ICANN75 | AGM – Transfer Policy Review PDP Working Group
Saturday, September 17, 2022 – 10:30 to 12:00 KUL

UNIDENTIFIED SPEAKER: Hello and welcome to the Transfer Policy Review PDP working group session. Please note that the session is being recorded and is governed by the ICANN expected standards your behavior. During the session, questions or comments submitted in chat will be read aloud if put in the proper form, as noted in the chat. If you'd like to ask a question or make a comment verbally, please raise your hand. When called upon, kindly unmute your microphone and take the floor. Please state your name for the record and speak clearly and at a reasonable pace. Mute your microphone when you are done speaking.

This session includes automated real-time transcription. Please note the transcript is not official or authoritative. To view the real-time transcription, click on the closed caption button on the Zoom toolbar.

To ensure transparency of participation in ICANN's multi-stakeholder model, we ask that you sign into the Zoom session using your full name. For example, a first name and last name or surname. You may be removed from the session if you do not sign in using your full name.

With that, I'll turn the floor back over to the chair, Roger Carney. Please begin.

ROGER CARNEY: Thanks, and welcome, everyone. I'm going to try to leave my mask on. So if I don't come across clearly, just let me know. And I can remove that to hopefully help for that. But again, welcome everyone that made it here to Kuala Lumpur and those who are online participating as well.

Before we jump into anything, we always start every meeting with stakeholder comments and everything. So I'll open that up. If there's any stakeholder groups that went up providing comments or from suggestions or meetings that they've had, I'll open the floor up to any of the stakeholder groups that want to mention anything.

Okay, again, we'll try to do that at every meeting just to give everybody a chance to bring in questions or comments from their stakeholder groups. Hopefully this group can answer get those answered for them. I think from that, I don't have anything else.

We're going to focus today on the gaining and losing FOAs. Hopefully we can make good progress on that. We've got a lot to cover. We started that on Tuesday. So we got a good base to jump from. But I think we've got to get into it a little deeper. But I think I will turn this over and we'll do a brief public introduction and everything. So hopefully we can keep that small so we can get jump into our work. Emily, please go ahead.

EMILY BARABAS: Thanks, Roger. Hi, everyone. This is Emily Barabas from the ICANN Org staff team. As we traditionally do for these sessions, we tend to give a little bit of a background to the PDP for those of us who are visiting and new to the subject matter. We're not going to go through everything. There's a lot of backgrounds that could potentially be useful. But this will hopefully allow you to follow the conversation a bit. And if you're interested in the subject area, and you are new to it, please feel free to come to the staff team after the session and we can help connect you with additional resources for more information. So as I said, this will be quite brief, but hopefully helpful as context. Next slide, please.

So what is the transfer policy? As many of you know in this room, it’s an ICANN consensus policy governing the procedure and requirements for registrants to transfer their domain names from one registrar to another. Key goals include domain portability, greater consumer and business choice, and allowing registrants to select a registrar that offers the best services and price for their needs.

The policy was originally called the IRTP—inter-registrar transfer policy—and went into effect in 2004. And the GNSO has gone through one policy process previously, a series of policy development processes, IRTPs Part A through D. Next slide, please.

There are quite a few issuers with this PDP and a phased approach has been used. So we've recently produced or the group has recently produced a Phase 1A initial report that went out for public comment. You can see here on the screen the topics that were covered there. During the time that the public comment period was happening, the group did some introductory deliberations on Phase 1B, which focuses on change of registrant. And then now that the public comments are in for Phase 1A, the group has focused back on reviewing those comments, incorporating the feedback into any potential revisions into the report. And then we'll return to Phase 1B to continue those deliberations. There will be a final report out of Phase 1, and then there will be a phase 2 of the work as well. And I think that I've mostly actually already covered that. So I think we can go to the next slide.

So the focus of today's session is going to be on forms of authorization or FOAs, the gaining and losing forms of authorization. And so just for those who are new to the topic, we'll briefly define those so that you can follow along. So we'll use the terms gaining registrar and losing registrar in this session. The gaining registrar is the registrar to which the registrant is transferring a domain name where the losing registrar is the registrar from which the registrant is transferring the domain name. And the gaining formal authorization is a required form sent by the gaining registrar to the registered name holder to confirm that the RNH or registered name holder does indeed intend to transfer the domain name. This has typically been an email to the RNH to confirm the intent to transfer by clicking on a designated link. And before the GDPR, that transfer could not occur without this confirmation. The losing form of authorization is sent by the losing registrar to the RNH. It's a notice to confirm the RNH's intent to transfer and without an objection to the transfer within five days, the losing registrar will process that request. Next slide.

Most of the recommendations from this report really need to be taken as a package. And it's very important to look at all of the recommendations together and there's quite a bit of interplay between them. But just to give a little bit of context, the working group has recommended as part of its recommendations to essentially remove the requirements from the transfer policy to have these gaining and losing FOAS, and instead has recommended a series of additional measures to replace those notifications. So this includes notifications to the registrant about changes that are happening to the account specifically around transfer as well as a number of new measures around the transfer authorization code or TAC.

So I think that that's all the context we're going to provide for those who are new to the subject area. I think a lot of the people in this room and those joining us on Zoom already know quite a little a lot about this subject. So I'll just pause for a moment in case there are any questions.

Okay, so that's it for our intro. So the subject, as Roger said, for today is to dig a little bit more into the feedback that has been received for recommendations 1 and 2 through public comment. And I think what we'll do, then, Chantelle, if you want to stop sharing the slides, and what I'll do is bring up the working document for the session. Okay. And this is rather tiny on the big screens. So it's helpful potentially to follow along in the working document itself.

During last week's working group call, hopefully those who were not able to attend were able to catch up with the recording. There were some folks already in transit. But briefly, we have for each of these recommendations a full summary document that gives you all of the comments in full text, and I'll share that as well.

The expectation is that all of the working group members have read and reviewed all of these comments in full so they have the full context and understanding of the input as it was submitted.

But because it's hard to be flipping between the pages and between the documents during these sessions, the staff support team has attempted to at least create something that's a little bit boiled down to look at as we go through the discussions—not at all a substitute for the original comments, of course.

And on the last call, we also went through some sort of key principles for this public comment review. So I'm not going to read through those, I'm not going to go through them in detail. But please do take a look at those if you're not yet familiar with those or miss last week's call.

So what we started to do—it wasn't even last week, it was Tuesday, only a few days ago, was to go through this first set of comments. And we've captured some of the key points from the discussion that can hopefully act as a launching point for today's discussion.

So as you can see here at the top of the screen and as we discussed yesterday, there was a number of comments, both from registrants and also from groups that are referenced in the right-hand column here that centered around a specific theme for the losing FOA. And that is that domains are an important and valuable asset. It's important for registrants to have a real opportunity to approve or reject a transfer before the transfer takes place in all cases. And it appears that in some cases, under the new procedure, the transfer will have already taken place by the time the registrant has received the notice and wants to take action on it.

The working group's proposal eliminates this. And it's an important security check, therefore increasing the risk of the domain being stolen without the knowledge of the registrant. And in particular, when someone has access to the TAC to initiate a transfer that the RNH doesn't want.

And Roger, I think we'll just briefly go through what was discussed last week. And I think we'll continue to go through the first few points of this, and then Roger will kind of get some additional inputs from all of you on these comments. So again, here, this is not quoted from any of the text, this is really just sort of the theme that exists in some of these comments to help the group discuss.

So in the initial discussions last week or on Tuesday, what we saw is that the working group members who spoke on the call did not believe that there was new information necessarily being introduced in these comments, that there was previously discussion about this point of view. But while the recommendations may be appropriate, at this time, and the language of the recommendation itself is okay, the rationale may need to be further expanded to explain specifically why the recommended approach is considered appropriate and why it provides the necessary security to registrants.

A few points that were raised during the call is that it is the first and most important line of defense and the main point of control is the point of logging into the account of the registrar. And from the working group perspective, that is essentially the affirmative consent to initiate the transfer. And once an attacker has logged into the control panel, they can change for example, points of contact, including who would be receiving the losing FOA or the notifications. And therefore once that's happened, that essentially eliminates the utility of the FOA or those notifications, because it's going to the attacker or to a different email address. This is true in the current scenario, but would also be true in the notification. So that's roughly equivalent. And the properties are similar.

Another point that was raised on last week's call was that the TAC is generated on demand and therefore less vulnerable to theft. And that's a really a significant difference between the FOA as it exists today, where it's out in the clear for long periods of time, as opposed to the future state that's recommended by the package of recommendations.

It was also noted that the losing registrar still has five days to provision the TAC and that it's a business decision that registrar has at their discretion to delay provision and take additional steps including performing due diligence. So registrars will make a decision about if and how they use that period of time, depending on their own business practices as well as the value of the domain. And that due diligence can give extra protection to the registrant and also give the registrar more time to respond to the notifications to the extent that they are receiving those notifications. And registrants themselves will have the choice to pick a registrar that fits their needs.

Working Group members also mentioned the proposed 30-day post transfer lock helps to ensure that if a domain is stolen domains, domain hopping will be slowed, allowing the losing and gaining registrars to work together to resolve the problem. So I think these are some of the key points. And actually, Roger, do you want to start the discussion? And I will follow up with the other comments in just a moment.

ROGER CARNEY: Thanks, Emily. Yeah, and again, we were recovering what we discussed on Tuesday, mostly just to give a background and everyone here probably knows what was talking about. But again, I think that a lot of these comments that came in on the losing FOA and even on the gaining FOA kind of are interrelated. So we wanted to not pick a comment, but kind of get the comments out there to everyone so that they can think about them as a whole, and how that affects everything. So before we jump in, I see that George has his hand up. George, please go ahead.

GEORGE KIRIKOS: I just want to point out that I really disagree with the analysis that took place on Tuesday's call. As you know, I submitted very extensive comments, 60 pages worth, which went into great detail on issues that were actually not raised in the report. And for the group to just summarily say that there was nothing new is something I really disagree with.

And I want to point out a few specific examples, because people on the call said they would be able to refute the topics if they wanted to, which they never actually did. On page 39 of my comment, I actually quote from the SSAC report, SAC040, which literally said that you should treat transfer attempts as a security event. It says check and recheck. That's a little quote, on page 39 of my comment submission, and I made it in bold yellow text, yellow highlighting. And that really speaks to the need to preserve the losing FOA.

I also presented statistics from the Canadian mobile phone industry, where unauthorized ports were reduced by 95%—that's real data—using what's the equivalent of a losing FOA. And that's on page 36 of my comment submission. And similarly, ARIN’s procedures have a confirmation step.

And to say that these are not new, I really disagree with that. And one of the proposals I made as a counterproposal was retaining on an opt-in basis the losing FOA, I called that the best of both worlds proposal, and I did a twitter poll, and only 12% wanted to retain only the option that the working group proposed, which is basically elimination of the losing FOA. 24% would want to use the current system, which preserves the losing FOA, and 63% wanted a choice of both.

Obviously, that's not a scientific poll, but it really speaks to the need for the choice that registrants want to have the extra security if they need it, because the working group seems to focus on, as noted in the slide, that control panel access is all you need to prove security.

In a properly designed registrar system, you would have confirmations and have separation of the logins and the email address of the registrant. And I described in my own comment how I actually do that at Tucows.

And to say that the attack scenarios are being handled properly is totally incorrect. And to give one specific example of how the losing FOA would actually protect one, I gave an example on my blog today and it's in my comment as well, comment submission.

All the focus is on—there's actually no security once the TAC is generated. Basically, the registrant is on their own at that point. And so for security scenarios where the TAC is compromised after it's generated, your proposals do absolutely nothing, whereas the losing FOA would protect one in that scenario.

So let's suppose that I want to sell a high-value domain name to somebody who wants to transfer it to GoDaddy. Part of that process would involve giving them the Auth Info code, the TAC as it’s been renamed. And so I can generate a TAC legitimately in my registrar control panel without it being hacked. And then, after it's generated, it can somehow be compromised. Either the buyer or the escrow company, it's somehow compromised.

And so instead of being transferred to GoDaddy, that TAC is used at a Russian registrar or Alibaba in China. If you eliminate the losing FOA step, that's the end of the story, the transfer completes immediately. Whereas under the current system, I can actually see where the transfer is going to as part of the losing FOA. It says there's a transfer request from GoDaddy or there's a transfer request from Alibaba. And that's an important safety mechanism that the working group seems to ignore.

And so I hope that you listen to the comments that were submitted, because they are new, they are things that the working group hasn’t considered. And I know that the [ICA] supports me on many of these things as well. Thank you.

ROGER CARNEY: Thanks, George. And just to be clear that I agree with George's last comment there that there are some new things in our comments. And to be clear, on Tuesday, the group didn't say there was no new comments. I think one individual may have said that he didn't see anything new that he thought about, but I just want to be clear that the group didn't decide that there were no new comments here. And again, I think to George's point, there are a few new comments that spurred discussion and that's why we're here. Okay, any other comments? Emily, did you want to run through the rest of them?

EMILY BARABAS: Sure. no problem. Okay, so just a couple of other items that were discussed on the last call. One of the concerns raised was that the recommendation may prompt registrars to take what's called a backdoor security measure by the commenter, by delaying the time between people asking for the TAC, and the time in which it's issued, which, from the perspective of the commenter would ultimately burden domain registrants because they would not be able to complete the transfer process in one sitting.

And in those initial discussions, working group members noted that they see that optional delay as more of a feature than a bug in certain ways, because it would allow, as we discussed during the last block, it would allow the registrar to, as a business decision, take additional due diligence measures or other steps during that period, potentially adding an additional level of security for the registrant, and that the registrant could ultimately pick and choose or registrar based on their own judgement of the importance of safety measures versus other considerations and so forth.

And again, here, these summaries, I just want to note, are from our notes from the call. If they're wrong, it's totally possible that there's things we missed, there's things we didn't capture correctly. So that feedback is also important from all of you. And these are also, again, just initial points and not the final decision of the group.

The next thing that was discussed was a comment specifically referencing RFC 9154. And a quote from the definition section, stating that a transfer is coordinated by the registrant to transfer the sponsorship of the object from one registrar to another. And the respondent felt that the recommendations were not consistent with that statement.

In initial discussions, one of our working group members, Rick Wilhelm, who's one of the coauthors of RFC 9154, noted that he didn't feel that indeed, the RFC was making a normative statement that would impose any policy obligations on the ICANN process and that in addition to that, the registrar is still coordinating the process within the proposed recommendations, so he didn't view an inconsistency there. So, of course, Rick, please feel free to fill in any gaps if you're here.

So I think that that was the initial response to that one. Next one thematically was about TAC security. And we're going to be talking quite a bit more about TAC security in some of the additional recommendations. But this was sort of in the context of losing FOA so it's included here as well, that measures to increase security of the TAC are insufficient to justify elimination of losing FOA, that the TAC is an extremely valuable asset that is vulnerable to theft or use by third parties once it has been generated, and that the working groups recommendations to strengthen elements of TAC security do not address this vulnerability.

We'll talk about that some more as well when we get into Recommendation 1. But the initial discussions on Tuesday centered around some comments that with the new recommendations, the TAC will be generated on demand. So focusing on that element of it and the additional security that's provided there, as well as the limited amount of time that the TAC is available, so the TTL of 14 days and that that creates a significant improvement to the security of the TAC. While it can be stolen once it's generated, working Group members noted that this is the case in the current environment as well.

And then there were a couple of additional data points that had been suggested in some of the comments, specifically, number of NACK transferred as listed in the transfer policy status report. I think that that was actually from the first comment, that was the one that was discussed, there was also suggestion of data on Canadian mobile phone number transfers and thefts, ARIN’s procedures for the transfer of IP addresses and SSAC advice including SAC 40, 44 and 74.

I think the only one that had been discussed in depth so far was about the NACKed transfers. And one of the points that was raised in the initial discussions was that the total number of NACKed transfers can't necessarily be used to evaluate the number of domain names thefts because there are different reasons that NACKs may take place.

And then the additional suggestion for data was that data from registrars could potentially be gathered to look at how many times customers tried to stop fraudulent transfers after receiving the FOA. And I don't believe there was a deep dive into that suggestion yet, but it was included as well. So Roger, shall I pause there, and then we can dive in a little bit further? Thanks.

ROGER CARNEY: Great. Thanks so much. And again these comments aren't necessarily all the same thing. But they are, I think, when you look at them, driving to a very similar issue. And even if the comments themselves didn't say it, I think the big deal here is the call out—and we discussed this during our Phase 1A discussions.

In today's policy, there's two five-day windows. And in our recommendation policy, there's one five-day window. And again, in today's policy, there's two separate needs for that five-day window. The first one was to generate the current auth code and provide that to the requested transfer. And the second five-day window was the notification window of pending transfer. And it allowed registrant to ACK or NACK it. And I guess we can say that better than that, acknowledge and accept the transfer or deny that transfer, I should say, to get rid of the terminology there.

And I think that that's what—if you look at all these comments, that's what they're drilling into is, today's current policy provides explicit window for both of those activities and our recommended policy, there are not two explicit windows for that, there's only one window upfront that can be used for both of those effects. And we don't say specifically that it has to be used in a specific way. And I think that that may be where a lot of the questions are coming in.

And again, valid concern that the registrant from a policy perspective is looking like they lose the ability to deny a transfer. And again, I think that during our Phase 1A discussions, we had this discussion, and that first five-day window can be used for both of those effects, if the registrar wants it to.

And again, some of these comments, if you look at them—and that to me, everybody says the Leap of Faith document was large, there was a lot in there, but I think it was a fairly easy read. And there were a couple ideas in there that I think are useful to spin in this group. And probably the biggest one is the idea of the transfer starting in the reverse way, starting at the gaining registrar.

I've had some discussions over the past few weeks since I saw this comment. And I know some registrars have looked at this prior to this, but I know that this group didn't talk about that during Phase 1A looking at, is there an ability, and does it make sense to start a transfer at the gaining registrar?

So I think that that's a call out from the Leap of Faith document that we can take a look at. And the other one that I don't remember focusing specifically on the Leap of Faith, I saw multiple places, I think, was possibly a registrar-registrants opt-in, opt-out kind of idea of yes, let me transfer this as fast as I can or no, let me acknowledge it first kind of thing. And I think both of those were topics that we never covered in Phase 1A. So I think that that's two good things to talk about and look at and see if that makes sense or not. So I think that's why the homework was assigned Tuesday, specifically calling out these ideas. So I think that anyone that has any thoughts, please come forward. And let's discuss those proposals. Thanks. Zak. Please go ahead.

ZAK MUSCOVITCH: Thank you. I want to talk about possible solution to the issue. So Leap of Faith provided several proposed solutions. I'd love to hear from registrars whether they think they're feasible or not. I don't have the technical expertise or background to determine that myself. So those are potentially viable solutions.

But for myself, I'd like to focus on the existing solution to see whether it can be tweaked or not to satisfy maybe not everyone, but more people. So the elimination of the five-day window is perceived as problematic for registrants.

Registrants like to be able to NACK. We can explain to them that, listen, once the control panel is penetrated, all bets are off. But there's still this hesitancy. Maybe we got it a bit reverse. Maybe because we're supposed to be establishing minimum standards, we should have the default the five days, and then registrars can roll that back to zero if they like. That could be a possible solution.

But that still leaves the issue that George mentioned, not being able to identify the registrar that the domain’s been transferred to.

Also in his public comment, he mentioned that maybe we can build that into the TAC, the identifier of the receiving registrar. So that might actually be able to maintain the existing proposal as is. There's still a five-day window by default, but registrars who may be providing additional security mechanisms beyond that are able to roll that back to zero and instantaneous if they want to.

But we are setting minimum standards for registrars and perhaps that's the prudent approach and then tweak the TAC in order to be able to embed within it an identification of the receiving registrar.

Now, again, I don't have the technical expertise that you all do who are working at registrars, so I'd love to hear your feedback on that, genuinely as a proposal, but also, I don't want to lose sight of the more dramatically different proposals that Leap of Faith also canvassed in its comment. Thank you.

ROGER CARNEY: Thanks, Zak. And just to be clear, again, I've always thought about this when I was talking about in Phase 1A, I don't think that we're eliminating the five-day window. We're combining In them, and it's made it to be a flexible choice, a business choice of the registrar to implement or not.

And I think what Zak is saying and some of the comments may have alluded to is, should that not be flexible as it is, but more mandatory that when a request for transfer is made, a notice has to be sent?

We talked about this in phase one. We talked about what notifications were necessary. We talked about specifically this notification and said we didn't think that it needed to be mandatory. And again, I think that what we're talking about is there's comments coming in that are suggesting that maybe it should be mandatory, and that discussion should be open to that effect.

So again, I just want to be clear, I don't think the five-day windows are eliminated, they were combined and made as a flexible option. But should it be that the transfer request actually does send a mandatory notification?

Again, Phase 1A, we talked about it and we said no, it wasn't mandatory. Registrars can do that if they choose to or not. So I think that that's a valid question to ask. And I'd like to hear others' comments on that. Keiron, please go ahead.

KEIRON TOBIN: Thank you. Didn't we also discuss when you request like—so when you make the transfer for raw data and things like that, the gaining IANA ID was also on there as well, which [would be replaced] rather than the current registry logging code? That was something else that we also discussed.

So just to reiterate that as well, that there would, if we—I think that needs a bit more work in the second level. But that would also enhance security in terms of where it was going, and hopefully would help towards George's point as well. Thank you.

ROGER CARNEY: Great. Thanks, Keiron. And actually, I think we'll cover that specifically later. It was actually a question call out. And I think that we specifically made public comments to talk about if that made sense. But yeah, Keiron, you're right, we did talk about if that should get sent along, instead of, again, the technical reasons of each registry has their own database and can call the same registrar—it can have a different ID at every registry, but there's only one IANA ID for that registrar. So that was the discussion, was, could that be useful? And that was actually a question posed in public comment. So we will cover that more in detail.

So, but yeah, I think Zak has hit on—and I think that registrars should probably step up and say, okay, does this make sense? Is there a middle ground here? It doesn't make sense to maintain—or a mandatory maintaining of the acknowledgement window.

Again, I know that we've talked many times, and just last Tuesday, that, yes, we are talking about a small number of transfers, but typically it's a big impact, no matter how you look at it. There's hundreds of thousands of transfers a year that go through fine. No one says anything. We're talking about the few and how to better support that.

And again, you can look at it as a funnel and all these transfers, yes, many work well, and then you get down to, okay, there may be something was compromised, and you don't even know if it was the account holder or if it was something else that just went wrong. Someone's email address maybe got hacked, and they're in their email getting it also.

But again, I think that's a small number, but I think it's worthwhile to look at and say, okay, does a mandatory transfer request, does it provide a mandatory window there or, again, as we suggested, leave that optional for registrars and their business models. And obviously, you'll have different security risk profiles that a registrar can handle and support customers or registrants that don't feel that they need a high level of protection and can get it from a different registrar to those registrants that want a high level so they pick a different registrar and use their system because it provides that. So thoughts from registrars? George, please go ahead.

GEORGE KIRIKOS: Yeah. I understand the argument about picking your registrar for better security. My issue is though that that's all good and fine up to the point that the TAC is generated. It's completely ignoring the security attacks that can take place after the TAC is generated. And so that's why you need to retain the ability to keep the losing FOA, because at that point, your choice of registrar won't matter anymore. The TAC is generated, and then the registrant is on their own. And so I just wanted to make that quick point, because it seems to be missing from the analysis. Thank you.

ROGER CARNEY: Great, thanks, George. Any comments, suggestions from registrars on stepping in the middle, or registries? Anyone? Rick, please go ahead.

RICK WILHELM: Thanks, Roger. So I think that one of the things that we need to think about is what are we talking about as a practical matter, because when we were working on 9154, one of the things we envisioned was that registrars might vary the TTL of the TAC even down to a domain name basis, based on a risk analysis of the value of the domain name registration.

So when we talk about these things, the TTL is really, the TAC is really something that's closer to the kind of like when you would get a notification on your phone that you've got a Login PIN or something like that, when you're logging in to do something at an account.

And so whereas the auth info code, of course, was created probably when the domain got registered, and it's just sitting out there ambiently, stored in a whole bunch of databases. The TAC is ephemeral, very short lived and maybe had a lifetime of down to like 5-15 minutes, depending on if you're transferring a very valuable domain name. Like, let's say, icann.org or something like that.

And so the notion of wanting to transfer names fast, super fast, normal, slower, I think, was thought of in terms of the TTL being shortened down to very low levels, is the way that I've always thought of that sort of a thing. Thank you.

ROGER CARNEY: Great. Thanks, Rick. And again, I think it goes back to what Emily finished her introduction of the slide deck with, is the majority of these recommendations go together, not as an individual solution. So you have to look at the whole package. And as Rick mentioned, the TTL helps there. And the flexibility with the TTL also helps registrants restrict that window even further. And again, I think all the notifications help this process.

So it is something that we have to look at and look across all recommendations. But again, I think that our focus here is for this working group to look at the sets of comments. And again, when you look at them, there's a lot of comments in here, but they're really drilling down to the fact of the perception that the registrant is no longer getting an explicit five-day window. So I think that that's what we need to focus our discussions on. Thanks. George. Please go ahead.

GEORGE KIRIKOS: Yeah, this emphasis on the RFC 9154 being some huge improvement, that analysis is incorrect, because it's focusing again on the length and complexity of the transfer authorization code, TAC, the lifetime of that TAC. But once again, it doesn't actually prevent the TAC from being used in an unauthorized manner at a different registrar. And so this idea that it's some big improvement is completely erroneous, in my view.

And in my counter proposal, which I called the breakthrough proposal on page 11, Section E of my comments, I showed that you could have a completely public and completely insecure alternative as to a code in terms of where the domain is being pushed to. Instead of some 32-character mix alphanumeric and symbols, you can literally have what I call the PTID the pending transfer ID of one letter, the letter A.

So the counterproposal was you go to the gaining registrar, you generate a PTID, and then you go to the losing registrar and input that PTID. And so the TAC scenario has to be that somebody at a different registrar has to generate a different PTID and convince you to use it at that registrar. So, if you go to GoDaddy, I make a PTID of, say, example.com, ABCD. I take that to the losing registrar and I have to type in that code to complete the transfer. I'd still want to retain the losing FOA.

But for an attacker to be successful, they have to convince me to type in their PTID, which is Alibaba-1234. And so you can have a completely auditable perfect audit trail, you can actually score this PTID, it's a complete improvement compared to this idea that you want to keep a valuable secret.

As we know, from all the hacking attacks, if you make a high value target, people will try to obtain it. And so my solution, counterproposal, totally flips it on the head. You can have actually a public address of where you're going to transfer to. The TAC scenario becomes completely much harder to implement under my approach. And so I hope it's taken seriously because these improvements that you call improvements are actually not improvements. Thank you.

ROGER CARNEY: Thanks, George. Yeah, and we don't need to get into an argument about how much it improved or not. I think that when you look at the suggested changes to the auth info to the TAC, and actually 9154, I don't think mentions TAC but I don't remember, the improvements are there, because we know today in systems out there that there are auth codes generated by the registrars—and we know this, that are password1 on domain names, and they put them on there at create, and it stays there until someone transfers it somewhere to a different registrar that updates it, or the registrant would go in and update it.

So I think that we are talking about improvements. And when you start adding in the improvements that the policy is suggesting, you do start to see a large improvement over the current system of an auth code that can live forever versus a transfer authorization code that is only valid for so long post request. So we do see an improvement there. And if you don't like—big improvement or small improvement, to me, it doesn't really matter. It's where we're improving the system. That's what we're here to do so.

But I still think—open this up to anyone that sees issue with the current recommendation of dropping the losing FOA completely. And again, when we were discussing this in Phase 1A, I didn't see it as dropping it. But obviously these commenters see it that way. And I think that that's important for this group to either respond with an update to the recommendation or respond with language that explains how it's not what they believe it is, because these commenters believe that the registrant is losing control that they have today. So I think that's what this group has to get to. So Jothan, please go ahead.

JOTHAN FRAKES: I think the key thing here that we lose out on is registrants don't spend their lives logged into their registrar or really want to. They kind of set and forget their domain name. And the way the current FOA works, they will receive from their current registrant a notice that says, "Hey, your domain's about to move registrars. Click here to stop it."

And the way the new method works, they might get a notice that says, hey, the security code was set. That may not register with people to understand what that is, and then they'll get a subsequent notice that, hey, your domain has moved to another registrar. And there's no agency on that registrant to do anything to stop it.

And I'd say that a lot of registrants don't log into the registrar very frequently. And there's an opportunity lost here to have an ability to act upon a notice. And that's what I think a lot of the issue is here. I know we're trying to remove friction in the way that the transfer happens. But I think that's where the majority of the resistance to the change of losing that FOA and the NACKing opportunity come from, if that adds any color or is helpful. Thank you.

ROGER CARNEY: Great. Thanks, Jothan. Okay, any other comments? Again, we need to solve—either increase language to explain this better or find a different path here. Again, this was probably the number one commented recommendation. So we've got 22 recommendations. And fortunately, many of those were not highly questioned or commented on. But there are a couple that we need to really get into it and get into the details. And I think that obviously, this is one of those. Zak, please go ahead.

ZAK MUSCOVITCH: Thank you. So Roger, just in terms of if we're going to keep the existing approach, which I don't know if we are, but if we do, and improving the explanation of it, I just want to point out something in Section 3.2 of the initial report. I'm not sure if staff is able to put it up. They're amazing. But it might be just too short notice for them now.

But at 3.2, it says the following elements must be included in notification of TAC provision. And the third bullet point down says instructions detailing how the registered name holder can take action if the request is invalid, and then in brackets, how to invalidate the Tac.

And to me, the existing text appears to convey to registrants that there is a means to invalidate the TAC, when in reality, there may not be any delay between the provision of the TAC and the transfer. So that's one area that if we do keep the existing approach, we need to better explain and perhaps make clear that there may not be such an opportunity at all registrars. Thank you.

ROGER CARNEY: Great, thanks, Zak. And that's it's a good point to bring up. George has mentioned in his interventions here, and I think Zak as well, that—and actually it was one of our goals in Phase 1A, is to make this a fairly immediate transfer process. And I think that when you talk about that, yes, there's always still a chance, even if they're not given an explicit window to ack or not, when a TAC is provisioned, it can be invalidated up until the time it's transferred. And Zak's point there was, that may be a fairly small window. But that does exist. And we did talk about that, and we talked about that existing up until obviously, the TTL expires, and then no longer valid anyway.

But that is something to look at, is, there is a window. And again, it may be small, it may be several days or weeks even. But there is a window, there is a spot where the registrar can stop a transfer from occurring.

But the question is, before that even happens, again, to get to the commenters' issues, is there a chance to stop that before that even happens? Or again, in today's language, it's not mandatory for registrars to provide a transfer request notification, it's only mandatory to provide the provisioning of the TAC notification. So I think that that's where all these comments are getting to, is that spot of allowing the registrar at that time. And should it be mandatory? Should it be flexible? So Zak, please go ahead.

ZAK MUSCOVITCH: So another way of perhaps putting it is in the form of a question to registrars and to other members of the working group and ICANN attendees: what is the problem that you see in making the five-day window mandatory for registrars, or making it three days, or making it two days or making it one day? What is the problem?

It seems that many people are, through their comments, or some people through their comments, at least, are making the point that although they may appreciate the faster ability to transfer that the working group has proposed, there's a trade off—at least perceived trade off—in terms of security. And so what is the argument against having the five days or four days or three days or two days or one day? But some period that would enable, in all cases, an opportunity for registrant to invalidate that TAC. Thank you.

ROGER CARNEY: Great. Thanks, Zak. And, again, I don't remember all the discussion we had around this. But I do remember the discussion here being that we were looking to, not necessarily expedite, but make it efficient for a transfer request. A lot of registrants don't understand, in this world, especially with this group of people that have such a big influence, that they can't technically get a transfer to happen inside 10 days. It's like, how is that possible that it requires moving the world to get a domain name transferred from the people that are supposed to be well equipped technology to handle that? And again, I don't remember the specifics, as Zak was requesting arguments against the specific window. The current window is a five-day window. And in recommendations, that window has been made optional, and is at the front of the process. So George, please go ahead.

GEORGE KIRIKOS: The length of the window, it really is immaterial for the main TAC scenario, which is if TAC is generated and misused, the attacker uses it at the wrong gaining registrar. And so I as a registrant who's security conscious, I want to be able to know which gaining registrar that code is being input at and have an opportunity to cancel the transfer if it's going to the wrong registrar.

And under the current losing FOA, I can do that. If the losing FOA is eliminated, I can't do that. And so it all comes down to the working group seems to have decided, without consulting registrants, that they know better, that they'd rather have the faster transfer in terms of security versus speed argument. And so the best of both worlds proposal, the compromise that I put in Section F of my comments, give registrants the choice, and that would actually create data for ICANN. You'd actually be able to see what percentage of registrants actually wants the higher security option. And this report suffered from lack of data. And so this is something where if you find five years from now that only 1% of the population or 0.1% opted into the higher security, perhaps then you could argue that we would want to eliminate the losing FOA, but as an incremental step, being security conscious, taking an appropriate policy choice, you'd want to move baby steps, and at least give registrars the choice. Thank you.

ROGER CARNEY: Great, thanks, George. comments from anyone?

ZAK MUSCOVITCH: Obviously, not a controversial issue, Roger.

ROGER CARNEY: Yeah, thanks, Zak. Again, it's our number one commented thing. And there is obviously a disconnect of, again, either language or process here that we need to resolve before moving on from there. So I expected everyone would have reviewed the comments and everything prior to today. So I thought we would have a good discussion on this. But at this point, I'm not sure that we're getting a lot of feedback on even the proposals or, again, the comments. And again, I am trying to generalize the comments because they all kind of bubble down to the same thing, and it's that the choice that this working group made specifically to combine the two five-day windows into and removing the mandatory window for registrants to NACK or accept or acknowledge or deny I should say. Brian, please go ahead.

BRIAN: Thanks, Roger. Just would note, in the language that kind of defends the decision to do the five-day period. It uses some language that says what registrars might do or could do during that five-day period. And just in the interest of setting a floor for ICANN policy, it should probably not exist as far as trying to be persuasive in terms of what a good floor is. It either is good enough where the floor is, or it isn't. And I'm not making an argument either way. I'm just saying that the language about well, what a registrar could do if they wanted to, during that period probably isn't persuasive as to where the absolute floor should be. So just want to note that might be better if that was either omitted or cleaned up. Thanks.

ROGER CARNEY: Great. Thanks, Brian. Zak, please go ahead.

ZAK MUSCOVITCH: Thanks. So Leap of Faith and George has proposed some significant proposals. And I think we just heard from George that he believes that his proposals are superior to the existing system that we proposed. But my question is that if the proposal were revised—this is really a question for George, because he's provided a critique of the existing proposals, so my question really is if the existing proposal were to be revised to make that a minimum period mandatory, whatever that number is between zero and five, combined with the TAC having an embedded IANA code of the receiving registrar, I know that that won't be as good as George's proposals are perceived to be. But would that nevertheless be an improvement over the existing proposal as far as George's critiques are concerned? Thank you.

ROGER CARNEY: Great, thanks, Zak. George, did you want to respond to that? George, please go ahead.

GEORGE KIRIKOS: That was one of my proposals. We can embed the IANA code into the TAC. The TAC can then only be used at a specific registrar. That's equivalent to the losing FOA where I have the opportunity to cancel the transfer if it's going to the wrong registrar.

So yeah, that would satisfy my concerns. The question was, which is technically easier to accomplish? And so I think keeping the FOA that we have now is probably technically easier to implement. Embedding the gaining registrars to the TAC might be much more complicated in terms of programming. But all these are inferior to the breakthrough proposal where you do basically an inter registrar push which was my preferred solution. But it'd be better than what the working group definitely proposed, which is unacceptable to me. Thank you.

ROGER CARNEY: Thanks, George. I think the other part to Zak’s question was on if there was a mandatory window placed at the beginning as well, so that if the recommendation was updated to say that registrar had to provide at least X number of days, as Zak said, whatever that number is, we can figure out, but does that also help? George, please go ahead.

GEORGE KIRIKOS: The length of the window is totally immaterial, wouldn't be affecting my analysis at all. All these attacks are basically going to be automated in terms of the TAC. And so speed—an automated attacker can instantaneously respond. So you can shorten that period. It's not going to have an impact. You can lengthen it.

ROGER CARNEY: Yeah, sorry, George, I think the question is if the mandatory part is changed, if the registrars had to provide a window—whenever that window is can be decided, but would that help if the current recommendation stated that they had to provide a window before the TAC provision? George, please.

GEORGE KIRIKOS: You're saying a delay?

ROGER CARNEY: Not a delay, but a window that allows the registrant to be notified and action.

GEORGE KIRIKOS: I don't see that as an improvement. We can talk about it offline. But it's not really a security improvement in my view. I thought about all these very carefully. You've read the 60 pages.

ROGER CARNEY: Great. Thanks, George. Zak

ZAK MUSCOVITCH: Thank you. I do think that it's an improvement. And I believe even GoDaddy may have made a comment along these lines. I know, Roger, you're somewhat constrained being the chair position. But there was a proposal along these lines within GoDaddy's comments that there be an opportunity to—maybe we're not calling it NACKing anymore, but to invalidate the intended transfer after the provisioning of that TAC.

So although that might not be an ideal security solution, given the critiques we've heard, it may be a viable option that maintains the overall structure of the current proposal, makes some tweaks. It's not going to be satisfactory at all. But it might be a viable approach worth considering as an alternative. Thank you.

ROGER CARNEY: Great, thanks, Zak. Yeah, and I think that that's the point we need to get to is, I think we we've got just a few options, really, in front of us, is if we keep the language as it is, we have to provide better rationale somewhere, to be able to explain to these commenters why their concerns are addressed or are not an issue. Again, maybe some of you think that's not even an issue and it shouldn't be addressed. But those things have to come out and have to be bubbled up so that we can document it and move on from it. And I thought there was a third option—or modify it so that it does support the concepts that the commenters feel are missing. So, Catherine, your hand is up, please.

CATHERINE MERDINGER: Thanks. I wanted to kind of chime in on the idea of including the gaining IANA ID in the TAC. Thinking about it operationally. I like the security of that, but operationally from a registrar perspective, I mean, name.com has named.com Inc. 625, IANA ID. If you're going to that IANA ID, that works very easily, you find maybe name.com, you find 625. You put it in.

But what if you're going to a TLD that's only accredited on name.com sister registrar Name 106? You don't know who that is, you've never heard of it. How do you as the registrant know that, oh, I need to be on that one, and I don't see Name.com on this list, because they're not accredited to sell dot whatever the TLD is?

Alternatively, for resellers, they might be using multiple different registrars, you know who the reseller is, you don't know who their backend registrar is. And so I think, from a registrant perspective, they don't know about IANA IDs, they don't know about any of this kind of stuff from an average user perspective. And I think that will be intuitive for a very small selection of registrants. And I think it's not operationally going to work very well. I don't know how we fix that while balancing the security aspect of it. But I don't think including having the registrant say I want to go to this registrar works all that well, because they don't know about this kind of stuff, realistically. Thanks.

ROGER CARNEY: Great. Thanks, Catherine. Yeah. And that’s a good thing to point out, is when the flow is the same as it is today, that gets tricky, and it also kind of pigeonholes a registrant into having to know that prior to even initiating a transfer. A registrant may have four different accounts at four different registrars, and they just don't even know where they're taking it yet.

But to balance that—and again, when you flip it over, and you look at Leap of Faith discussion of starting at the gaining registrar, then that ID becomes known, and it's easy to track, even if it is a reseller that they're going through, because then that reseller knows the ICANN ID correctly of the registrar that they're going to use.

So I think flip that over and say, “Okay, does that still make sense?” And again, in today's world, to me, I think trying to embed the ID into the TAC is a bad idea. I think it gets very complicated and unwieldy to do. And as Catherine mentioned, it may be simple for that tenth of a percent of registrants that actually know what's going on. But the majority of the people that prefer not to get into the details and just like things that work the way they're supposed to work, it'll just overcomplicate the system without providing that extra security feature that we're hoping for.

So thanks, Catherine, for bringing that up. Any other comments or questions on that? I haven't been following chat because I've been talking too much. But if someone wants to bring something up—Zak, please go ahead.

ZAK MUSCOVITCH: Those are compelling arguments, Catherine. And that's exactly the kind of feedback I was hoping to hear from registrars because as I said, I do not have the technical background. So my follow-up question really is, I appreciate that the registrant may not recognize the identity of the receiving registrar in that theoretical embedded TAC. But is that not much different from the current situation with FOA, that the registrant may not recognize where the domain name is going when it receives the notification currently? Would it be even less certain under that proposed regime? Thanks.

ROGER CARNEY: Thanks, Zak. And I'll hopefully answer for Catherine and say, yes, it's still a problem today. Registrants get notices saying—especially reseller registrants for resellers—get notices and they have no idea where that name even comes from. And that causes a slew of customer service calls about, hey, my transfer is going invalid, and it's like, no, it's actually valid. That's going to where it's supposed to go. But yeah, it does today, it's a problem that we don't have a solution for today.

ZAK MUSCOVITCH: So at least as far as I'm concerned, I'm going to go back and look and think more about how a system would work if it were initiated at the gaining registrar. That might be the stone that we have to overturn to find the right balance and solution here. And I haven't given it much thought yet. But I intend to. Thank you.

ROGER CARNEY: Great, thanks, Zak. And it's actually where I was going to pivot and put George onto the spot. But before that, I'll call on Jothan, since he put his hand up, Jothan, please go ahead.

ROGER CARNEY: Hi, thank you. So we have to be really considering modesty of changes to the SRS system as we do this. Because the more changes and more tweaks we make, we're going to potentially cause affectations we didn't expect in other areas. And so the concept of pivoting over to a pull or push, flipping that dynamic, you could take maybe some of what George is proposing for the very deliberate transfer, that the gaining registrar could provide you the number, whatever that number is that they intend to receive the domain at. And that doesn't necessarily have to change your polling. It would cause the transfer, when you go to request the TAC, and it was included somehow in the TAC, that that deliberate IANA ID is used in that transfer, that could really reduce the surface of problems from a security perspective without radically changing how we're looking at transfers. So that's just a thought here, maybe a hybrid of some of the suggestions that were made and some of what we're already contemplating. And it addresses the concerns about the registrant is not going to know what number or understand any of that. As a gaining registrar, you're motivated to make it easier for a customer to come to you. So you would just provide that number as part of what you're doing with the transfer. Here's what you do to transfer to us. Here's a number you'll use. Here's— go to your losing registrar, current registrar, request the TAC using this number, period, simplifies it, and it solves that piece of it. Thank you.

ROGER CARNEY: Great, thanks, Jothan. Yeah, and again, you bring up a good point of when you start making changes to not just the SRS, but the whole interaction of registry-registrar-registrant, when you start changing those things, you have to look at the risk benefit to it, because as Jothan mentioned, you may be introducing things that you didn't think about, issues, but also the communication back out to registrants, this process has been in place since—staff will correct me—2004 I think and updated in the early teens.

So again, I mean, it's a huge outreach to registrants, customers to explain these changes. So when they do happen, you have to be mindful of those things. And again, as Jothan mentioned, the systems have to be, hopefully, you mitigate any of the [bleed out of a change.]

But to get to what Zak was suggesting, didn't prep, George, on this, but I've over simplified his breakthrough suggestion of flipping this over and going from the gaining registrar. But I wanted to see if George would talk to more specifics of his breakthrough. And again, get away from my oversimplification of just flipping it. And George providing, not just those things, but where he sees the issues at and has solutions to those. So George, if you could.

GEORGE KIRIKOS: It's on Section E of the PDF, which I think has already been posted to the chat. But basically, what I propose is you go to the registrant—doesn't have to be the same registrant, it could be a buyer of a domain name, they would go to their preferred registrar where they want to transfer to, the gaining registrar, pay their money, and that registrar would create an ID for them. And it doesn't have to be a secret ID. It could literally be one character, letter A, there's no secrecy of the TAC.

But as a preference, you'd want to maybe identify it through the domain, the actual registrar's name, and then some random digits. And then you would take that to the losing registrar and input that code. And how does an attacker who has knowledge of that code get anywhere? There's actually no advantage to stealing that code. Whereas there's a huge advantage to stealing the TAC at present.

And so all the security is based on keeping that TAC code secret. Whereas that's no longer the case under this reverse scenario. So you have this account that the domain has been basically pushed to. You enter that at the beginning registrar. And then I would still preserve the losing FOA step. But basically, you're done.

And I explain in the document why this is comparable to an internal registrar push where you push it between accounts, but also compared to cryptocurrency and wire transfers, because similar situation, and so you know, it's not hard. It's just different from what people have been doing now. So the people who are opposed to change will be opposed to it, because it is a change, but they're already proposing a change through the current proposal. So it's like, which change is better? This change is better, because it's comparable to what registrars are already doing with internal transfers. Thank you.

ROGER CARNEY: Great. Thanks, George. Yeah, and again, I think that as Jothan mentioned in chat real quick, there's a lot to think about there. And then again, I think the process has to be fleshed out. There's a lot of steps that our high level discussion hasn't hit. Okay, how does that code get passed from registry to registrar, blah, blah, and how does it do all those things to get validated? But Zak, please go ahead.

ZAK MUSCOVITCH: Thank you. So what I'm not clear about is one of the criticisms of the current proposal is that someone could just penetrate the registrant’s control panel and effect the transfer that way. But isn't the same true under this proposal, that if that TAC is not a secret, or someone obtains it and then goes into the registrant’s control panel and uses it, aren't we back where we started? And asking as a genuine question, so I can understand it. Thank you.

ROGER CARNEY: Great, thanks. Yeah. And again, I think there's a lot of questions there. But I’ll let George respond to that real quick, George, please go ahead.

GEORGE KIRIKOS: Yeah, as I noted in the comment, it doesn't stop that attack scenario. So you still need to keep the losing FOA.

ROGER CARNEY: Okay, thanks, George. I think the problem there is the losing FOLA has no value if the attack vector is that they have control of the control panel, because then the losing FOA is going to go to them anyway. But, again, we need to think these things through. So it's good. Rick, your hand is up, please go ahead.

RICK WILHELM: So when I was reading section E, my read of it was more sort of in the analogy that when one transfers a financial account, like in the United States, you transfer a retirement account from one bank to another and you sort of go to your place where you're going and you say, what are the wiring instructions, and you get an account number, and it says, like, I'm going to Fidelity and it's for the benefit of Richard Wilhelm, and then here's my account number. And then you take that information, and you go over to whatever the place where your 401k was, let's say T Rowe Price. And you give them that information at your T Rowe Price account. And then they send the money through the banking system to Fidelity, hypothetically, or the other way around. Sorry, I didn't mean to—if someone works for T Rowe Price or something like that, right.

But that's sort of the way that I thought of it. And so there's not really a code that I get from Fidelity, it's just my destination account number, externally visible destination account number, which may or may not be an internally visible destination account number, along with some routing information that makes it flow through the banking system properly.

So for those folks, if you're looking for an analogy, that was the way that I thought of that when I was looking at this. It's a different way than the transfer model works now. In the way that the US banking system works, all of the pressure is on my Fidelity account or my T Rowe Price account where I'm going from to make sure that that account is not penetrated, because if a bad actor gets a hold of my T Rowe Price account, then they can drain that thing and send it over to wherever, so all the pressure is there on that on the quote unquote, losing registrar, the current or losing registrar account. So that's just the way that I thought about. Thank you.

ROGER CARNEY: Great, thanks, Rick. George, your hand is up, please go ahead.

GEORGE KIRIKOS: Yeah, I literally use the wire transfer example on page 17 of my comments. And that's going back to this idea that if you control the control panel, you have everything. That's not necessarily the case, though, because if it's a high value wire transfer, my bank will use an out of bound method to contact me, they'll call me up by telephone, they'll do that extra check. And that's really what the losing FOA is.

If you have a properly designed registrar system, the losing FOA can be done—doesn't have to be done by email, the registrar in a properly designed system will ensure independence between the control panel and the registrant’s emails for the actual domain.

So, in my submission, I described how I’d do that, like basically four-factor authentication, up to four factors for my domain names at Tucows, because I have separate credentials for the control panel, I don't allow password resets to email, use a totally different computer even to access the domain email, totally different two-factor authentication system, hardware key versus Google Authenticator.

So going back to bank wire transfer, if you do a small wire transfer of $10,000, they're probably not going to follow up by phone. But if it's a $10 million wire transfer, they're probably going to contact you to do extra verification. And that goes back to the comments when I first spoke, SAC 040, on page 39 of my comments, literally says, treat a transfer as a security event, check and recheck. And so you want to retain that losing FOA because that's the recheck. Thank you.

ROGER CARNEY: Great. Thanks, George. Yeah, and again, I think that that's one of the things that if you look at the rest commendations as a whole, is that those things are—what we went through is how do you layer upon security?

Yeah, and again, I know George doesn't think that 9154 is a big deal, but it is an improvement over the current auth info. And then add on to that, the TTL, and then add on to that, that registrars have a five-day window of doing due diligence to make sure that a high transfer—three-letter domain, two-letter domain, whatever it is, that they have a time period that they can use to validate, and maybe as George just suggested, some of that may be electronically validated, okay, the account hasn't changed in a year so we can probably be safe and transfer it, or in case of a two-letter domain, there's probably going to be five phone calls made prior to the transfer being—TAC being provisioned.

So I think you do look at the ability here to layer security here to make that function. Go ahead, Zak.

ZAK MUSCOVITCH: Thank you, Roger. I'm getting to the point where I'm nearly concluding that what we're building here is not going to be a secure transfer system, because the security ultimately is in the multi factor authentication and other security protocols that a registrar may choose to implement. All that we're really able to do is to build a somewhat secure and reliable transfer mechanism.

But at the end of the day, it doesn't seem like we can implement it with these rules unless we took it a step farther and said registrars have to have this kind of multifactor system, this kind of out of band communication, there must be no verbal confirmation. These are all services that registrars offer independently and on top of the transfer policy. And that's ultimately where the registrant’s security may lie. And so what we're really should be aiming for, practically speaking, is something that's reasonably secure, but not completely secure, completely secure if there is such a thing, happens outside of the transfer policy. Thank you.

ROGER CARNEY: Great, thanks, Zak. We have just a couple more minutes, and we've got a few people in queue. And I think that what Zak just mentioned is what we talked about in Phase 1A, is we can't solve every scenario, but we can try to make it better than it is today. And again, what features of making it better is what we make decisions on. But again, we've got just two minutes and a queue here. So I'll let Crystal go. Please, Crystal.

CRYSTAL ONDO: Thanks, Roger. And what Zak said, I completely agree with right there. But also, I wanted to point out for those listening that registries have registry level lock. If you are looking for additional security, that practice is available right now. You don't have to get it from your registrar, you can get it from your registry, which requires a phone call. So it's not like these options aren't out there right now.

ROGER CARNEY: Great, thanks, Crystal. Yes. And a good reminder that there are other options out there to secure your domains. George, please go ahead quickly.

GEORGE KIRIKOS: Yeah, first, registry lock doesn't prevent the—doesn't stop the transfer, because you have to remove the registry lock to do the transfer to the gaining registrar. I actually asked my own registrar whether there was a way to retain the registry lock, because I have registry lock on some very valuable domain name, to allow a secure transfer between registrars, and that turns out to not be possible. If that was possible, that would be a workaround, enable registry lock on high-value name, and then do a directed transfer that can only happen to one registrar all through registry lock. But that doesn't appear to be possible.

Also, I'd like to thank the working group for allowing the interaction because I appreciate that you actually want to improve security and come up with a good solution. And so I applaud you for the opportunity to participate today. And I hope you actually consider my proposal to allow members of the public like myself to actually participate directly in the working group, because we have expertise to offer that the working group hasn't really considered and I'm probably the best representative given the comments I've submitted. And you do have Steve Crocker, I think, participating as an independent expert, so might want to consider allowing somebody like me to participate. Thank you.

ROGER CARNEY: Great. Thanks, George. And just real quick clarification on that. As far as I know, registrars can't remove a registry lock even if they tried. They have to go through usually offline resources to get a registry lock removed. But that's just what I understand. So, Jothan, please go ahead. You’ve got the last word.

JOTHAN FRAKES: I like this. I would like to move that that is used in my home. So for the concept of this IANA ID that we've been [inaudible] about, one thing that we run into when we're having discussions is registries and registrars both have different attitudes about how this might work.

And so if there were an ID somehow included in this transfer process that would make things more deliberate or focused when something transfers, having something like that be registry-enforced would make things more secure. And I often feel that there is a resistance to registries making enforcements of certain aspects of the transfers that they want registrars to do the majority of the sort of enforcement of anything related to the transfers.

So as we talk about this, as we may evolve these discussions, we may want to look at, are there ways that we could have help from the registries [as] registrars in the enforcement of some pieces of this? So thank you very much, and great session today. Thank you.

ROGER CARNEY: Great, thanks, everyone. Again, great session. We will continue to discussion. We have several more weeks of review of comments. I think Berry has more weeks on it than I do. I hope we get through it quicker. But today's discussion was great. And let's keep it moving forward. So anything from staff before we stop? Okay, great. Thanks, everyone.

UNIDENTIFIED SPEAKER: Thank you. And that concludes today's meeting. We can end the recording.

[END OF TRANSCRIPTION]