IRTP Part D PDP Working Group – Public Comment Review Tool
23 June 2014

For complete overview of comments received, please see http://forum.icann.org/lists/comments-irtp-d-initial-03mar14/msg00001.html.

#	Comment	Who / Where	WG Response	Recommended Action
Recommendation #1: The WG recommends that reporting requirements be incorporated into the TDRP policy. Outcomes of all rulings by Dispute Resolution Providers[1] should be published on Providers' website, except in exceptional cases. The Group recommends publishing reports that follow the example of the Asian Domain Name Dispute Resolution Centre (ADNDRC).[2] These reports should include at a minimum: a) Information about parties involved in the dispute; b) The full decision of the case; c) The date of the implementation of the decision				
1.	In general, this is a good idea that you support. This will give precedents we can all refer to and make the rules more clear to everybody.	Arthur Zonnenberg	WG acknowledges the comment	**No action needed at this time**
2.	BC considers that reporting requirements for registries and dispute providers should be developed in order to make precedent and trend information available to the community and allow reference to past cases in dispute submissions. BC supports the details of our position on Charter Questions A that are encompassed into of recommendation #1	Business Community (BC)	WG acknowledges the comment	**No action needed at this time**
Recommendation #2: The WG recommends that the TDRP be amended to include language along the lines of this revised version of the UDRP: 'The relevant Dispute Resolution Provider shall report any decision made with respect to a transfer dispute initiated under the TDRP. All decisions under this Policy will be published in full over the Internet, except when a Dispute Resolution Panel determines, in an exceptional case, to redact portions of its decision. In any event, the portion of any decision determining a complaint to have been brought in bad faith shall be				

[1] The Working Group recommends in Charter question C to remove the Registry as the first dispute resolution layer of the TDRP. Therefore, despite wording of Charter question A, no reporting requirements for the Registries are included here.

[2] See four ADNDRC Reports on TDRP decisions: http://www.adndrc.org/mten/TDRP_Decisions.php?st=6

#	Comment	Who / Where	WG Response	Recommended Action
published.’				
3.	BC supports the details of our position on Charter Questions A that are encompassed into of recommendation #2	BC	WG acknowledges the comment	**No action needed at this time**
Recommendation #3: The WG recommends that the TDRP be amended as follows: “Transfers from a Gaining Registrar to a third registrar, and all other subsequent transfers, are null and void if the Gaining Registrar acquired sponsorship from the Registrar of Record through an invalid transfer, as determined through the dispute resolution process set forth in the Transfer Dispute Resolution Policy.”				
4.	The RySG is supportive of this recommendation. It is the opinion of the RySG that an invalid transfer should be defined as a transfer that occurs in violation of the Inter-Registrar Transfer Policy. With regard to the question of whether costs would need to be refunded to registrars in case of negating/reversing transfer under a multiple-hop scenario, because the “undo” of a transfer in cases where it has been determined that the transfer occurred in violation of the IRTP changes only the Registrar of Record and the expiry date of the domain remains the same, it is the view of the RySG that there should be no refund of the registration fees (i.e. costs).	Registry Stakeholder Group (RySG)	WG acknowledges the comment	**No action needed at this time**
5.	Additional provisions should be included Multiple transfers in the Transfer Dispute Resolution Policy (TDRP) that set out how to handle disputes when multiple transfers have occurred. As they could help clarify the process and facilitate the handling of disputes, multiple transfers are used in domain hijack situations, and also since the aftermarket has developed after the policy was written, a third party can easily purchase a hijacked domain in good faith. BC supports the details of our position on Charter Questions B that are encompassed into of recommendation #3, #4, #5, and #6. The BC particularly appreciates the work of the WG in developing these complex and carefully composed recommendations.	BC	WG acknowledges the comment	**No action needed at this time**

#	**Comment**	**Who / Where**	**WG Response**	**Recommended Action**
6.	Could ‘null and void’ be rephrased? As an automatic undo of all subsequent transfers poses some risks that could be mitigated if a human actually reviewed them to make sure they were warranted. Possible re-phrase: “may be reversed at the direction and within the discretion of the dispute resolution panel”	ICANN Staff	The wording of ‘null and void’ was a deliberative choice to address the issue of multiple hops that occur within the statute of limitation.	**Re-visit this wording before finalizing the recommendation**
Recommendation #4: The WG recommends that a domain name be returned to the original Registrar of Record if it is found through a TDRP procedure that a non-IRTP compliant domain name transfer has occurred. The TDRP as well as guidelines to registrars, registries and third party dispute providers should be modified accordingly.				
7.	The wording ‘original Registrar of Record’ might be too clumsy. Proposed re-phrasing: The WG recommends that a domain name be returned to the complaining Registrar if a TDRP procedure finds that an invalid transfer has occurred, regardless of any subsequent, legitimate transfers. The TDRP as well as guidelines … … …	ICANN Staff	WG agrees that the wording could be improved. A list of definitions of key terms could be included in the IRTP.	**Drawing up a list of definitions of key terms.**
8.	If multiple transfers have occurred after the first one that is wrong, then only that one should be checked. Checking the entire chain does not seem useful to me. Wherever the domain may be afterwards, it should be rolled back to the state before the first breach, preferably actively by the registry. Most of the affected 'registrants' are puppets by a hacker, or real users that saw a deal that was too good to be true (an inviting price for a highly valued domain). Then it usually is. But it's pretty much a corner case that does not occur often.	Arthur Zonnenberg	WG acknowledges the comment	**No action needed at this time**
Recommendation #5: The WG recommends that the statute of limitation to launch a TDRP be extended from current 6 months to 12 months from the initial transfer. This is to provide registrants the opportunity to become aware of fraudulent transfers when they would no longer receive their registrar’s annual WDRP notification.				
9.	The RySG can support this recommendation but with reservation.	RySG	WG acknowledges the	**No action needed at**

#	Comment	Who / Where	WG Response	Recommended Action
	Specifically, the longer the statute of limitations is to file a request for enforcement would also mean that there is greater opportunity for multiple transfers to occur between when the alleged violation occurred and the request for enforcement is filed.		comment and agrees broadly with the assessment but the 12 months seems to a good compromise	**this time**
10.	The ALAC particularly supports Recommendation 5 that would extend the statute of limitation to launch a Transfer Dispute Resolution Policy (TDRP) be extended from the current 6 months to 15 months from the initial transfer.	ALAC	WG acknowledges the comment and agrees broadly with the assessment but the 12 months seems to a good compromise	**No action needed at this time**
11.	Since a lot of registrations are paid for 1 year, it would only be after that time that customers might spot they are no longer the owner of a domain name. This would especially be true in case the domain is abducted but the DNS remains unaltered. If then the statute of limitation is one year and if the incident occurred almost at the time of payment / renewal, the registrant would most likely loose the opportunity to take action as there would be no or little time left to do so. Example: Abduction of domain name is on renewal date +3 days. Limitation would become effective 1 year later, which would leave the registrant almost without a chance to notice that he has not been invoiced and the domain has already gone. Additional 3 months would not really make a difference to the registrars, but they could be very beneficial for the registrant, who - in most cases - is unsuspecting and will need some time to find out about the measures he / she can take.	Thomas Rickert	WG acknowledges the comment and agrees broadly with the assessment but the 12 months seems to a good compromise	**No action needed at this time**
12.	The justification seems a little weak since registrants are unlikely to notice (and take action) because of a missing WDRP	ICANN Staff	WG acknowledges the comment.	**No action needed at this time**

#	Comment	Who / Where	WG Response	Recommended Action
	notification.			
Recommendation #6: The WG recommends that if a request for enforcement is initiated under the TDRP the relevant domain should be 'locked' against further transfers. The TDRP as well as guidelines to registrars, registries and third party dispute providers should be modified accordingly.				
13.	It might be useful to add this 'lock' under the bases for denial of transfers.	ICANN Staff	Have 'IRTP' and 'URS' added to denial reason 2. As discussed in previous working groups, a domain name lock is a situation where a registrar must knack a transfer request.	**Amend recommendation to include IRTP and URS under 'denial reason 2' and explicitly described the lock requirement in the TDRP section of the policy because otherwise registrars may treat it as optional**
14.	The RySG is supportive of this recommendation. Some TLD registries currently have a practice of 'locking' a domain name by applying server TransferProhibited, serverDeleteProhibited and serverUpdateProhibited to the domain name upon receipt of a request for enforcement. In those cases, the 'lock' remains in place for the pendency of the case, including the period of time that a domain name dispute is appealed to a second level dispute resolution provider if the non-prevailing party elects to appeal the decision.	RySG	WG acknowledges the comment	**No action required at this time**
Recommendation #7:.The WG recommends not to develop dispute options for registrants as part of the current TDRP.				
15.	The BC believes that there must be a mechanism for registrants to initiate proceedings when registrars decline to initiate them. BC supports the details of our position on Charter Questions C that are encompassed into of recommendation #8 and #9	BC	This issue was substantially debated by the WG. The TDRP is a dispute mechanism for registrars – concerned with intra-registrar transfers. The WG	**Recommendation should specify that the ICANN help-site should be clear with regard to what the options for registrants are when**

<table>
<tr><th>#</th><th>Comment</th><th>Who / Where</th><th>WG Response</th><th>Recommended Action</th></tr>
<tr><td></td><td></td><td></td><td>has drawn up a list of used cases that involve intra-registrant transfer issues and recommends that these should either form prat of the implementation of IRTP C or should lead to an issue report for a new PDP concerned with inter-registrant transfers.</td><td><b>their domain has been subject to a suspected non-compliant inter-registrar transfer.</b></td></tr>
<tr><td colspan="5"><b>Recommendation #8:</b> The WG recommends that the GNSO ensure that IRTP-C inter-registrant transfer recommendations are implemented and include appropriate dispute-resolution mechanisms. The IRTP-C and IRTP-D Implementation Review Teams should determine whether the inter-registrant transfer use cases documented in Appendix [?] have been addressed. If there are use cases that have not been addressed by the implementation of IRTP-C-2, the Implementation Review Teams are charged with formulating a request for an Issue Report to review the remaining use cases and consider whether any additional dispute resolution mechanisms (or changes to the TDRP) should be developed. That request should then be forwarded to the GNSO Council for consideration</td></tr>
<tr><td><b>16.</b></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="5"><b>Recommendation #9:</b> The WG recommends that the TDRP be modified to eliminate the First Level (Registry) layer of the TDRP.</td></tr>
<tr><td><b>17.</b></td><td>The RySG is supportive of this recommendation for several reasons. First, as the number of gTLDs and Registry Operators increases, the potential for inconsistencies in the interpretation and administration of the TDRP is likely to occur.
Second, the expense that Registry Operators incur to have staff with the expertise to process and render decisions in dispute cases is not justified by the small number of disputes that are raised at the first level.</td><td>RySG</td><td>WG acknowledges the comment</td><td><b>No action required at this time</b></td></tr>
</table>

#	Comment	Who / Where	WG Response	Recommended Action
	Third, other ICANN dispute policies, specifically the UDRP and the URS, do not include the Registry Operator into the dispute process but, instead, call for dispute resolution providers that have been approved by ICANN as having the expertise necessary to adjudicate domain name disputes to handle disputes. Finally, with the vertical integration of Registry Operators and Registrars now possible, the potential for a conflict of interest exists if Registry Operators continue to be the first level layer of the TDRP. Consistent handling of cases by subject matter experts (i.e. dispute resolution providers approved by ICANN) has the potential to improve the overall TDRP process.			
18.	I would like to encourage the ITRP D work group to consider recommending removing the fees (keep the fines), as they can currently and are seen by us as prohibitive. Registrars starting procedures in vain or without good cause can be warned, fined and ultimately de-accredited based on the RAA. I feel gTLD registries should take more responsibility, in order to deal with this. Ultimately they are responsible for their database, not others, even if it's a thin registry.	Arthur Zonnenberg	WG plans to re-visit the issue of fines in this context	**Re-visit this comment once discussion on fines is completed**
Recommendation #10: The WG recommends that ICANN create and maintains a one-stop website containing all relevant information concerning disputed transfers and potential remedies to registrants. This should include: a) Improvements to the ICANN website regarding the display of information on the Inter Registrar Transfer Policy and the Transfer Dispute Resolution Policy is regularly updated; b) Links to the relevant information for registrants on the ICANN website being clearly worded and prominently displayed on the ICANN home page. This will contribute to improving visibility and content of the ICANN website that is devoted to offering guidance to registrants with transfer issues; c) ICANN Compliance clearly indicates on its FAQ/help section under which circumstances it can assist registrants with transfer disputes. This should include situations when registrants can ask ICANN Compliance to insist on registrars taking action on behalf of said registrant; d) Improvements in terms of accessibility and user-friendliness should be devoted especially to these pages:				

#	Comment	Who / Where	WG Response	Recommended Action
	http://www.icann.org/en/help/dispute-resolution#transfer http://www.icann.org/en/resources/registrars/transfers/name-holder-faqs http://www.icann.org/en/resources/registrars/transfers/text Links to these registrant help-website should also be prominently displayed on internic.net and iana.org in order to assure further that registrants have easy access to information			
19.	In general, yes this is a good idea. But a lot of text on the ICANN website needs to be shortened and simplified, because it still uses way too much text and acronyms to explain something simply. This not only applies to the transfer FAQs which are actually directly linked from the homepage (a good step), but also to the registrants rights and responsibilities, and other policies like WDRP, ERRP or Whois Accuracy Specfication, which are actually not explained to the public at all, while missing / bouncing one of these e-mails means your website and e-mail are disabled within 15 days. *sarcasm on* Always nice to find out when you get back from your holiday, and learn about ICANN the "positive pro-active" way with your domain disabled. *sarcasm off*. Seriously, the ICANN website needs educated text writers who can write in a more accessible way in layman's terms. The registrant impacting policies should have short pages no longer than 1 screen, explaining each of them separately. Answering questions like "Why is this policy here? How does it affect me? What can I do about it?" I fully agree with your recommendations on this point.	Arthur Zonnenberg	WG acknowledges the comment	**No action required at this time**
20.	The term "user-friendliness" should be augmented comprehensively to make it clear that this site should be understandable to a registrant who does not have to deal with such problems on a regular basis.	ALAC	WG acknowledges the comment	**WG agrees to assure user-friendliness is key in this context.**

<table>
<tr><th>#</th><th>Comment</th><th>Who / Where</th><th>WG Response</th><th>Recommended Action</th></tr>
<tr><td><b>21.</b></td><td>In the interests of consumer protection, the BC recommends establishing requirements for registrars to publish information pertaining to transfer dispute resolution options available to registrants. BC supports the details of our position on Charter Questions D that are encompassed into of recommendation #9 and #10.</td><td>BC</td><td>WG acknowledges the comment</td><td><b>WG notes that a centralized depository will provide the most effective information point for registrants. WG members believe that additional requirement for registrars are not practical but agrees to add best practice suggestions to the recommendation.</b></td></tr>
<tr><td><b>22.</b></td><td>It might be helpful if the WG were to specify in more details how to ‘improve visibility and content’</td><td>ICANN Staff</td><td>WG acknowledges the comment</td><td><b>WG agrees to re-visit this issue to clarify the term.</b></td></tr>
<tr><td colspan="5"><b>Recommendation #11:</b> The WG recommends that, as best practice, ICANN accredited Registrars prominently display a link on their website to this ICANN registrant help site. Registrars may chose to add this link to those sections of their website that already contains Registrant-relevant information such as the Registrant Rights and Responsibilities, the WHOIS information and/or other relevant ICANN-required links as noted under 3.16 of the 2013 RAA.</td></tr>
<tr><td><b>23.</b></td><td>It is essential that, in addition to Registrars, Resellers be explicitly included</td><td>ALAC</td><td>WG acknowledges the comment and notes that the reseller has no direct link with ICANN but communication usually flows via the registrar</td><td><b>WG is going to recommend that Registrars pass on the best practice recommendation to their resellers.</b></td></tr>
<tr><td colspan="5"><b>Recommendation #12:</b> The WG recommends that no additional penalty provisions be added to the existing policy. The WG concludes that the penalty structures introduced in the 2009 RAA and the 2013 RA are sufficiently nuanced to deal with IRTP violations</td></tr>
</table>

#	Comment	Who / Where	WG Response	Recommended Action
24.	Financial penalties are almost always efficient when dealing with registrars violating policy. Alternatively, ICANN compliance has enough tools as it is for those registrars unfased by fines.	Arthur Zonnenberg	WG acknowledges the comment	**No action required at this time**
25.	The BC believes there should be penalties for specific violations other than 'notice of breach'. The BC "hopes" that the 2013 RAA will address this issue. BC supports the details of our position on Charter Questions E that are encompassed into recommendation #11, #12.	BC	WG acknowledges the comment	**No action required at this time**
Recommendation #13: The WG recommends that, as a matter of principle, GNSO Consensus Policy should avoid policy-specific sanctions. Rather, it is desirable that the overarching RAA and RA penalty structures be drafted in a way that assures uniformity and consistency of policy violation penalties .				
26.				
Recommendation #14: The WG recommends to maintain FOAs.				
27.	In day to day administration the FOAs are redundant. However, in cases involving unauthorized transfer requests in which the Registered Name Holders's email address has been hijacked, or its access credentials to the control panel have been stolen, the gaining registrar's obligation to obtain the FOA from either the Registered Name Holder or the Admin Contact can help protect the domain names from being hijacked, given the Registered Name Holder's Whois contact information is different from the Admin Contact's. BC supports the details of our position on Charter Questions F that is encompassed in recommendation #13.	BC	WG acknowledges the comment	**No action required at this time**
28.	Here's the only issue we disagree on. In the report 5.2.6.1 Observations are made by ICANN compliance, that "FOAs are essential to help resolve the dispute and to reverse it if appropriate. It is for this reason that ICANN Compliance also	Arthur Zonnenberg	The Working Group thanks Arthur for his thorough comments. The FOA process would	**Assess the current use/role of EPP and establish how the FOA adds to this process**

#	Comment	Who / Where	WG Response	Recommended Action
	expressed its support for maintaining FOAs, reasoning that its continued use may help prevent hijackings in certain cases or serve as evidence in disputes." Yet no examples or numbers are given where the FOA made the difference, above and beyond the AuthInfo code. Why should compliance dictate the rules for 250.000+ successfull transfers per month based on a couple of disputes? (see the .com registry report for november 2013, com-transactions-201311-en.csv from http://www.icann.org/en/resources/registries/reports/com) If there are 500.000+ failed transfers each month (timed out waiting for owner approval), isn't that a far bigger and more serious issue than a handful of hijack cases? Let me inform you that the FOAs are our single most common source of pending orders costing time and often revenue in our registration systems. The typical way a gTLD transfer proceeds - as James Bladel describes in the full report - is somewhat incomplete. Please allow me to add important elements to it pertaining to the FOA and other relevant elements: a) A Registrant sends a transfer request to the new registrar ("Gaining Registrar"); b) The Gaining Registrar provides instructions to the registrant, incl. get the AuthInfo Code from the current registrar ("Registrar of Record"); including unlocking the domain name and updating the admin-c email address. c) After confirming the Registrant and/or Administrate Contact email address, the Gaining Registrar sends the FoA to the Transfer contact; and confirming the domain being unlocked and the auth code being reported as retrieved. d) The Transfer contact confirms the FOA and sends the AuthInfo		benefit from improved streamlining The transfer process differes between registrars as some do not 'lock' domains and so there is no need to 'unlock' WG argees that FOAs are used only for a very very small number of disputed transfers. Registrars should look into ways to improve the user-friendliness and usefulness of FOAs The FOA is the only stat where the domain holder actually is involved and there needs to be something where the domain holder actually has to take an action to effect the transfer. Getting the affirmative approval of the transfer is what the role of the FOA provides whereas	**Working GROUP to discuss the benefit vs. the burden of the FOA**

#	Comment	Who / Where	WG Response	Recommended Action
	code that was obtained from the Losing Registrar to the Gaining Registrar; No, typically the transfer times out the first time, because the registrant has no idea what to do with the FOA. Then the domain is locked after time x for typical "safety reasons" by the losing registrar, and you first have to inform the transfer contact to unlock the domain again. Often the losing registrar will have updated the AuthInfo code "safety reasons", leading to many failed gTLD transfer with the wrong (previous) AuthInfo code. Most transfer contacts (customers) give up, you don't hear about them and you don't see them in the statistics. The FOA is a primary reason for this. My careful estimate is that the number of failed transfers are at least twice the number of successfull transfers. e) The Gaining Registrar requests the transfer and sends the AuthInfo code to the Registry; If your customer is a seasoned or thoroughly instructed and persistent Transfer Contact, then yes. f) If the domain name registration has no status that impedes the transfer (e.g., client Transfer Prohibited) and the AuthInfo code valid, the Registry sends notice that the transfer is pending to the Gaining and Losing Registrar; That's a big if. Often a domain does have an impeding status, even if it was removed before. The domain lock client Transfer Prohibited is also a primary reason for transfer contacts (customers) giving up. g) The Losing Registrar must send an FOA to the Registrant. However, the transfer is not depending on this step. It's a big shame the losing registrar does not actively ACK to reduce the 5 day waiting time, which is a long time and wasted time is wasted money. For large teams building big websites, this is costly. h) After 5 days with no objections ("NACK"), the transfer is complete. And all kinds of winbacks of		the auth info code is really just a key that a lot of people could know the key to that domain name is under the doormat	

#	Comment	Who / Where	WG Response	Recommended Action
	transfers can still occur. But usually yes you're done. However, if you as a transfer contact have to update your admin e-mail address, while at the same time unlocking the domain and requesting the auth code, some registrars (NetworkSolutions, Ascio, ...), trigger additional "safety measures" leading again to transfer contacts giving up. You have to phone call them to tell them you're leaving. Per domain name. Or you have to confirm the FOA from the losing registrar or they will NACK the transfer by default, even if they have no right to, and they'll typically only do it once. Per domain name. The effort that goes into contacting legitimate registered name holders, explaining to them this "extraneous" step they need to take, after it has already failed once, means any gTLD transfer typically takes 3 weeks for those unaccustomed to the process. That's after a delay of 2 weeks before even starting with the FOA, telling customers to unlock their domain name first and get the AuthInfo code. Even those end users that have experience, often forgot which email address they used at some point in the past to register those domains, or forget 1 step and face failed transfers and more delays due to 5 days waiting time per transfer attempt. A lot of providers as resellers still enter their own email address instead of that of the end user, and you have to time the new attempt to transfer and inform the end user to chase the losing provider/reseller to cooperate, because they will ignore the email whenever they can. Again leading to transfer contacts giving up. Let's stop kidding ourselves. An authorisation is an authorisation. And the majority should not suffer from the minority. A trust model is possible, where gaining registrars are trusted in the			

#	Comment	Who / Where	WG Response	Recommended Action
	transfers they execute with valid AuthInfo codes. In the case of abuse or dispute, it should be easier to complain, rollback and fine the abusing registrar. The original registered name holder should be retrievable and verifiable after one or more transfers have been made, where the original registrant can prove their identity and say: "I want my domain name back, it has been hijacked." FOAs add nothing to this. If as a hacker you can get access to the auth code and unlock the domain, the email address is a piece of cake since you can update it via the same registrar control panel. Please read this article: http://gizmodo.com/how-i-lost-my-50-000-twitter-username-1511578384 Currently 3 factors are required for 1 successful transfer (unlock, FOA + email address, auth code), where every factor beyond the auth code does not add either authorisation or true security. All 3 are often accessible through 1 control panel or email address. It's actually possible to have domains unlocked by default. In that case, locking and unlocking your domain name could be a 2 factor authenticated process (identification documents, phone calls for identification, hardware or software tokens uniquely linked to a personal secret, etc.), so it would actually add security. Currently the clientTransferProhibited has been watered down in my opinion compared to what it could be. The more difficult you keep gTLD transfers, the less competitive the market will become. GoDaddy is the biggest registrar here, and the more factors they can keep to prevent transfers away, the more business revenue they can and will protect (see transfer contacts giving up above). The same can be said about the other large registrars. They might say it's all about security and safety,			

#	Comment	Who / Where	WG Response	Recommended Action
	but really it isn't.			
29.	ICANN's Contractual Compliance addresses unauthorized transfer complaints with both the losing and the gaining registrars. - The losing registrar is requested to provide evidence that: -The AuthInfo code was sent to the RNH (or retrieved from the control panel). -The FOA was sent to the RNH. - The gaining registrar is requested to provide evidence that: -The FOA was sent to a Transfer Contact. -The FOA was confirmed by a Transfer Contact. Concerning the AuthInfo code, the vast majority of registrars provide time-stamped logs of when it is retrieved from the control panel. These logs sometimes identify the email address used to request/send the AuthInfo code as shown in the following examples: Example 1: [domain name] [agentXXX] [jonhdoe@example.com] [2014-02-01 21:43:58] Example 2: 2013-07-06 23:05:11 john.smith@example.com jonh.smith@example.com 112.126.127.63 However, some other times the logs only display User IDs. The	ICANN Compliance		

#	Comment	Who / Where	WG Response	Recommended Action
	email or name used to identify the registrant are not shown: Order ID: 123456789 User ID: 987654321 Originator User ID: 987654321 Order date: 2014-04-04 20:34:45 At times, registrars state that their systems provide the code instantaneously upon request and do not retain time-stamped data for the release of the AuthInfo code. Without the FOAs, the only evidence available for Compliance to determine whether registrars comply with the IRTP would be logs that do not include RNH or Administrative Contact identifying information from the Whois of the domain names or no logs at all. As a consequence, ICANN's Contractual Compliance would not be able to properly investigate unauthorized transfer reports. Considering that TDRP proceedings are only to be initiated by registrars, users will be left with no other option than to initiate legal proceedings to dispute a transfer. Further, ICANN notes that the registrant is often not the only one with access to the control panel. Many times, the control panel is managed by a third party, such as the website developer or the reseller. In these cases, without the FOAs, the AuthInfo code can be retrieved and the transfer completed without the knowledge or permission of the registrant. In addition, FOAs are also used as evidence by registrars while working amongst each other to resolve the matter; and by registries and dispute resolution providers, while investigating TDRP proceedings.			

#	Comment	Who / Where	WG Response	Recommended Action
Other Comments				
30.	Overall, ALAC strongly supports the recommendations of this Initial Report	ALAC		