrars inadvertently transferring a domain despite a "lock" being applied.

The public comment noted the following issues with the IRTP:

- A gaining registrar may not be on notice that a domain is subject to a UDRP proceeding, which results in that registrar accepting the transfer and being (unknowingly) in violation of the Transfer Policy.

- In some cases, registrars obligated to transfer a domain name to a complainant following a UDRP decision disclaim responsibility for that obligation, claiming they are only obliged to unlock the domain.

- In some instances inter-registrar transfers are rejected due to those transfers being requested within 60 days of the creation date or last transfer date.

- As it relates to cyberflight, incidences [reported to WIPO] have decreased, but still occur occasionally. The public comment notes the lack of a mechanism for dispute resolution providers to enforce registrar responsibilities as they relate to transferring a domain name back to the original registrar or registrant. Thus, despite a UDRP decision in favor of a complainant, sometimes domain names are still not returned to the original registrar and/or registrant.

WIPO recommends that ICANN establish a standardized process for indicating that a domain is "locked" due to a pending UDRP case (e.g., using an EPP code) and for communications between losing and gaining registrars to confirm a domain's status as it relates to UDRP proceedings before initiating a transfer.

WIPO's recommendations as they relate to the above involve developing clearer processes, instructions, and standards for:

- Enforcing the obligations of gaining and losing registrars to (not) transfer a domain as a result of a UDRP proceeding (e.g. by clarifying domain name "lock" status in the context of inter-registrar transfers);
- Communications between gaining and losing registrars regarding transfer requests for domains that may be subject to a UDRP proceeding;
- Engagement between dispute resolution providers and registrars to enforce a provider's decision requiring transfer of a domain name back to a complainant and/or original registrar.

The public comment suggested that the metrics from ICANN Contractual Compliance provided in the PSR do not show data or indicate a mechanism by which UDRP providers can report IRTP breaches to ICANN Contractual Compliance. However, this information may be reported to Contractual Compliance. The Compliance data in the PSR contains a field showing "transfer[s] [that] cannot be completed because there is a pending Uniform Domain Name Dispute Resolution Policy (UDRP) action" (see PSR Section 3.1, Table 6, p. 35: "Transfer Related Complaints by Closure Code, 2012 – 2018"). The data shows that since 2012, Compliance has received two complaints regarding a transfer that could not be carried out due to a pending UDRP case.

WIPO also requested further breakdown of the data presented in the PSR regarding "nacked" ("not acknowledged," or rejected) transfers to illustrate those incidences where a transfer was nacked due to a pending UDRP case. As Specification 3 of the Registry Agreement does not require this level of breakdown in reporting, such data does not exist.

Survey Response Summary

Questions 1 through 24: Questions for Registrars

1. On a scale of 1 to 10, how effective is the transfer policy generally as it exists today (10 being most effective)?

   Overall: 6/10
   Answered: 35
   Skipped: 3

   Answer Breakdown:[1]

	1	2	3	4	5	6	7	8	9	10	TOTAL	WEIGHTED AVERAGE
☆	2.86% 1	8.57% 3	5.71% 2	2.86% 1	22.86% 8	11.43% 4	22.86% 8	8.57% 3	5.71% 2	8.57% 3	35	5.97

[1] For each "Answer Breakdown" table in this report, the "Weighted Average" reflects the average star rating given by respondents (no special weights were assigned to any response field). This is rounded to the nearest whole number in the results presented in "Overall" field directly above each table.

In their comment, the RrSG responded to this question with a "6 or 7," but ranked the dispute process at "0," stating it is ineffective and cannot be used to reverse a transfer.[2] They also argued the FOA and other process are unnecessary and do not prevent hijacking

2. More specifically, on a scale of 1 to 10, how effective has the policy been at facilitating transfers?

Overall: 6/10
Answered: 35
Skipped: 3

Answer Breakdown:

	1	2	3	4	5	6	7	8	9	10	TOTAL	WEIGHTED AVERAGE
☆	2.86% 1	5.71% 2	5.71% 2	2.86% 1	22.86% 8	11.43% 4	17.14% 6	20.00% 7	8.57% 3	2.86% 1	35	6.11

The RrSG gave the policy an "8" for inter-registrar transfers, but critiqued the "Change of Registrant" process (see question 12 below).

3. On a scale of 1 to 10, how effective has the policy been at preventing fraudulent or abusive domain transfers?

Overall: 6/10
Answered: 34
Skipped: 4

Answer Breakdown:

	1	2	3	4	5	6	7	8	9	10	TOTAL	WEIGHTED AVERAGE
☆	11.76% 4	0.00% 0	8.82% 3	5.88% 2	14.71% 5	14.71% 5	17.65% 6	5.88% 2	8.82% 3	11.76% 4	34	5.91

Here, the RrSG gave the policy a "0", arguing it did not prevent fraudulent transfers.[3]

4. Per year, approximately how many transfers have you/your company been a party to (either as a "gaining" or "losing" registrar) as a percentage of your total domains under management?

Answered: 30
Skipped: 8

Average: 30%
Median: 30%

[2] "0" was not an option in the survey. The RrSG provided this response in their public comment, which was based off the survey questions. It was not factored in to the averages resulting from the survey.
[3] "0" was not an option in the survey. The RrSG provided this response in their public comment, which was based off the survey questions. It was not factored in to the averages resulting from the survey.

Maximum: 100%
Minimum: 0%

5. The transfer policy has evolved over the last six years. In your opinion, have the policy modifications improved, worsened, or had no effect on the process for transferring domains between registrars and/or registrants? Please provide details to support your answer.

Answered: 31
Skipped: 7

Responses to this question varied from "complicated" and "worsened" to "simple" and "improved." Several respondents indicated the Temporary Specification for gTLD Registration Data, which allows registrars affected by the European Union's General Data Protection Regulation (GDPR) to redact a number of fields in the public WHOIS, decreased fraudulent transfers and streamlined the transfer process.

Representative excerpts and summaries follow:

- "For registrants it is overly complicated and a bad experience. This is primarily due to issues with fraudulent transfers and not having effective and efficient means to address them."
- Form of Authorization and email authorization not secure means to validate transfers.
- "The policy lags far behind acceptable technological options that could help prevent fraudulent transfers."
- Transfer Emergency Action Contact (TEAC) 4-hour response time unfair to registrars in different time zones.
- "…marked improvement in domain security and fraudulent transfers are effectively a non-issue now."
- "[Temporary Specification for gTLD Registration Data] a huge improvement"
- "The policy that allowed (mostly required) registrars to lock domain names due to a registrant change caused endless trouble that prevented legitimate transfers…Removing the requirement of an FOA to WHOIS has helped immensely."
- "Redacting of the WHOIS removed a huge attack vector. We have not seen any theft reports within the domainer community since May 25th with the one exception of one domain name stolen. The WHOIS info from this domain name was not redacted."
- The RrSG reiterated its previous statement that the policy works for inter-registrar transfers, but the "Change of Registrant" process is flawed, being "overly complicated and a bad user experience."

6. Many of the recent IRTP changes centered around protecting registrants from domain name hijacking. Do you believe the policy changes helped to mitigate this threat? Why or why not?

Answered: 31
Skipped: 7

Responses varied, but negative responses outweighed the affirmative. Affirmative responses tended to lack specifics, although one respondent noted:

- "With the requirement for the Losing Registrant to approve any email or name changes this has resulted in domains remaining secure unless the registrant email itself has been compromised."

The negative responses tended to provide more details, and described a number of issues, interpretations, and potential solutions regarding domain hijacking. For example:

- "Fraudulent transfers are most often the result of a registrant's email being hijacked first. This allows the hijacker to gain access to an email owner's various accounts and manage them directly. The transfer requirements included in the current policy do nothing to prevent hijacking under those conditions."

- "Removing attack vectors [such] as registrant WHOIS information is a no-brainer. Displaying such data makes it very easy for hackers if they know the name and email address."

- "The IRTP changes required notifications be sent to the current and new registrant but did not include an immediate reversal option or a validation option. For example, if a domain registrant was being updated to 'Company A' there was no validation that the email address listed for 'Company A' actually belonged to the company."

- "They may conceivably have made some hijackings not happen for the sole reason that they made ALL transfers more difficult, but that's all, and even that effect is limited: Any hijacker with experience would simply know not [to] update the registrant contact before hijacking it."

- "Other measures not directly tied to transfers are way more efficient. Such as forcing a 2 factor authentication to log under customer accounts, login notifications etc."

- The RrSG posited that the policy did not help mitigate the threat of domain name hijacking, noting they have not seen a decrease in hijacking cases since the implementation of IRTP-C.

7. What methods do you use to mitigate domain name hijacking outside of the IRTP framework?

Answered: 26
Skipped: 12

Respondents noted the following methods to prevent domain name hijacking:

- Default domain locking

- Direct verification—either via phone call, email, or paper form—from clients prior to taking action on a domain
- Domains only placed in unlock status once registrant confirms transfer via direct verification
- Two-factor authentication
- Manual comparison of IP addresses and other available customer data with customer's historical IP addresses and data
- Regular updates to and high security standards for transfer AuthCodes

8. Compared to previous years, do you see more, less, or the same amount of hijacking cases?

Answered: 32
Skipped: 6

More	6.25%	2
Less	34.38%	11
No change	59.38%	19

The RrSG reiterated that its members witnessed "no change" in the amount of hijacking cases they process.

9. In your view, did the Form of Authorization (FOA) requirement work to mitigate problems surrounding unauthorized domain transfers? How might this requirement be improved or changed to mitigate such problems?

Answered: 29
Skipped: 9

Most respondents indicated that the FOA was no longer required, was an annoyance or complication for customers, and outdated. They noted that the use of email to send/receive the FOA was problematic given that many hijacking cases are a result of a registrant's email being compromised. Respondents indicated that AuthCodes within EPP and domain locking at the original registrar provide sufficient security.

One respondent's answer was generally representative of the negative responses:

- "The FOA was helpful to compare contact details for the gaining and losing registrar, but every time the details were the same surrounding unauthorized transfers; meaning the hijacking always happened before the transfer request itself."

Another replied:

- "We saw no increase in issues since the FOA has not been required under [the] Temp Spec and therefore feel it does not add any value."

A small number of respondents replied that the FOA was useful in that it created a paper trail for transfer issues and ensured that a registrant understood his/her domain was being transferred.

The RrSG noted that responses varied within their group:

- "Some registrars find that the FOA increases risk because it relies on a non-secure method (email), which can be accessed improperly to transfer a domain without the [registered name holder's] approval. Other registrars find that the FOA helps mitigate problems by ensuring the current registrant understood the domain was transferring to a new registrar.
  There is agreement that we should move away from the FOA and focus on [AuthCode] security."

10. Do you think the FOA should continue to be a requirement given most systems are now based on the Extensible Provisioning Protocol (EPP)? Why or why not?

    Answered: 30
    Skipped: 8

Answers were relatively balanced between affirmative and negative responses. The affirmative responses generally argued that the FOA provides an extra layer of security, and that confirming a transfer via the registrant's email was necessary. Some respondents argued that an FOA from the losing registrar should still be a requirement. Three responses are representative:

- "FOA approval should continue. Some Registrants might inadvertently share their EPP code without understanding the effects. Approval from the Registrant email is a must."

- "…FOA should absolutely remain. Even if it never comes up in 99.9% of cases those additional records can help resolve potential issues or disputes when they arise and have proven invaluable in the past."

- "…all efforts to confirm a transfer should be taken to protect the owners."

The negative responses argued that technical solutions are available which obviate the need for the FOA, that it's an unnecessary barrier to carrying out a transfer, and that it does not work to mitigate unauthorized transfers given that most are carried out using compromised registrant email addresses. For example:

- "No, because all you need is the AuthCode. The FOA only adds 'paperwork' to the process and does not provide any protection."

- "No, there are technical ways to ensure that the transfer was requested by the registrant that do not require additional emails be sent."

- "No, FOA is redundant to people who have confirmed that they want to transfer. And unable to suppress unauthorized domain transfers."

Some negative responses offered solutions to maintain domain transfer security without the FOA:

- "No, because the password itself should be enough (plus domain transfer lock)…however…there should be work around a scheduled EPP password rotation or expiration…"

- "Due to GDPR the FOA process is broken and we need to get rid of it. Short lived Transfer Tokens in the EPP could be a solution."

- "Most systems are already based on EPP. With the Temp Spec we can no longer do FOA. Therefore we should have better security surrounding [AuthCodes]."

- The RrSG provided a detailed response:

  No. Prior to Temp Spec changes, the FOA functioned as a second factor of authentication for the transfer, but was cumbersome for the Registered Name Holder to use effectively. Removing the FOA requires the enhancement of other security measures, specifically the [AuthCode]. There should be best-practice guidelines for [AuthCode] security; TechOps leans towards Registrars bearing the responsibility for the [AuthCode].

11. <u>It is no longer required for the losing registrar to provide the FOA as a result of the "Temporary Specification for gTLD Registration Data." Is this a transfer solution you support? Do you have concerns with this? Please explain your answer.</u>

    Answered: 31
    Skipped: 7

    Answers to this question were skewed toward the affirmative (i.e. they supported removing the FOA requirement). In general, they noted that they experienced few or no issues when the requirement was removed as a result of the GDPR/Temp Spec, and that redacting much of the public WHOIS increased security in-and-of itself. Some representative answers follow:

    - "We support the elimination of the FOA…that is, we support simply making the 'Temporary Specification for gTLD Registration Data' permanent…In fact, the lack of public WHOIS data is almost certainly making domain names more secure against hijacking, as it prevents malicious actors from using WHOIS to determine which email address they need to compromise to hijack a domain name."

    - "Yes, this is how the thefts are occurring. It is too easy to create a new fake account and request the transfer."

- "The GDPR is now in effect for more than 175 days. If there were issues they would have emerged already. But we have observed no issues and is in line with our experience as a ccTLD registrar for many large ccTLDS which have no FOA requirement."

- Yes we support the [removal of the FOA requirement]. Transfers should be redesigned to a) [be] GDPR compliant b) real time and c) safer."

As in previous questions on the FOA, some respondents suggested relying on the AuthInfo code as a default method to verify transfers and increasing security of those codes:

- "…the AuthInfo code should be the default method (like it is the case for a lot of ccTLDs) but every registrant should be given an alternative, should he/she not be able to obtain the code of his/her domain name."

- "We support no longer attempting to send the FOA. We support both registrars (gaining & losing) properly notifying registrants. We maintain the existing 5-day grace period to be an important mechanism for stopping unwanted transfers. We strongly suggest changes in registry-level auth-info practices for domain security."

- "I am concerned about who receive[s] [the AuthCode][.] [I]f we could confirm that only [the] registrant can receive [the AuthCode], then we may no longer need FOA."

Responses that supported keeping the FOA provided the following rationales:

- "…still [need] the FOA process…Without FOA, as a registrar, we are unable to provide this to [a] judge."

- "Having the FOA included as part of the transfer process lets us pull additional information should there ever be a dispute or claim of hijacking with a domain transfer and ensure it is handled correctly. It's always better to have more records and be over-prepared than not."

12. What issues, if any, have you encountered with the 60-day "Change of Registrant" lock requirement? Do you see this as an effective policy requirement? Please explain your answer.

Answered: 28
Skipped: 10

Respondents were somewhat ambivalent about the 60-day "Change of Registrant" (COR) lock requirement, but gravitated toward lack of support. While acknowledging it helps the security of transfers, they expressed that their customers often did not understand it or viewed it as burdensome, which resulted in more calls to registrar support teams. Some viewed the period as too long. Some representative answers were:

- "[The COR lock] has been a frustration for registrants and registrars alike. There are many reasons registrants choose to lock or unlock their domains. Automatic locking causes confusion. This often leads to increased contacts from registrants when transfers fail."

- "We support having a delay as it is effective and gives registrants an opportunity to act/respond in cases of fraud. However, forcing parties to accept it has over-complicated the issue. Additionally, overuse of the designated agent has negated the Change of Registrant policy, making it ineffective. Ultimately, the 60-day change of registrant transfer lock should be at the registrar's discretion."[4]

- "The 60-day Change of Registrant lock requirement can at times be a burden, both inbound and outbound. An example would be when a registrant is simply correcting information before a transfer. This also hinders corporate acquisitions and divestitures, as companies are legitimately updating large lists of domains to new legal entities."

- "Many registrants don't understand the 60-days lock policy. So they think that [it] is [an] inconvenience. But [it is] an effective policy requirement."

- "It is not an effective policy because it only traps legitimate registrants; hijackers by now all know to avoid changing the registrant before a hijacking. It should be eliminated."

- "We support the 60-day 'change of registrant' lock requirement. This prevents immediate transfers after a domain has been updated."

- In their public comment, the RrSG assigned a score of "3" (out of 10) to the "Change of Registrant" process, arguing it is too confusing for registered name holders to navigate, creates unnecessary burdens, and offers few benefits."

13. Do you lock domains by default upon registration of a name?

Answered: 32
Skipped: 6

Yes	68.75%	22
No	31.25%	10

14. When implementing "Change of Registrant" lock requirement, did you chose to implement the opt-in option vs. the opt-out? Why or why not?

Answered: 27
Skipped: 11

[4] See icann.org, "Transfer Policy," Section II.A.1.2: "'Designated Agent' means an individual or entity that the Prior Registrant or New Registrant explicitly authorizes to approve a Change of Registrant on its behalf." See also Section II.C.1.2-4, which details the change of registrant process and the role of the designated agent. https://www.icann.org/resources/pages/transfer-policy-2016-06-01-en

Responses and rationales were split on this question. “Opt-in” respondents indicated they did so to increase security, while “opt-out” respondents did so for the sake of simplifying the transfer process for their customers. Others provided their customers with the choice. For example:

- “Opt-in for greater protection” and “for security purposes.”
- “We chose the opt-out by default. The 60-day Change of Registrant lock requirement can at times be a burden, both inbound and outbound. An example would be when a registrant is simply correcting information before a transfer.”
- “We give the option to select either. We do not default to one or the other. We allow the customer to choose.”

15. Should the duration of the “Change of Registrant” lock stay the same, or be shorter, longer, or no longer a requirement?

Answered: 34
Skipped: 4

Same	26.47%	9
Shorter	17.65%	6
Longer	8.82%	3
It should no longer be a requirement	47.06%	16

16. Should there be more standard reporting requirements across registrars as they relate to transfers? If so, what should these reporting requirements include?

Answered: 24
Skipped: 14

Responses generally expressed ambivalence or no opinion (although skewed toward the negative), were short, and respondents indicated they weren’t clear on what this question was asking. Some offered suggestions for reporting requirements. Some representative examples follow:

- “Yes. All registrars/services providers should be required to provide a health scorecard which includes transaction data including transfers.”
- “Once every registry will be thick, it should be a requirement for the registry to keep a record of WHOIS details before a transfer for one year.”

- "We might want to check how often [the Transfer Emergency Action Contact, or TEAC] is used to asses if it is effective. We also might want to check IRTP-D and see how many disputes have been filed. And check with compliance how many cases of REAL domain theft occurred."

- "No, this would be an additional cost to registrars with no business benefit or benefit to end users."

- The RrSG responded: "Definitely not. Reporting by registrars should be voluntary and on an as-needed basis."

17. Would you be willing to share transfer data publicly in order to enable assessment of the transfer policy's effectiveness, even if not a contractual obligation?

Answered: 33
Skipped: 5

Yes	18.18%	6
No	27.27%	9
Not sure	54.55%	18

18. Do you think the Transfer Emergency Action Contact ("TEAC") is an effective way to handle urgent inter-registrar transfer issues between registrars, or does the TEAC process require changes?

Answered: 25
Skipped: 13

Most respondents indicated they had little to no experience with the TEAC. Those that had indicated the required 4-hour response time was unfair to registrars in different time zones. One suggested the TEAC response time be extended to 12-24 hours. Some substantive responses were:

- "We would like to see TEAC be the start of a process requirement where both registrars work to come to a resolution."

- "Yes it is very useful. Most of the time we can resolve issues this way."

- "What is needed is a deadline by which a TEAC response must give a final answer on whether the transfer will be reversed, not merely a deadline on when they have to send a generic useless response."

- The RrSG provided a detailed response:

  The TEAC **does** require changes [emphasis in original]. The TEAC is an effective way to make contact regarding an urgent transfer issue, but it does not go far enough, because it does not require that both registrars work together to investigate and reverse the disputed transfer if needed. The process should be revised to require the two

registrars to come to a mutually acceptable resolution, potentially with the assistance of a neutral mediator.

There is significant concern with the 4-hour response time requirement, as this can be a burden especially across different time zones and languages. One option could be to require the current 4-hour response time for registrars with overlapping time zones, while registrars with significant disparities in time zone could have a longer response time.

19. In general, what issues are your customers having, if any, as they relate to transfers?

Answered: 25
Skipped: 13

Responses to this question varied greatly by the experience of a given registrar. A comprehensive sampling of responses follows:

- "The main issues are 1) customers are not able to get their domain name back if hijacked, 2) customers hate the Change of Registrant policy, and 3) in general a lack of good dispute mechanisms."

- "Currently some registrars do not make it easy to transfer away large lists of domain names [and] make it difficult to in [unlock] domains at the registry and retrieving auth codes. Some registries allow bulk transfers but the process to do so is [onerous]. ICANN should mandate registries allowing bulk transfers as long as losing and gaining registrars [agree]."

- "EPP and access to email id"

- "Since the temp spec implementation our customer have given us nothing but great feedback on how easy and simple the transfer process is. It gives the customers the option to choose to right Registrar for them without delays/ complications with transferring."

- "Process is needlessly complex and confusing, and takes too long to complete. Process to undo in case of error or actual hijacking is unclear."

- "Contact updates leading to inadvertent blocking of legitimate transfers. That's by far the #1 problem."

- "Registrants are frustrated by the automatic lock. They are also frustrated by the additional consenting via email. There are too many steps to complete a transfer when they have already supplied the auth code."

- "The biggest issue is the complexity of the transfers which makes it very hard for registrants to transfer their domain names. The option or the lack of the option for resellers to transfer domain names in bulk is a blocking factor and forces resellers to stay where they are even if they can get a better price at a different registrar or if the registrar has a better and more secure platform. We are hindering innovation and security here."

- "Most of our customers transferring inbound are leaving their existing provider due to a service delivery failure. The last thing they want to do is have the transfer process involve the losing registrar. If the domain name is locked in some cases it can be enough trouble for them to request the losing registrar unlock the domain name so the losing registrar should not be involved any more than this when transferring domain names."

- The RrSG provided a detailed list in its public comment:
    - Registered Name Holders often think transfers should be instantaneous
    - They're annoyed by the FOA and think providing the [AuthCode] should suffice
    - If a domain **is** hijacked, there is no effective dispute or resolution mechanism
    - Bulk transfer of domains should be improved and streamlined
        - Difficult for Registered Name Holders to retrieve [AuthCodes] for a long list of domains as there are no requirements to permit bulk [AuthCode] requests
        - Registry often does not allow for bulk transfer requests

20. What do you consider to be measures of success as they relate to transfers?

Answered: 25
Skipped: 13

Responses were more or less consistent, stating they would consider the following indicators as "measures of success":

- Satisfied customers

- Low rates of fraud, hijacking, and/or abuse complaints (to ICANN and/or the registrar)

- A transfer process that takes less time and is more efficient, but is still secure and underpinned by strong record-keeping requirements

- Ability to obtain AuthCodes to transfer domains in bulk

21. What do you think the ideal transfer process should look like from a policy and a technical perspective?

Answered: 27
Skipped: 11

Respondents' answers were generally focused on removing or modifying the FOA requirement, improving technical standards for verifying transfers (e.g. with improved AuthCode security), and ensuring a registrant's consent to a transfer is legitimate. Some representative responses include:

- Eliminate FOA and modify, reduce, or remove lock requirements

- AuthCode standardization and rotation

- Effective and immediate transfer reversal process via EPP
- Registrants and registries may reject transfers
- Effective and accessible dispute mechanism that puts the burden of proof on the gaining registrar and the requesting registrant
- Two-factor authentication and/or opting for delay before a transfer completes to give a registrant time to object
- Changing the length of the waiting period in which a transfer can be disputed to when a registered name holder requests the AuthCode, rather than after the transfer is initiated with the registry (at which point the transfer should be completed immediately)
- Keep the requirements of the "Temporary Specification for gTLD Registration Data"

One respondent described an ideal transfer process that is representative of other responses, the steps of which are summarized here:

- A registrant logs in at his/her losing registrar to get the AuthCode.
- The registrant provides relevant information—i.e. AuthCode, desired authoritative DNS nameservers, and WHOIS details—to the gaining registrar and initiates the transfer using the gaining registrar's account.
- The registrant is then required to log in to his/her losing registrar to approve the transfer.
- The losing registrar instantly transfers the domain to the gaining registrar while the registry instantly updates the WHOIS record to reflect the changes.
- [A transfer should be completed with no down time.]

22. If the GNSO was considering further review of the transfer policy in addition to the IRTP Policy Status Report, what priority would you assign it given existing policy efforts: high, medium, low, or no priority?

Answered: 31
Skipped: 7

High	29.03%	9
Medium	48.39%	15
Low	16.13%	5
None	6.45%	2

23. In your view, what could be improved in regard to making domain name transfers?

Answered: 23
Skipped: 15

Respondents generally repeated or reiterated their previous responses. Some representative responses on improvements to the domain name transfer process and general comments on the transfer policy include:

- "Setting minimum requirements for [AuthInfo] codes throughout the domain industry [and] enforced by registries. These requirements would include[:]
  - Minimum and maximum number of characters required for [AuthInfo] code
  - Generic terms such as 'password, authinfo' not allowed
  - Maximum [time-to-live requirement] for [AuthInfo] codes"

- "Remove the change of registrant requirements as they have no impact to domain hijacking. Also improve the process between gaining and losing registrar where a separate 'code' is used instead of emails to confirm transfers between each other."

- "Make the temporary elimination of the FOA permanent. Add rules to make reversal of fraudulent transfers easier."

- "If the issue is domain theft you should not look at the transfer process but more how to secure registrar or reseller control panels."

- "The IRTP in its current form is a patch work. Technology has evolved and moved forward but the policy is by and large about 15 years behind."

- The RrSG added that "ease and speed of transfer" and "ease of undo (for registrar) in cases of unauthorized transfer" could be improved.

24. <u>If you have any additional input on the IRTP and/or transfer process in general, please do so here.</u>

Answered: 23
Skipped: 15

Respondents provided a few answers here, which were generally reflective of responses received to previous questions:

- "1. ICANN Compliance needs to be more responsive to bad registrars
  2. More flexibility is needed [around] the use of AuthCodes
  3. Allow for business decisions around transfers, such as use of [an] EPP command for initiating a transfer back"

- "The requirements around changes of ownership had good intentions but are incredibly frustrating for registrants. It is a policy that is almost impossible to implement in a customer-friendly way."

- "Scope the size of the issues and use real data for the scoping. In addition review such processes [to see] if they are data protection law compliant."

- "The right to enforce [a] transfer should be given to the registrar. The registrar should follow the policy of both ICANN and the laws of the country."

- In their public comment, the RrSG recommended the following:
    - "When a transfer request is submitted, both the registrar and the registry should watch for a 'brute force' style attack, where many potential [AuthCodes] are tested against the domain until one succeeds, and prevent such abuse of the transfer process."
    - "Authorization should be allowed via whatever form the registrar uses to contact their clients; email should not be specifically required."
    - "Allow for business decisions such as being able to use an EPP command to initiate an immediate transfer reversal."
    - "For a Change of Registrant, both the gaining and losing registrants should be notified of any requests, and should have the option to accept or reject, over EPP notifications."

Questions 25 through 29: Questions for Registrants

25. How would you characterize your experience transferring your domain name(s) from **one registrar to another**: very easy, easy, neither easy nor difficult, difficult, or very difficult? If you have any details, please provide them to support your answer.

Answered: 22
Skipped: 16

Very easy	13.64%	3
Easy	31.82%	7
Neither easy nor difficult	27.27%	6
Difficult	4.55%	1
Very difficult	4.55%	1

Some respondents provided details about their answers:

- "…I would characterize transferring from one registrar to another for a novice [registered name holder] to be difficult as there used to be several emails involved to process a transfer if they needed to make any contact changes on the registrant details. Then after that is done, more potential email and waiting."

- "[A] problem arises…when the domain was arranged through a reseller who then vanishes…"

- One respondent provided a detailed list of suggestions to improve the transfer experience for registrants:

    1. "[The] domain transfer time is too long and not consistent[,] which can lead to delays in fixing issues with WHOIS record[s]…[or] DNS misconfiguration at the new registrar. Registrars and registries should be required to complete near instant domain transfer once transfer has been approved by registrant."
    2. To avoid authoritative DNS nameserver and WHOIS info misconfiguration problems[, the] gaining registrar should be required to allow registrants to configure all authoritative DNS nameservers and WHOIS contact info prior to the domain transfer[,] and gaining registrar should update this info at the registry level when [the] transfer completes."
    3. Registrants should be able to transfer domains without having to first remove WHOIS privacy protection.
    4. …I would rather not have the 60-day wait period for inter-registrar domain transfers or change of registrant contact.
    5. Prior to a domain transfer[,] registrars should be required to inform [the registrant] of what…the new expiration date [will be] if [registrant decides to pay for the domain transfer."

26. How would you characterize your experience transferring your domain name(s) from **one registrant to another**: very easy, easy, neither easy nor difficult, difficult, or very difficult? If you have any details, please provide them to support your answer.

    Answered: 22
    Skipped: 16

Very easy	9.09%	2
Easy	31.82%	7
Neither easy nor difficult	27.27%	6
Difficult	9.09%	2
Very difficult	4.55%	1

Some respondents provided details about their answers:

- "I find this very difficult now due to the change of registrant process. Reputable registrars have security measures in place outside of the transfer process itself in order to prevent hijacking and those need to be entrusted."

- "This largely depends on the registrar."

27. How would you characterize your experience using the transfer process to acquire a domain name **from another registrant**: very easy, easy, neither easy nor difficult, difficult, or very difficult? If you have any details, please provide them to support your answer.

Answered: 21
Skipped: 17

Very easy	4.76%	1
Easy	23.81%	5
Neither easy nor difficult	28.57%	6
Difficult	23.81%	5
Very difficult	0.00%	0

While the majority of respondents indicated the process fell into the "(very) easy" and "neither easy nor difficult" range, some respondents noted the following:

- "…sometimes there will be ownership dispute between the [registered name holder's] name and the [registered name holder's] email."
- "[The ease of the transfer process] largely depends on several factors [such as the] [e]scrow company[,] [d]omain brokers[,] [d]omain name sale platform [such as] Sedo, Afternic etc, [and] registrar(s)"

28. In your view, what could be improved in regard to making domain name transfers?

Answered: 13
Skipped: 25

Responses included:

- "I like the current process, [but] add the [Change of Registrant requirement] back in for gaining registrars."
- "Confirmation with [domain name] owners should always happen via more than 1 means [e.g.] email, [text], mail, [or] phone."
- "While the [AuthInfo] code is a good system, I should also be able to transfer my domain name without any intervention from the outgoing registrar, should that one not be cooperative."
- "On the transferred registrar platform, select the registrar to be transferred, confirm the operator by password, email, face recognition or other means. After the transfer to the registrar platform is successful, you can transfer to the new registrar."

- "Fewer steps for the registrant to take."

29. If you have any additional input on the IRTP and/or transfer process in general, please do so here.

Answered: 7
Skipped: 31

Responses were few, but included the following:

- "ICANN should define clearly [the] resolving procedures for transfer abuse in the transfer policy."

- "The easier the transfer process is [the] more it encourages fair registrar competition."

Section IV: Analysis of Comments

General Disclaimer: This section intends to provide an analysis and evaluation of the comments submitted along with explanations regarding the basis for any recommendations provided within the analysis.

The survey and public comments provide qualitative details on issues surrounding the IRTP. The survey was not designed to be statistically representative of the communities it targeted—i.e., registrars and registrants—but rather to provide insight into specific IRTP-related issues affecting the registrar and registrant communities.

Overall, comments were mixed. Some favored certain aspects of the policy while others were against those same aspects. The major issues and recommendations noted in the survey and public comments centered around transfer verification and security, and modifying the steps for carrying out a transfer. A thematic summary of the comments is presented below. Note that any issue or recommendation presented herein does not necessarily reflect consensus in the survey on the topic; some respondents may disagree with what was put forth by others.

Transfer Verification and Security

- Improve standards and security for transfer AuthCodes, and rely on them to carry out transfers via the Extensible Provisioning Protocol (EPP)

- Reduce or eliminate need for email verification of a transfer, as hijackings regularly occur using compromised email addresses

- Verify transfers with registrants using all available means, including voice calls, email, text, and paper forms

- The Transfer Emergency Action Contact (TEAC) requirements should be modified. The mandated 4-hour response time is unfair to registrars in different time zones and registrars do not have a process to work together on resolving an urgent transfer issue.

- Improve capabilities and/or processes to determine whether a domain being transferred is subject to a Uniform Domain Name Dispute Resolution Policy (UDRP) case, and strengthen enforcement of dispute resolution providers' decisions

Transfer Process Steps

- Fewer and/or less complicated steps for registrants to transfer their domain(s), and quicker transfer times. Respondents indicated the 60-day "Change of Registrant" lock requirement was frustrating.

- Eliminate or modify the "Form of Authorization" (FOA) requirement—especially for losing registrars—as it does not prevent domain hijacking. However, some respondents indicated the FOA requirement should remain as it provided an extra layer of security around the transfer process.

- The “Temporary Specification for gTLD Registration Data,” which eliminates the FOA requirement, is an improvement over the previous process and should be kept in place [see IRTP PSR, Section 1.3]