
ICANN Transcription

Transfer Policy Review PDP WG

Tuesday, 28 September 2021 at 16:00 UTC

Note: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. Attendance and recordings of the call are posted on agenda wiki page: https://community.icann.org/x/KgA_Cg

The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page <http://gnso.icann.org/en/group-activities/calendar>

JULIE BISLAND:

Good morning, good afternoon, and good evening, everyone. Welcome to the Transfer Policy Review PDP Working Group call, taking place on Tuesday, the 28th of September, 2021.

In the interest of time, there will be no roll call. Attendance will be taken by the Zoom room.

For today's call, we have apologies from Tom Keller (RrSG), Zak Muscovitch (BC), and Steve Crocker (SME). They have formally assigned Eric Rokobauer (RrSG) as their alternates for this call and for remaining days of absence. As a reminder, an alternate assignment must be formalized by way of a Google assignment form. The link is available in all meeting invite e-mails. All members and alternates will be promoted to panelists. When using the chat feature, please select either Panelists and Attendees or select Everyone in order for all participants to see

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

your chat and for it to be captured on the recording. Observers will remain as an attendee and will have access to View Chat only. Alternates not replacing a member are not permitted to engage in the chat or use any of the other Zoom room functionalities. If you are an alternate not replacing a member, please rename your name by adding three Z's before your name and add in parentheses "alternate" after your name, which will move you to the bottom of the participant list. To rename yourself in Zoom, hover over your name and click Rename.

Statements of interest must be kept up to date. If anyone has any updates to share, please raise your hand or speak up now.

And Farzaneh, go ahead.

FARZENAHDADIEI:

Hi, Julie and everyone. I forgot to tell you last week. I have left Yale Law School and I have started my own consultancy. It's called Digital Medusa. Hope you can for a visit at that website. Thank you.

JULIE BISLAND:

Thank you. Anyone else?

All right. If you do need assistance updating your statements of interest, please e-mail the GNSO Secretariat.

Please remember to state your name before speaking for the transcription. Recordings will be posted on the public wiki space shortly after the end of the call. And as a reminder, those who take

part in the ICANN multi-stakeholder process are to comply with the expected standards of behavior.

Thank you and over to our Chair, Roger Carney. Please begin.

ROGER CARNEY:

Thanks, Julie. Welcome, everyone. I think we've been making some good progress, so I think we're going to continue on our gain FOA discussions today. I think we had, I guess, a couple of charter questions left that we needed to touch on, and then we'll try to get into some discussions on the purpose of the gain FOA and make sure that we're keeping what we want to keep and at least providing rationale for things that we're changing or getting rid of.

But first off, the only thing that I want to do is offer up again, like we try to do every week, some time for anyone that's had some discussions since last week or even over the past few weeks with their stakeholder groups and have any comments or questions or concerns that they want to bring forward to the whole group. We'll leave it open now for anyone that has anything to bring forward, and we can discuss it or we'll move on.

Anyone have anything?

Okay. Again, if you guys have discussions at your stakeholder groups that you want to bring forward, we'll try to remember to allocate some time at the beginning to do that and at least get them acknowledged. And hopefully we can discuss them rather quickly.

Okay. Let's go ahead and move into our agenda then and jump into, I think, the last two charter questions that we didn't get to last week—I think Charter 4, which Sarah jumped in and answered for us before we even read it. So let's go ahead and discuss it and see if anybody has any other thoughts on it moving forward.

Again, Charter Question 4 on the gaining FOA is: "If the working group determines the gain FOA is no longer needed, does the auth-info code provide sufficient security? The transfer policy does not currently require specific security requirements around the auth-info code. Should there be additional security requirements added to the auth-info codes—e.g., required syntax, two-factor, issuing restrictions, etc.?"

So, again, I think that, as Sarah read ahead on this last week, we kind of have answered this, but I want to leave it open and see if there's any other comments or questions on anything additional or anything that we're missing possibly. I know that, through our TAC discussions for the first several meetings, we came up with some different changes or some enhanced security features of the old auth-info—what we're calling the TAC [now]. So I think we're kind of answered this even before we got here, but I'll open it up to people.

Sarah, please go ahead.

SARAH WYLD:

Hi. Thank you. So certainly I think, as you just said, we've had a few very productive discussions about the security around the auth code, and I think that's where this work should fit.

I actually had kind of an administrative question. So this is probably for Emily. And I know that we've got—and I'm sorry. So I know we've got this shared drive in Google Docs, and I know that we've done some work around the auth codes. I'm just ... I couldn't find where it was.

So would it be possible, Emily—I'm really sorry. Could you make a master list of all the documents that can be pinned to the top of the Google Drive or something? Because there's just a lot of ... Oh my God. It exists. I'm so sorry. Thank you.

ROGER CARNEY: Thanks, Sarah, for bringing it up.

Emily, please go ahead.

EMILY BARABAS: Thanks, Roger, and thanks, Sarah. Since I've got the wiki up here, I can just show you where everything is stored on the wiki. So here are all of our working documents. I'll drop the link in here to the chat. And what you can see here are the live versions in Google Docs. And staff is regularly making updates to these documents as the deliberations progress. So what we're doing is saving off Word or, where applicable, Excel versions of these documents at regular intervals and keeping them here as well so that we're accepting changes and progressing so that the changes don't build up so much that the documents become unwieldy.

So that's hopefully everything that you need. And the losing FOA document here—I'll just share the link as Sarah hinted at.

And it's good moment for me to remind everyone that we now have some candidate recommendations and draft responses to charter questions beginning on Page 16 of that document that folks can start reviewing and comment on, based on the deliberations that have taken place on that topic.

Happy to answer any questions.

ROGER CARNEY:

Great. Tanks, Emily.

Okay. Any questions for Emily on that? Again, just a good reminder of our working space and what's available out there. If you can't find anything, just drop a line to the list, and we'll get it found.

Okay, great. All right. So back to Charter Question 4. Any other comments on this, specifically on Question #4, I guess? Again, I don't know if anybody has any comments or questions or concerns. It may be mostly concerns here because I think everybody recognizes that we have had some pretty long discussions on improving the TAC. So if anybody has concerns, really, I think that's the big thing here, since we've already gone through those substantive discussions in it.

Okay. Then let's go ahead and go on to Charter Question 5 and take a look at that. So: "If the working group determines the gaining FOA is no longer needed, does the transmission of the auth-code—the TAC now—"provide a sufficient paper trail for auditing and Compliance purposes?"

So, comments here? Questions? Concerns? I think that maybe the biggest concern here is everyone recognized that the gaining GOA provided at least one more piece of the audit trail—are we able to keep that functionality or have we made sure that that functionality is embedded elsewhere? Or do we need to come up with something to include there?

Kristian, please go ahead.

KRISTIAN ORMEN:

Thank you. I would like to answer this question with: the auth-info code and the TAC notification e-mail provides a sufficient paper trail because I think the TAC notification e-mail adds to the paper trail, and that makes it better.

ROGER CARNEY:

Great. Thanks, Kristian. Yeah, that's a good point to bring out. It's not just what we've done to the TAC but, yes, our discussions [about] losing FOA with the TAC notification. And even the notification of the transfer-complete provides additional pieces of an audit trail.

Holida, please go ahead.

HOLIDA YANIK:

In terms of Compliance, I'd like to note about our current practices in investigating unauthorized transfer cases. So currently we are addressing the issues only with the losing registrar and requesting that the auth code and the losing FOA has been provided to the

registrant. So considering that the losing FOA will be replaced by the tech notification and transfer, pre-transfer, and transfer completion notifications, I guess, in terms of our investigations, that would be sufficient for us. Thank you.

ROGER CARNEY: Great. Thank you very much.

Any other comments here?

Okay. Well, we got through all of our charter questions. I think that the key here is the feeling that we're getting rid of the gaining FOA. I can't say that I feel that we're actually get rid of the gaining FOA. I think we've moved things around. Again, the TAC presentation provides some of what the gaining FOA was doing. And, obviously, the forced losing registrar notice back of the complete transfer really supplements the old losing FOA. So we're not getting rid of the losing FOA or the gaining FOA. We've just enhanced it to better reflect how it should function today, I think.

And I think that, when we answer these questions—"Are we getting rid of the gaining FOA?"—it's interesting because, to me, that's a hard one. Specifically, are we getting rid of the current text and everything around it? Yes. But I think the important part is to ensure that we're getting the reasons why the gaining FOA was being used addressed. It's one of the things that we've put together a poll for today. So we'll go through that once we've finished these discussions as well.

Jim, please go ahead.

JIM GALVIN:

Thanks, Roger. Let me take what you said and turn it into the following concrete question. Rather than thinking about getting rid of the gaining FOA, the question for, I think, this group here is, should we be taking the features and requirements that were served by the gaining FOA? And we need a specific policy recommendation that you have to keep certain records.

Now, in the same way that we were talking about, conceptually, with notifications, there's several kinds of notifications that have to happen—and we're having some discussion about multiple notifications or just one—I think that those are implementation details, and in that sense, this can be, too.

I think the question that we have to meet is, do we want to make sure that we somehow say that there is a paper trail, you're required to keep one, and this is what it has to have in it: "This is the kind of information it has to have"? Maybe it's tracking the notifications that you sent. Maybe it's tracking the issuance of the TAC. As far as I know—I could be wrong here, so please correct me if I've got this wrong—that's not covered anywhere. Those kinds of requirements aren't there. So maybe we just need to abstract back those things and put those in. Thanks.

ROGER CARNEY:

Thanks, Jim. And I appreciate the rewording. I think it always helps, too. And I completely agree with what you're saying, and I hope that matched what I was saying. It seemed to.

So, again, I think the important part, as Jim mentioned, is that the gaining FOA served a purpose—multiple purposes, probably. And I think the key is to pull those purposes out—what was it doing?—and confirm that either we’re going to continue those in some other fashion or provide rationale on why we’re not going to continue it at all. I think that’s really our two options: to look at how we’re replacing or enhancing it, or how we’re just not going to serve that purpose anymore whereas we don’t feel it’s needed for whatever reason that is and document those reasons.

Okay. Any other comments or questions on that? Again, I think that’ll be our key to finalizing these charter questions. It’s just coming up with, “Okay. The gaining FOA served a purpose of notification. The gaining served the purpose of providing the way to stop this transfer from occurring. It served a purpose of [inaudible] [trail].” And, again, whatever other purposes there are, I think we just have to put down and see how we’re going to handle those moving forward so we can answer these questions and get them put to paper.

Okay. Well, let’s go ahead and jump into the poll questions. Maybe that’ll help spur some discussion on that. And, again, I think we just did need to come back to identifying those purposes and what we’re going to do with them. And I think the gaining FOA discussions will probably be near complete then.

All right. So let’s go ahead and jump into the poll ... Okay, great. All right. So, did the gaining FOA serve as a security function?” “Yes, and new requirements should exist to replace the gaining FOA security function.” “Yes, but this function is no longer

necessary.” “No, it did not serve the function.” Or “Not sure. Needs further discussion.”

Again, let’s limit the responses to the active participants and not the observers all the alternates. Just the active participants. So please go ahead and answer that. And if there’s any questions in it, let me know. But please go ahead and answer the question.

All right. Let’s go ahead and show the results. All right. Wow. Okay. I fairly good split there. I think that obviously some discussion here for ... If 70% thought it did have a security function, and 40% , or more than half of the 70%, actually thought it doesn’t need it anymore, that’s definitely something to discussion. And I’d definitely like to hear from people who didn’t think it served this function and just get a feel for how they saw that.

Theo, please go ahead.

THEO GEURTS:

Thanks. Well, I wasn’t there when this FOA was created. That was way before my time. But when I always looked at it, starting as a registrar, I saw that the old registrant had to give permission, and the new registrant had to give permission. In my mind, it was always a vehicle to transfer domain names. And, at a later point, somebody started adding security features to it or sort of thought it was a security feature. I think that is not correct, in my mind. It has always been a way to transfer a domain name. Get consent from a new registrant and an old registrant, and the transfer will be done. Thanks.

ROGER CARNEY: Great. Thanks, Theo. I don't think you're the only person that's mentioned that. They don't feel that it's exactly a security function but that it's more of a ... I can't even think of a term. It's more of a loose security feature.

Greg, please go ahead.

GREG DIBIASE: I think I was about to go down the same road you're saying. I chose "Yes, but the function is no longer necessary." So its primary purpose was not a security feature, from my view. It's to facilitate the transfer. And I said I suppose it could serve as a security function, but I don't think it was a strong security function. Or I don't think it was strong enough to try to figure out how to incorporate. I don't think we have evidence that it was serving as this strong security measure.

But I think that added step could serve something. Some small degree of security could be added, but I just don't think it's necessary, given its low utility from what we've seen since the GDPR came into effect.

ROGER CARNEY: Great. Thanks, Greg.

Okay. Any other comments on that? Thinking back to Theo's comment on him not being around here when this started, I do believe—maybe someone can correct me—that the gaining FOA

requirements were actually predated auth codes/autho-infos. And maybe Jim actually knows that timing better than anybody. But for some reason I was thinking that the gaining FOA requirements pre-dated the ability for EPP to even have auth-info.

Okay. Any other comments? Questions?

Greg, I assume that's an old hand.

Thanks, Jim, for confirming that.

Okay. I think we get out of this what we're looking for. Again, I'm not sure that everyone sees it as a security feature, but again, just like Greg and I were trying to describe, it somehow seems like it provided some kind of, but not necessarily a true feature.

Jim, please go ahead.

JIM GALVIN:

Thanks, Roger. The way that I like to think about it is that, back in the day, we weren't thinking in security terms. So the security requirements and needs were not particularly documented or well-understood or felt to be needed. But as we all know, this domain name industry kind of grew just enormously quickly as soon as we migrated to ICANN and this more formal process, multiple registrars and registries. Then EPP came into existence.

So I think that, as a community, we shared our experiences and acknowledged, at least verbally, what we needed and, "Oh, by the way, we kind of have this already. This is working." But it never really got documented in that way because that wasn't the way the

question was framed, and it certainly wasn't top-of-mind in those first few early years. That's all. Thanks.

ROGER CARNEY:

Great. Thanks, Jim.

Okay. Again, I think the tough part is [on] "Is it security? Is it not?" ... And maybe someone from outside the Contracted Party House could actually maybe touch on that if they feel that it is a security mechanism somehow or ... Again, it's one of those where it seems like it adds something, but I'm not sure that you really call it security or not.

But anyone want to discuss that?

Okay. All right. And, again, on this one, it seems like it's possibly not a security function, and I think that's where everyone is heading. It does add something, but it seems that it's not specifically a security feature as in that auth-info or the TAC is in itself.

Okay. Let's go ahead and move on to the second question. We'll give some more responses as we go through. Okay, second question: "Did the gaining FOA serve a notification function?" "Yes, and new requirements should exist to replace the gaining FOA's notification function." "Yes, but this function is no longer necessary." "No, it did not serve this function." Or, "Not sure. Just needs more discussion."

And, again, let's keep this to just the actual members. Alternates and observers, you don't need to respond to these. Just the active

members, please. Go ahead and respond, and we'll give everybody a few seconds.

Okay. Let's go ahead and show the results of that one. Okay. So this is notification. And it seems like everybody did s that it was a form of notification. And a large majority of people thought that, yes, that purpose, that idea, of the gaining FOA being a notification should continue. A large chunk said no, and I'm interested in that—knowing if it's just because we've already kind of replaced it or if it's just no longer needed. It would be great to hear from anyone that answered that it's no longer necessary.

Sarah, please go ahead.

SARAH WYLD:

Thank you. I did answer that it is no longer necessary. I do not think that we need a policy requirement to make sure that the gaining registrar notifies the domain owner. The losing registrar will have that obligation. And I don't think that they both need to do that.

I do think it is possible that the gaining registrar might want to notify the domain owner for marketing purposes, and they might have a GDPR or similar obligation to disclose to the data subject that they are processing that person's data. But I don't think that there is a transfer policy reason to require that notification from the gaining registrar. Thank you.

ROGER CARNEY:

Great. Thanks, Sarah.

Theo, please go ahead.

THEO GEURTS: When Sarah frames it that way, I actually completely agree with it. I chose the other option, but yeah. Put it like that? Yes, I agree, Sarah. Good point. Thanks.

ROGER CARNEY: Yeah. And I think Sarah kind of put a good twist on this question and really kind of highlighted the gaining FOA from the gaining registrar's perspective. Did it serve a notification? I think Sarah [says], yes, it did. And it sounds like Sarah and Theo ... Well, Sarah answered that way, but maybe Theo and Jim actually moved their votes down one here. And it's not necessarily that the gaining registrar needs to do anything. Obviously, they can, and most likely will, as Sarah mentioned, even if it's a welcome or something that's required by law for them to do ... They may have to, again, talk about their purpose for collecting certain data and everything else. But the simple requirement of specifically a gaining FOA from the gaining registrar is, notification-wise, probably not necessary.

Thoughts on that from anyone else?

And, again, outside the Contracted Party House, anyone that thinks that maybe that should continue because they see a different reason for that, it'd be great to hear as well. So, again, the poll showed a fairly even split, though Sarah kind of explained why the no was her choice and several other's. So, again, if

anybody else thinks differently, please bring that forward so we can discuss it and come to the best conclusion here.

Okay. So it sounds like everybody is in agreement there. That's great.

All right. So let's go ahead and move on to the next question. Okay. So, "Did the gaining FOA serve as a paper trail function? Did it add to the audit trail? Did it add to an easy-to-use compliance checkpoint—and not just for ICANN Compliance but for anybody that's looking at if the transfer was valid or whatever? Did it serve that function?" "Yes, and the new requirement should exist to replace that?" "Yes, but this function is not longer necessary." "No, it did not serve this function." Or, "Not sure. Just needs further discussion."

So, again, just active members. If you want to answer this, please go ahead and answer, and we'll discuss it in a few seconds.

Keiron, please go ahead.

KEIRON TOBIN:

Sorry. On the last question, I think that's where my mind was going to in terms of notification. I feel like this question just kind of changed with paper trail. I don't know how other people feel about that.

ROGER CARNEY:

Thanks, Keiron. And I think that this is not so much a forward-presentation kind of thing to the registrants themselves, but as you

kind of tied it together, this it most likely in electronic form. It doesn't have to be. If people are still doing things by hand, maybe it's not going to be electronic but still serving as a true paper trail kind of feature, not just notification. But obviously—I think Jim may have said it, or somebody said it—that notification is probably going to drive audit trail functionality, and maybe we have to say that it has to. Maybe that's a requirement: we have to say that it needs to do that. You don't just send a notification. When you send a notification, you also have to document that that was sent. So I think that's what the purpose of this question was.

All right. Let's go ahead and look at the results. Okay. So yes. Again, fairly high on "Yes, it did serve this function," but a pretty big on if it should continue to serve this function or not. Again, I think that those that said, "No, it doesn't need to serve this question" ... I think the key want to come to is, "No, this function doesn't need to exist," or, "No, this function has already been replaced this something." I think that's what we need to know here: "Yes, it did do this, but it's no longer necessary." I think anyone that answered that, if they want to discuss in detail what they were kind of looking at and why it's no longer needed it would be nice to hear from. And anyone that actually mentioned, "Not sure."

Theo, please go ahead.

THEO GEURTS:

In my opinion, the function is no longer necessary. I'm not going to restate why that is. I've said it a couple of times. But it's more interesting to go to the yes answer and "new requirements should

exist with the gaining FOA.” So you’re looking at the purpose of a paper trail and you still want to have a paper trail through to a gaining FOA. Is that a question? And if that is the question and then we answered yes—44%—how does that look like in reality? Because that would be an interesting discussion to see what the requirements there are and what would be the technical barriers and perhaps legal barriers to get to that point, if we still want to do this. Thanks.

ROGER CARNEY:

Great. Thanks, Theo. Good point, too.

Any other comment/questions, especially on how Theo, again, spun that around and says, “Okay, look. Let’s look at it the other way and see if that makes sense”?

A very quiet group today. Okay. And, again, Theo kind of spun that nicely, but I think the key here ... The majority of people thought it did provide the one piece of check. And I think that the key is we’ve discussed the notifications and everything, and I just wonder if part of that discussion of the notification needs to also address ... and those notifications need to be logged, and that actually provides that backup of that paper trail kind of idea of the transfer process from beginning to end.

Okay. Well, let’s go ahead and move on to the next question then. All right. So this is the other big question here. “Did the gaining FOA serve any other functions that we haven’t talked about?” I mean, did it serve any other purpose? We’ve kind of talked of probably three things, I think, of what did for different individuals or

different groups, but is there anything missing? Did it do anything else? So the question here is, did the gaining FOA serve another function not listed in the previous three questions? “Yes.” “No.” “Not sure.” And, again, I think the key here is thinking about the gaining FOA as a whole. And it goes back to what we were discussing earlier: what are purposes?—just so that we can make sure that we’re identifying, “Okay, yes, they need to continue to exist, and we’ve handled it this way,” or, “No, it just doesn’t need to exist at all anymore”—and, again, not the gaining FOA specifically but those purposes of that gaining FOA. So please go ahead and answer, and we will discuss in a few seconds.

Okay. Let’s go ahead and look at the responses. Okay. I think this is good. I think that those few things that we’ve talked about are the things everybody can see. And, again, I’d invite all groups to think about that because I’m not sure each individual group sees all the same purposes. So I think that’s a big thing to come through.

Greg, please go ahead.

GREG DIBIASE:

[inaudible], but I just kind of wanted to raise something that’s, I guess, related to this question but not specific to this question. It’s that sending e-mails, having a required e-mail that requires action, could be used potentially by bad actors for phishing. I know registrars have seen that. And renewals for sure. We’ve seen fake renewal notices being sent to our customers. But I want to maybe flag that it’s not a function of a gaining FOA but just maybe something to note: when we do have mandatory e-mails that

require action from the registrant, that could potentially open a vector for phishing. And maybe that's something to consider if we're considering whether to try to reinstate this from a holistic perspective.

ROGER CARNEY:

Interesting. Thanks, Greg. I never thought about it that way. And maybe that's even one of the nice features that we've talked about—not talking about, kind of?—and not being specific on the communication mechanism itself. And I was just thinking, when you were talking about, that maybe a registrar allows transfer notification, again, and multiple different mechanisms. And maybe that actually provides an enhanced security because those threats may not know what mechanism the customer actually chose. Maybe they did choose e-mail. Maybe they chose phone or Facebook—whatever it is. But maybe those threat actors don't actually know that. So, interesting. Thanks, Greg.

Owen, please go ahead.

OWEN SMIGELSKI:

Thanks, Roger. I'd like to agree with Greg there and then also add on. The reason why I answered no is because we're talking about the gaining FOA as is. It was requirement, if my recollection is correct, that we needed to the exact form of the gaining FOA and could not modify it. I think it could be translated into another language, but English had to be first, and we couldn't really update or modify the content otherwise. So using it for marketing purposes or other things, which seems like some people have

said could be a desirable, could be a future-forward thing but wasn't necessarily we had been doing. I don't know if that's something we want to try to recapture: being able to market or promote things or, "Hey, you don't really want to leave" kinds of communications. Thanks.

ROGER CARNEY: Great. Thanks, Owen.

Theo, please go ahead.

THEO GEURTS: Greg makes a very good point there. You could think of alternatives. I mean, you mentioned Facebook. You could also use all kinds of apps, [inaudible] session—whatever—wire [inaudible] [out of there]. But I fear that, if every registrar is going to implement some [out-band] form of communication ... There is a little bit of fear within me that we might get a very sticky process with some implementations across several registrars. So that is something to look out for.

So I'm not shooting it down. I'm just a bit on the cautious side. Like, if we want to do this, just don't talk about e-mail notifications but notifications in general. We need to acknowledge that there might be a risk that we get a whole bunch of different implementations, which is maybe not very beneficial to the registrant but to the registrar. Thanks.

ROGER CARNEY: Great. Thanks, Theo. Yeah, I think that is important. And, again, obviously, we've tried to leave that open, and we'll have to look at, to your point of how that affects the registrants, especially those that use multiple registrars for doing business, or even if they don't and end up moving, obviously, how that affects them. So, yeah, great.

Jim, please go ahead.

JIM GALVIN: Thanks, Roger. I don't know if this needs to be part of policy or not. That would be for this group to think about. But I offer, as a suggestion, that we try to take lessons from other industries on security principles. Financial services are actually generally in a pretty good place with this kind of model, and that is that the principle here is not to make notifications have actions embedded in them [but] for them not to have embedded actions. We have to keep that kind of thing in mind.

Now, to make this concrete, Greg is right: you don't send an e-mail message which says, "Click here to confirm/Click here to deny"—that kind of thing. What you do is send an e-mail message that says, "Log into your portal, and you'll find messages there. And you need to go deal with them." And you don't even give them a link to get there. Or maybe you do. That brings in another set of issues that you have to get past. But you want people to come and deal with that issue in that way. It's the same kind of thing with credit cards. Somebody calls you on the phone and asks you for your credit card number. What do you do first? They tell you they're from your bank. "Well, I think I'm going to call my

bank back, and I will give you the number, with the number that's on my card, not the one you give me" kind of thing.

As an Internet people, we're not in a good place where we deal with these kinds of things well, but I think that, as more industries—this is just another example of one—move in the direction of getting people to do the right thing, we raise everybody.

This also applies to text messages, by the way. You can't just send somebody a text message that says, "Click here to confirm or deny," or whatever it is that you want to do. That's what's wrong with those kinds of messages. A notification itself can't be itself directly actionable. And that's just a principle in today's environment that applies, unless you want to move to secure e-mail and all kinds of other things. But we don't have to go there. Thanks.

ROGER CARNEY:

Thanks, Jim. Yeah, I think that's an important thing to keep in mind. I don't know if Sarah was kind of hinting at it, but yeah. It's one of those where it's kind of weird because, as a consumer, I think about it and certain things I don't mind. But to your point about banks, as you look at more secure concepts ... I'm trying to think of things that I don't just go type in the URL, but I probably do it more now than I've ever done it. But, yeah, I think it's important to try to eliminate physical ... not physical but that action, even if it's a little less convenient, obviously, than embedding that in there.

To Sarah's point, though, I think it's still important to tell them what it's about, even if you're not providing that directly.

Berry, please go ahead.

BERRY COBB:

Thank you, Roger. I'm partially channeling this Question 4 as well as Question 1 back on the security question and channeling Jim's interventions during our losing FOA discussions. So this is really just something for this group to keep in mind. Maybe it starts to come together when we think about losing and gaining FOAs or what the new world might look like.

But I'm looking back at an old staff report that was April 2005. By Internet standards, that's considered the Stone Age, but there is a particular statement in there that has stated, "In order to provide strong protections against unauthorized transfers, and to facilitate choice and domain name registration, all registrars are required to use a clear, standardized form of authorization that provides for the express consent of domain name registrants prior to the initiation of any registrar transfer."

I think we've had some interventions today that question how strong or weak those protections are or might be, but I'm also recalling what Jim was saying about the timing of these particular notifications. So in the context of whether it's security or it's another function, what is interesting to me is that [on] the gaining FOA, when we think about pre-GDPR, was the first notification that the registered name holder would receive. And at that point, they're consenting—maybe "consent" is not the appropriate word,

but they are agreeing—that they do want to transfer the domain, which is, in effect, outside of the losing registrar’s account panel. But then, secondarily, I believe that there was an option to reject that transfer if it attempts or hopes to mitigate unauthorized transfers.

Anyway, my takeaway here is thinking about the timing and some of our initial discussions that we’ve had on the losing FOA. If the gaining FOA is, as noted earlier, no longer a requirement, that definitely changes up the timing and who’s notifying who. And to me, that seems like that is connected to the conversation about whether the gaining FOA played a part in any kind of security mechanism or not. Thank you.

ROGER CARNEY:

Great. Thanks, Berry. I like it when Berry can find those things from, as you mentioned, the Stone Age. And honestly, the text to that still seems—obviously I didn’t memorize what he said—applicable today. You still want to do those things to ensure a valid transfer or even an efficient transfer.

Okay. Any other comments? Again, Berry was introducing Jim’s thoughts from the previous discussions on losing, on timing. Any other comments specifically around that or anything that Berry was just mentioning?

Okay. All right, let’s go ahead and move to, I think, the last question. “What statement do you support with respecting to gaining FOA?” “Requirements should be removed from the policy with no replacement.” “Improved FOA security and new

notifications are sufficient to replace it.” “The working group needs to explore other possible measures to replace it.” “Not sure,” or, “Needs further discussion.”

Again, I think this goes back to, are we solving the purposes of the original gaining FOA or, if we’re not ... Again, I think that’s okay if we’re not going to replace it. We just have to come up with the rationale of why we’re not going to replace it moving forward. Or we come up with the replacement or the enhancements that we’re going to make to it.

So, again—Sarah, do you have a question?

SARAH WYLD: I do. Thank you, Roger. Just to confirm: the second option means that we continue the gaining FOA but it’s different? But the first options means no more gaining FOA? Is that correct?

ROGER CARNEY: Yes, that is correct.

SARAH WYLD: Okay. Thank you.

ROGER CARNEY: Thank you, Sarah. Again, active members, please go ahead and select this, and we will discuss shortly.

Okay. Let's go ahead and pull up those results. All right. So a pretty good split between that the FOA should be just gotten rid and that nothing needs to be done to replace—again, the first one, as Sarah tried to make some clarity on those two different first and second points—and, again, that the improved FOA and new notifications are sufficient. So it looks like we've got a fairly even split here. And maybe those that picked one of those can explain why. And, again, I think the key here is probably maybe the first one—to me, anyway ... Those respondents with the first option here—the requirements should be removed with no replacement, meaning we would have to come up with rationale for all those ideas that the gaining FOA represent and present that back as why we would not replace any of that functionality ...

But anyone else want to talk about this?

Theo, go ahead.

THEO GEURTS:

I said this before, but if you look at the current situation where sending the gaining FOA is nearly impossible because there is nothing to parse from the WHOIS that is usable, you're kind of wondering, if we at some point as a group try to provide these rationales to everybody else and the Board, etc., etc., are not trying to create a solution and then seek a problem to it.

As far as I'm concerned, things are in pretty good shape at the moment. I don't signal any major issues when it comes to unauthorized transfers. It could be that other registrars have a completely different opinion, but it would be good to voice those

issues so we know that there is an actual problem there which needs addressing. And if it's low numbers, then I don't think we should have to do anything much up to the point than just stating what the issues are and why it's going away. And it's a high number among registrars, oh, yeah, then maybe we have an issue. But as long as I don't hear anything or I don't see any statistics on it, like I said, we're creating a solution and then seek a problem to it. Thanks.

ROGER CARNEY:

Thanks, Theo. And I think, if you're watching chat—everybody, take a read of the chat—Farzaneh talks about, "If we can't send it, then what are we talking about?" I think we all agree that today's gaining FOA can't be used because, again, the reason we're not using it is because it doesn't comply with GDPR.

But I think that the important thing is there's purposes for the gaining FOA, and that wasn't necessarily to share [PII] data. Obviously, they created an audit trail to allow Compliance to check on if it happened and if it was the right person or whatever. Did it provide another level of security? These other things that it was doing ... Obviously, we can't share the personal information anymore. Again, that's why we stopped using it more than three years ago. But I think that the gaining FOA had multiple purposes. And are those purposes needed? Again, notification—is needed that we notify the registrants when certain things are happening? Again, I think here it comes into—I think Sarah talked about, and Theo and Jim kind of supported the idea—not necessarily from the gaining registrar, the notification, but any notification ... And specifically I think Kristian may have mentioned—or someone

did—a way to provide instructions on how to stop this transfer from going forward if it's not valid or if the registrant doesn't want it to occur any longer. And, again, we kind of tied all those things into our losing FOA discussion and the TAC presentation and the losing registrar notification. And, again, I think we're trying to—or we have already started to—pull out some of the purposes of the gaining FOA, but we know that the gaining FOA can't exist as it does today. And I think that what we want to do is try to replicate all those things that e can't replicate, if they make sense to continue in moving forward. So hopefully that helps.

Jim, please go ahead.

JIM GALVIN:

Thanks, Roger. I said, no, we need to explore the measures to replace it. But I have a suspicion I really did misunderstand the question. I think you just clarified and explained it for me, but if you'll indulge me for a moment, I want to play this back and make sure I've got the right story here. I saw requirements—plural—in the first possible answer as talking about everything that the FOA does—the gaining FOA. I think this question was just about the gaining FOA as a document itself, not about all of its requirements.

So, from my point of view, I said we need to find ways to replace it because, correct, I don't think we want paperwork, but I do think we want all the things that it stood for. I think that we're in agreement on that point.

And, with that in mind, the answer here is I think I would support the first one, which is that the FOA itself needs to go away, but the requirements that it stood for are going to replace it.

And the second answer was about keeping the FOA in some form or another and maybe other things. So I think I would switch my vote to A. But have I characterized all that correctly, please? Thank you.

ROGER CARNEY:

Thanks, Jim. And, again, I really appreciate it when you try to at least reword it for me because I know it always helps to have multiple—and hopefully the same result—ways of looking at it. And I think that's right, Jim. And I think that's the point.

And maybe that's how people saw it was. A, the first response was, yes, the FOA needs to disappear. And I think that, when we say it as it exists in the transfer policy today, everybody agrees that we cannot enforce what we were sending exactly the way we were sending it. But, again, the purposes of what the gaining FOA tried to achieve ... I'm hoping that we can find—and maybe we can't. Again, that's okay. But hopefully we can find ways to keep what those purposes were—again, notification, “security,” audit trail. I think that was the three big features saw that the gaining FOA was doing. Are we able to replicate those or not or make them better or not or just not do them at all?

And I think that the group agrees—at least this is what I am hearing—that the FOA needs to go away as it does today, but we can keep those items. Hopefully I'm just repeating what Jim said

because it seems like I'm getting to that same spot. But we can keep those other items in a different, maybe, way but still keep those purposes moving forward.

Steinar, please go ahead.

STEINAR GROTTEROD: HI. Two things, actually. I have transferred some generic domain names recently, and when it has been completed, I got a message from my new registrar that the domain name is in my account and I can now start adding services, etc. For me, that is kind of the information I need, and it's very similar to what I believe is the point or the purposes with the gaining FOA. But it won't help if the account is hacked because, well, then it seems I won't receive that kind of message anyway because ... So that's the case. So, personally, I don't believe we need that gaining FOA. I think we will have information from the registrar—of my new registrar in my example—informing about service and so on.

But the other thing is also something we discussed at the previous meeting. That is, my understanding is that, if we do try to seek some sort of information to be sent by the gaining FOA with respect to the GDRP, there has to be some sort of contract between the losing and gaining registrar because of the GDPR in order to transfer data back and forth and so on.

Is that something that is forgotten in this discussion, or has it just been altered into something else? Thank you.

ROGER CARNEY:

Great. Thanks, Steinar. That's an interesting point that you bring up. We stopped the current process because it no longer allowed—again, everybody can argue about the timing or whatever ... But GDPR made it perfectly clear that it was no longer allowed the way we were doing it.

And, Steinar, your question of, “Is there a way to continue, possibly, sharing whatever relevant personal information”—like you mentioned, maybe a contract from registrar to registrar, however that works—I think is a great thing to think about and see if there are ways. I think what we heard the last couple meetings was that no one could come up with a good way to do that. And one of the strong arguments someone kept making or multiple people kept making was that the transfer policy in its current Compliance-relaxed/relaxed Compliance form doesn't require any [PII] to be transferred and still functions at a level that's acceptable to all stakeholder groups. So it's one of those where, if it's functioning, the argument of the GDPR of, “If it's functioning, then why do you need it?” comes into play. But obviously I think that, Steinar, is one of the key things: can you just still do that?

Theo, please go ahead.

THEO GEURTS:

Thanks. I want to backtrack a little bit on Jim's comments on, if we lose the gaining FOA, would we want to keep in place what it stood for. Maybe I'm terrible here, but I don't see how that works. As a registrar, the registrant starts a transfer. It used to be that I, as the gaining registrar, would harvest or get the data from the other registrar regarding the registrant, and based on the data

which I would get from the registrant, I would assemble a FOA and then I would send the registrant the FOA e-mail with a question: "Do you want to transfer the domain name to us or not?" That was how it was based.

Okay, that is no longer the case because the data is no longer accessible anymore. The only data that I have is the data which the registrant provides me. I can't act on that data. I don't see how that data is useful to me to preserve the function of the gaining FOA. What I'm going to do? The registrant starts a new transfer. Am I going to e-mail a registrant an FOA or a notification saying, "Hey, you just started a transfer." I would assume that a registrant already knows this because he or she logged into the account to start a transfer.

So I don't see how you preserve that functionality of the FOA while you only have the data from the registrant which the registrant provided to you as the gaining registrar. You can't match it with the losing registrar. There are no checks and balances there anymore because the data is no longer available to me. So I don't see how you get to a point where you sort of keep the functionality or the security if you will if you can't match that data with the other registrar. That doesn't work, in my opinion. But maybe I'm terrible here and I'm looking at a micro-level while I should be looking at a much higher level to understand this. But I don't understand it. Thanks.

ROGER CARNEY:

Thanks, Theo. Again, I think some of the keys here ... I think everybody agrees that the gaining FOA as written today in the policy can't move forward. It's not something that we can support.

But I think that, again, getting to the notification and "Does the notification help?" I think that's one of things that we talked about when we went through the notification process: who should be notified? Again, maybe the registrant isn't the one that's logging in and initiating it, but they should be made aware that it's happening. And, again, possibly [it's] what we talked about.

And I think that's some of the keys: ... Obviously, someone gets hacked and maybe they change the right things and the registrant will never get notified, which is a possibility. And that's something that's beyond the scope of this transfer to solve, for sure, if it's even solvable. But what we can solve is related to the transfer. And, once initiated, the notification to the registrant seems like it would [inaudible] a purpose and use. So I think that still exists because of that notification. So I think that's important to maintain.

Okay. Other comments? Questions? I see a lot of talk in chat here.

To kind of go the chat here real quick and not go through everything individually, what we're talking about is the gaining FOA as written in the current requirements going away, but we're talking about, are there reasons to keep the other purposes of the gaining, not the sharing of personal identifying information, obviously. But is there a reason to keep a notification feature of it? Is there a reason to keep the audit trail features of that? And, again, is there a reason to keep [what Eric] called a security

feature that allows that, again, outside of keeping the FOA, because everybody seems to agree and acknowledge that the current form cannot exist going forward [for] exactly the reason why it hasn't been used for over three-and-a-half years.

Farzaneh, I don't know. Farzaneh asked a question a chat on if there was a stakeholder group pushing to keep the gaining FOA. I haven't heard of a stakeholder group pushing to keep it. And, again, I don't know if that's because, again, we haven't been doing it so long or that the stakeholder groups anticipate us---again, this transfer group---resolving this issue. And, again, to my point, resolving the issue isn't getting rid of it or keeping it. It's getting rid of it and possibly doing and keeping the purposes of it.

Okay. Any other comments or questions on this? This is our last poll question, so everybody is off the hook for the homework there or for the study guide.

Okay. And, again, I think the key to finishing this gaining FOA discussion is the agreement that I think we have---please speak up if no one thinks that---that getting rid of the current FOA requirements---either policy as they exit---needs to happen. That is what we're recommending.

But we're also recommending that there's ... Again, this is probably the discussion we need to go through: identifying those purposes and what we're doing with them. So what I've heard is we've identified that it serves a notification---the current one does---and we'd like to see that continue in some form---and, again, not by the gaining registrar because it changes there so it's different.

Theo, please go ahead.

THEO GEURTS: Yeah, right there: the notification. I still don't see how that is somewhat related to security. If I obtained the TAC illegally and I'm going to a registrar and I fill in my own information—which would be stupid—but again—I start a transfer with the illegally obtained TAC, I get a notification. How does that help? I know what I'm doing. I'm stealing a domain name.

ROGER CARNEY: Theo, I agree, and I think that that notification has to come before that. And I think that's what our goal was when we said the TAC presentation notification is that notification because, to your point, once it's after that, there's no use of it, if that makes sense.

THEO GEURTS: But can we then already conclude—maybe I'm a little bit too hasty here—that we sort of already came up with a solution a couple of sessions ago when we created the requirements for the TAC?

ROGER CARNEY: I think that's a great question and I present that to the whole group to say. To me, I thought that that's what we had done. And maybe that is not what we did. But I thought that that was what the TAC presentation notification was doing. And maybe others didn't believe that. So that's a great clarification, Theo.

Jim, please go ahead.

JIM GALVIN: Thanks, Roger. If I may, let me try to walk through a potential example scenario that I think will speak to Theo's concern, if that's okay, Roger.

ROGER CARNEY: Perfect. Thanks, Jim.

JIM GALVIN: So I would image that a registrant goes to their incumbent registrar, they ask for a TAC, and they get a notification that the registrant, the account holder, asks for the TAC. The registrant gets a notification that a TAC was provided, and the registrant can now disable that TAC because they're going to get a means to do that, or there is at least a mechanism in that message that says you can cancel this.

Now the registrant goes about their business and they bring that TAC over to the gaining registrar, but maybe along the way they lose it and they know that they lost it. And if they know that they lost it, now they can go back to this message and they can click on "Cancel. Give me a new TAC. I don't want that one anymore because I lost it and I don't want it to be used." So that's one potential scenario in which all of this plays out quite effectively.

Another possibility is they don't know they lost it. The gaining registrar gets it. Somebody types in a bunch of stuff and they give them the TAC. And now the domain name transfers. And what I would expect is yet another notification from the incumbent

registrar to the registrant that says, “Okay, the transfer completed.” And in that message, the registrant gets reminded that, “Oh, I had a TAC. Wait a minute. I didn’t actually deliver that to my registrar. I don’t know how that happened. Let me click on “Claw that back.”” We have gotten as far as talking about what the clawback procedures are, but I’m imaging there’ll be some mechanism for that to all happen. And that second notification that they get when it completes is an opportunity for them to get it back if they didn’t really want it to happen or if it was improperly used.

Beyond that, you’re absolutely right. If accounts have been compromised, then all bets off. But that happens anyway. As a registrar, you either run a pretty tight ship and ensure that only the right people get into accounts, or you don’t. And registrars have a mixed point of view about how to handle those kinds of things. And I think that’s just the way it is. Thanks. I hope that helps.

ROGER CARNEY:

Great. Thanks, Jim. Theo, please go ahead.

THEO GEURTS:

So basically what I just heard [inaudible] if it is a comprised account, all bets are off and a notification doesn’t work. That is a correct assessment. But I don’t see, when we are talking about the [GIT] transfers, how the gaining registrar is going to send notifications, how that will improve security. In my mind, it will only create extra overhead in an already complex transfer process because now you’re going to request the gaining registrar to send an FOA or a notification to do stuff there, even though he just

started the transfer. And that is something I don't see as very logical in the sense that it doesn't increase security, in my opinion, because we're talking about [illegitimate] transfer. I think now we're putting way too much burden on the gaining registrar with zero outcome—I don't want to say zero outcome, but with little purpose there. Thanks.

ROGER CARNEY:

Thanks, Theo. And I'd just make a couple comments before Jim comes in. And, again, I think of if an account is hacked. It's most likely nothing we can solve. But I still don't think that 99% or 100% of the time, there isn't going to be a possibility that notification still helps because someone was sloppy. And maybe that is what it is, but that's not what we're trying to solve anyway.

And again, to Theo's point, we need to look at this because we're trying to solve the 1 or 2%—maybe it's even less than 1%, to be honest—of scenarios that happen. Today, 99% of them go through fine. Maybe I don't have the right numbers. So no need to quote me on those. But the majority of transfers happen without issue.

But the third point I want to make—then I'll jump to Jim—is I don't think anybody is saying the gaining registrar needs to notify anybody. I think that the notification that's coming out is going to be coming from, as Jim calls it, the incumbent registrar or the sponsoring registrar of the original. So I think that that's where the notifications will be coming from.

So, to your point of that the gaining registrars notifications will be very limited in what they do, I think that's what everybody kind of agreed with over the last couple. And maybe we didn't require the gaining registrar to send any notification when we went through the process. So just my comments on that.

Jim please go ahead.

JIM GALVIN:

Thanks, Roger. I do want to give credit here. It was Sarah who had first said that the gaining registrar may have reasons, business reasons, for wanting to send out a notification, but the losing/sponsoring registrar really may not anymore. So I agree with you on that point.

And, Theo, I hope I did not misspeak when I spoke, but I meant to say that, when the transfer closes, it is the sponsoring registrar that sends the final notification, not the gaining registrar. So I think we're all in agreement on the status of the gaining registrar. And whether or not they send something is entirely up to them and not in policy.

And with that in mind, I also want to observe that, from my point of view, I don't believe there is a benefit to the registrant in having the sponsoring registrar send them a notification when the transfer completes. And the sponsoring registrar obviously gets a value out of that themselves, especially if it happened and it was inappropriate. So there's certainly value to them in doing all of that.

I think that it's kind of subjective as to whether or not that particular notification should be required or not. So I think that you can have more discussion around whether or not the sponsoring registrar is required to send that final notification, although you can certainly indicate the reasons why it would be a good thing. But I think, really, all the security requirements go on the front end about making sure that it at least can start and is initiated in a proper way.

Providing a way to claw back? Yeah, probably a good thing. I'd certainly support that. I'm not sure that I would be 100% on the side of requiring it, but I leave it for the discussion here to figure that out. Thanks.

ROGER CARNEY: Jim, just a follow-up real quick on that. When you're saying "sponsoring," you mean the losing registrar sending that notice.

JIM GALVIN: Correct.

ROGER CARNEY: Because when it's done, the gaining registrar is now the sponsoring. What we're talking about is the losing registrar sending that.

And my only comment on why that seems useful to me is that theoretically those are two different people: the losing registrars/registrar may not be the same as the gaining

registrars/registrant. So if you're notifying the person that owned it a second ago, to me that's very beneficial to that registrant because it may not be the same person.

JIM GALVIN: Agree.

ROGER CARNEY: Okay. Thanks, Jim. Theo, please go ahead.

THEO GEURTS: Just to build up on that, we also still have the five due diligence [inaudible]. We sort of mentioned it on the losing registrar side. So there is that period also, coupled with a notification that the losing registration has to do when it comes to the creation of a TAC.

So I think we've got it from the losing registrar side. We've got everything covered to make it as secure as possible as we can from that point of view. And from the gaining registrar side, that notification that a transfer has started serves no real purpose, in my opinion, because, like I said, the transfer [was legit] to begin with. At least we have to assume that. So it doesn't make any sense to send a notification to the registrant. That's it. Thanks.

ROGER CARNEY: Thanks, Theo.

Okay, we're running out of time quickly here, so I will just end this with ... I think we'll continue this discussion, and hopefully it won't

take a whole lot of time next meeting. But maybe it will take the whole time. I don't know. But I would continue the discussion with the idea that—maybe that's part of the discussion ... I think everybody is agreeing today that the current gaining FOA cannot exist going forward. We're going to recommend getting rid of it as it exists today. But we want to follow that with that we identified that the current FOA does provide these three features or how many ever we come up with—again, the poll kind of identified; we can then come up with anything else—and we've used those three features or replaced those three features somewhere else. And, again, as I mentioned, I think the gaining FOA notification has been replaced by the TAC presentation. And maybe we just need to make sure of that. And maybe I'm wrong. Again, please let me know.

But I think the homework for the next week is to look at that thing. We're going to get rid of it, but these three things exist and we've done these things to those three things. So we've kept them. We've put it here or we don't need it all. It's not a feature that needs to continue to exist. So think that that's the homework between now and then. Hopefully, we discuss that next week and we can resolve that. And I think that will probably at least, for now, end our discussions on the gaining FOA.

Does that make sense?

All right. We have one minute left. I don't know if staff has anything. Okay. Well, we can wrap it up and I'll give everybody a whole 60 seconds back. Thanks, everybody.

[END OF TRANSCRIPTION]