ICANN Transcription

Transfer Policy Review PDP WG

Tuesday, 25 October 2022 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/EwVpD

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. Welcome to the Transfer Policy Review PDP Working Group call taking place on Tuesday, the 25th of October 2022.

For today's call, we have apologies from Sarah Wyld (RrSG) and John Woodworth (ISPCP). Sarah assigned Rich Brown (RrSG) as her alternate 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. Observers will remain as an attendee and will have access to view chat only. Alternates not replacing a member should not engage in the chat or use any of the other

Zoom Room functionalities. If you have not already done so, please change your chat selection from host and panelists to everyone in order for all participants to see your chat and what's captured in the recording.

Statements of Interest must be kept up to date. Does anyone have any updates to share? Please raise your hand or speak up now. Okay. I'm seeing no hands.

Remember, please to state your name before speaking for the transcription. Recordings will be posted to the public wiki space shortly after the end of the call. And as a reminder, those who take part in the ICANN multistakeholder process are to comply with the Expected Standards of Behavior. Thank you. And over to our chair, Roger Carney. Please begin, Roger.

ROGER CARNEY: Thanks, Julie. Welcome, everyone. Just a few quick updates—maybe a little longer than quick—but a few quick updates before we jump into our agenda work on getting past Recommendation 2 and on to 3 and 4. But first off, just a reminder, there will not be a call next week due to the summit next week. Starting shortly, the week after that actually, we'll be going to two days a week. So many of us will be in Los Angeles at the summit and will probably talk about transfers, but we won't have an official meeting next week but we'll start up twice a week the following week. So I just wanted to make sure everybody was on that so that we're ready for that.

The other couple of things we have to cover that Berry had sent out, kind of a visual of the description on where the losing FOA fits or I should say the functionality of the … and he … the initial report state and maybe the stepping stone to get us to where we can resolve many of these comments. So maybe I'll turn this over to Berry—thanks, Emily, for posting that—and have Berry take us through this real quick. Please, if you have any questions, jump in and ask Berry or I or anyone. Berry, please go ahead.

BERRY COBB: Thank you, Roger. Berry Cobb from staff for the record. First off, apologies that we didn't get this sent yesterday. Our wires were crossed about getting it to the group. So I'm sure you haven't had enough time to really absorb what is trying to be represented here. I did provide a few bulleted talking points to the e-mail that Emily sent when she sent it earlier. I'm just going to try to basically try to repeat that from a verbal perspective to hope to reinforce what we're trying to accomplish here.

First and foremost, this is very much conceptual in nature and not a complete representation of all of the mechanics that go on when doing a domain transfer. But reading through the current policy as it exists today, what the group came to preliminary recommendations in the initial report and kind of based on some of the deliberations for reviewing through the public comments, what you see here basically kind of three depictions in that order.

The first kind of takeaway from here is that this is kind of roughly divided in fake phases, for lack of a better term. None of it can account for all of the variabilities that may occur during a transfer

such as if the domain is locked or there are several reasons why the domain can't be transferred at a particular given time, all of the various denial reasons and those kinds of aspects. So it's really just trying to focus on when the transfer can happen or basically when it when it's eligible, meaning that all issues have been cured, the domain is no longer locked, it's assuming that at some point in time, the Auth-Info Code or the TAC is submitted with the gaining registrar.

Then in between each of these vertical bars are the primary tasks or part of the process that's trying to be achieved with a focus on the timeframes by which these activities will occur. I think what is kind of neat about this approach is, you'll recall the swim lane that we developed in preparation for the initial report, one of its deficiencies is that while it's a closer representation of the all of the process steps that can occur through transferring of the domain name, it can't represent the timeline or the timeframes at which all of these different steps take place. So this is kind of a different view of that.

So starting up at the top is the current state, and I think the main takeaway here, which is part of the reason why this group got initiated, is the gaining FOA and the authorization that takes place was essentially broken due to the implementation of Temp Spec as a result of the GDPR and the masking of registration data. The current state of the industry has been operating for several years without this component. And as you can see, in the two examples below, the working group is preliminary recommending to get rid of the gaining FOA. But I did find it interesting that going back and looking through there that when an a transfer was initiated at the

gaining registrar that it could live as long as up to 60 days, of course, pre 2018 May timeframe. Then, essentially, once the domain is authorized for transfer, there are a series of EPP pull commands that initiate the transfer and to complete the transfer, as well as the current state where there's a requirement about the registrar of record submitting the losing FOA within 24 hours and the ability for the RNH to deny or NACK the transfer, should they choose to do so. And of course, at the end of that process, if there is no NACK and there's no response from the registrar of record, then the default approval is also set at five-days, by which in essence, the transfer would be completed.

When we move to the initial report section, I know what is included here is kind of outside of the scope for what we're trying to accomplish in Recommendation 2 and about whether the group determines to keep or continue to not support the losing FOA. But when looking at the broader context, I thought it was still helpful to include these other aspects with respect to timeframes. I think what's interesting here is you can really start to see a shift of what some of the preliminary recommendations do to current state about when the domain is actually eligible for transfer and some of the notifications that the group has preliminary recommended.

When we get into the middle of the process, one of the recommendations is that the TAC has a 14-day TTL. I know it's probably not an accurate reflection of what goes on in the middle part of this section, because right below that bar in the middle is the transfer and process. I didn't come up with an easy way to show that the TAC that gets submitted to the gaining registrar could, in effect, literally take place within five minutes or less than

five minutes at the gaining registrar. But if they don't, in effect, they could also wait until 13 days and 13 hours or 23 hours later before the TTL expires and still initiate the transfer process at the gaining registrar. But the idea is that the moment the TAC is submitted at the gaining registrar, that's when the transfer processes is ultimately initiated. Again, kind of the EPP pull commands to initiate and complete the transfer are roughly triggered.

A grain of salt here, I have no direct experience with how EPP really works, and hence, my disclaimer about this being conceptual. But the takeaway here is that once the domain is transferred, there is the transfer completion notice that's required from the losing registrar or the former registrar of record, the TAC is cleared so that it's not used again and of course as a different recommendation. Preliminary recommendation is about applying a prohibition on a transfer for 30 days.

Then finally, the last row is pretty much the same as the initial report. The only difference here is that the group is considering whether the losing FOA should be retained or not, and I've highlighted that in orange. Again, this in no way is meant to represent that there's a final decision here. There was some discussion about whether an authorization could be done up to the 120 hours but the TAC hasn't technically been disclosed yet or revealed to the RNH. But once it is revealed, the TAC notification that it's been revealed. Of course, the difference here is in the middle section, if the losing FOA is retained, what are the possible durations for that losing FOA to be sent? How many days should the registered name holder be able to NACK the possible

transfer? That really depends again when they would submit the TAC to the gaining registrar to kind of initiate that process. Based on what the group ultimately decides, we can move the losing FOA stuff around as necessary. But at least I hope this provides kind of a simple visual to understand what's going on and can help the group with deliberations. Thank you.

ROGER CARNEY: Great. Thanks, Berry. I think we'll just jump here right into our continued discussion from last week. Again, I know some people wanted to see this and see how visually looking compared. I think the important thing that we got to over the last couple of weeks is this piece in the orange here, I think everybody has agreed that it needs to be pulled back in so that we can get that functionality back to the registrant. I think Jothan was calling it last week agency. We'll use that term. I don't know if that's correct or not but it seems to fit. The registrant has that opportunity to NACK the request before it's actually completed there, giving them that functionality back that they currently have today. So I think that this piece of orange, the only discussion that I think we left last week was, okay, where does this belong? Can this fit in the same five-day window that the registrars have to provide the TAC? Or, as Rick mentioned last week, maybe it makes more sense if we're going to keep this functionality, to actually keep it in the place that it is today. And not just because it's easier system changes, there's no changes to make, but also that the registrants don't have to learn a new process that obviously registrars will have to walk them through for the foreseeable future. So I think that's

where we ended discussion was, where does this little orange piece fit best? Theo, please go ahead.

THEO GEURTS: Thanks. This just looks pretty good on paper. But we are adding still additional complexity to the process. Now we started with the creation of the TAC where the registrar sends a notification where the registrant can either deny. In my eyes, the flow is like that you can create a TAC and you can either nullify it or just go for it, then you start the transfer process. Then we start sending a losing FOA, which does not need acknowledgement. I wasn't on the call last week and I forgot to listen back to it, but it requires an additional action. You basically have made the process more complex. Thanks.

ROGER CARNEY: Great. Thanks, Theo. I think that the idea last week wasn't that there was anything additional besides the fact that the losing registrar would send the registrant that notice that, "Hey, this is about to be transferred. If you don't believe this is correct, click here or whatever." Provide instructions on what those registrants can do to stop it and give them a window of time as they currently have today. Again, that window of time I think is up for discussion. I don't think anyone really had an appetite to change it last week but maybe they've thought things through, and maybe it can be shorter than the current five-day window or it stays the five-day window, which I think is fine as well. But yes, it still as it is today. It's an auto ACK situation where if there is no response, it's

assumed that the transfer is good and it goes through just like it is today. Rich, please go ahead.

RICHARD BROWN: Hi. I want to discuss this a little bit, actually. Thank you, by the way, Berry. This is great, although I kind of have issue with the underdeliberation based on BC. Initially, I had mentioned that when we get the TAC request, we should send a notice saying, "We received the request for NACK. Click here to get it immediately. Otherwise, it'll be sent in five-days." That step is not listed here.

Also, the losing FOA, while the domain's pending transfer, there really is no pending transfer. You got to remember we wrote this TAC process under the idea that the losing FOA was going away. And you can see here how the losing FOA really does nothing if we put it back in. Because once the domain is eligible for transfer and it's submitted, done, transfer is done. We can send an e-mail but that transfer probably already went through. Once again, no room to NACK, because even here on this chart, the transfer has already been submitted. And once it's submitted, there's no NACKing because it's already done at the registry. Because once they get the TAC, they process the transfer.

So that's where I have issue with this chart. Well, not really issue, it's just I think it's proving that the NACK and the losing FOA do nothing, and by putting them back into the process continued to do nothing as we've rewritten the TAC process. That's why I'd like to see the option to decline, basically, in this case, decline the NACK to be up front. Well, yes, they must inform the gaining

registrar about the TAC. But the minute the TAC is released, that transfer is live. I can take two seconds submitted at the new registrar, and then the registrar sends their code and it's gone. Then the five minutes it took me to open, get my e-mail and all of that, my domain is already gone. So it sounds like a lot of people have things to say. So, go right ahead.

ROGER CARNEY: Great. Thanks, Rich. Yeah. I think the idea, Rich, is this orange box maybe moves to a new section here in the last part where it does go back to what it's doing today at the top and when the gaining registrar submits it to the registry that submits the TAC, that what we're suggesting here in this deliberation is that that does go to a pending transfer. And that that pull message is created for the losing registrar so they notice that there is a request that this TAC is being used and that they can get a confirmation from the registrant. Again, that would be that window where there would be again a pending transfer is what is under deliberation here from when the gaining registrar submits it to some window. So I think that that's where this orange piece would move to if it's moving as some suggestions for keeping it to where it is.

Otherwise, Rich, I think what you're suggesting and you have suggested for the last couple of weeks, I think, is this can actually be moved into the state before it. And when a request is made, the registrar sends a notice to the registrant prior to the TAC being provisioned. I think that some of the arguments against that were that still exposes for a period of time up to 14 days when the TAC is provisioned, that TAC is vulnerable then and can be stolen at

that point. Again, a lot of hypotheticals here, how often it happens, I don't know. But it is an exposure that if you provide the NACK feature prior to provision, once it's provisioned, the TAC can be stolen, or however you want to say it, and used to enforce this. If you put the NACK at the end, then it stops that ability. Someone can steal it, but then the registrant still gets the option to stop it. So I think that hopefully that's clear. Rick, please go ahead.

RICK WILHELM: Thank you, Roger. Rick Wilhelm, Registries. I'm generally agreeing with Rich's comments and observations about the cause and effect, and also, Roger, with your comments there about elaborating on the same. Just one thing that I want to clarify and elaborate, which is a little bit of a change from what Richard said with regarding the rationale about what was done with the TAC, because the security of the Auth-Info was kind of a mess because there were really no requirements on the Auth-Info Codes and they were generally long lived. That means they would get provisioned at the beginning and they would be running around unencrypted and they would be distributed all over the place. The way the TAC currently works, it kind of takes away a lot of those things and makes them short lived and puts other security requirements on to make those TACs more secure. So that's just saying something that everybody already knows, just putting a little bit of a spotlight on it. That's all. Thank you.

ROGER CARNEY: Thanks, Rick. No, it's a good reminder that we did make other changes to the TAC, the Auth-Info, that provide additional

measures. And as you called out, obviously Auth-Infos today on a lot of parts live forever and it can set in someone's e-mail for a year and someone can get into somebody's e-mail and use that and transfer it. So it's one of those where it's a little different. Obviously, our TAC is only going to live for 14 days and is only valid post request, post approval by registrar. So yeah, there are a few other measures that we put in place that add to this. So thanks, Rick, for bringing that up. Theo, please go ahead.

THEO GEURTS: And maybe I missed it in the last call last week. But if we are going to add additional requirements, then maybe it's not a bad idea to see if we can bypass the problem entirely, which is when a TAC request is made, that doesn't, in my mind, equal the generation of a TAC. I mean, if a registrant wants to generate a TAC, then we send a message, "Okay, we can generate a TAC for you. Do you wish to proceed? Yes or no?" If that request or that idea of the generation was not a valid one, then the registrant just clicks on "No one to e-mail," and no TAC will be generated. And there hasn't been an existing TAC because we didn't generate it yet when it was requested. So then you bypass the entire problem of sending losing FOA during a transfer, if that's possible or not. You just do it right at the front of the initial request of the generation of the TAC, you approve that or not. As soon as it's approved, you generate a TAC and you provide the registrant with a TAC. That would be a much cleaner process because then if the request was not valid to begin with, there is no TAC that can be compromised. Thanks.

ROGER CARNEY: Great. Thanks, Theo. Originally, I was thinking along that same path. I don't know that some registrars may even do to begin with. When I was thinking about it, when we talked about it last year, I was thinking that registrars would do that during that five-day period that they get. But I think that some of the comments brought up the fact of there's a window from when the TAC is provisioned and given either in the registrar's portal or secure e-mail, text, however it goes out, when that's communicated, there's a point of that TAC is the complete end-to-end solution here. So as soon as it's given to the gaining registrar, the registry is going to process it and it's going to be gone. So if it gets stolen in that time where it's provisioned to when it's being used, it could go somewhere else and not where it was intended to go. So I think that that's why the idea came back of, well, today's losing FOA—again, I don't think we need to pull back the losing FOA—but the functionality that gives the registrant the ability to stop the transfer once the gaining registrar is known, that functionality is still valuable to people. I think that's what came out in public comments is that ability to stop a transfer once the gaining registrar is known is kind of critical. Again, because that TAC could fall into the hands of someone else, they may take it to a different registrar and they wouldn't know. I think that that's why instead of it being in the first five-days, it adds another measure. If it's in the last five-days, basically, it would transfer. So I think that's the argument of the two sides is yes, the first part makes it cleaner to me, I think, as Theo mentioned, it seems like, "Okay, did you do this? Yes or no?" Then they could say yes right away or they could wait five-days or however long it is, or they could say no right away or is in that period, and then the TAC doesn't get

created and it's much cleaner. But I think that the problem is there still that possibility of exposure once the TAC is provisioned. Putting the ACK/NACK functionality at the end removes that issue or at least lessens that issue, I should say.

Again, I think that that's the whole point where we left the discussion last week and what this chart is trying to show. Hopefully, this helps everyone. I think it makes a lot of sense to me as where does those orange boxes get moved to because, again, I know Rich has talked about it. It's what I thought originally, it's what Theo just mentioned that those orange boxes could fit that stage or whatever we're calling this before where they're listed right now in that first five-day window, but I think it still leaves one exposure that the commenters have brought up. Whereas if we move those two pieces to maybe a stage or whatever we're calling it in between those last two, when a gaining registrar actually uses it and as it was today, the registry just puts it in pending, notifies the losing, and then the registrant gets that chance. It covers that measure of the exposure between provision and use. That way, the registrant, if they know, can show that are approved, "Yes, that's where I wanted that to be moved to."

So I think those were the arguments. Again, I think that Richard, Theo, and again, how I thought it was going to work even last year was it would be put in the stage before, but I think putting it in between the gaining registrar and making that pending and providing a window provides the solution that the commenters brought up that I hadn't thought about that as well.

Yeah. Thanks, Rich. This is something hopefully Jim—and I don't remember all the other people that volunteered because I kind of

voluntold Jim—to look at the threat vectors. I know that they're going to plan to talk about it next week as well. But one of the threat vectors is the account gets hacked, and then it's out the window. That's true. But if that TAC gets exposed somehow or if it's a web developer that can ask for the TAC and the registrant is actually the one that is approving these things, maybe the web developer just wants to move it and yet they have notified the registrants, they were going to move it. So the registrant can be a part of that. So I think that it's not necessarily just specifically when the account gets hacked because we're not trying to solve that issue. We're trying to solve the other issues around if someone gets the TAC somehow, I don't know, someone sees it over the shoulder, it gets copied to somebody, a forwarded e-mail to another person within the company and they get to move it, those kinds of things can happen. As long as that TAC is provisioned, it can move in our current recommendations. So I again, I think that there's several scenarios that is not an account hacked scenarios where this TAC can be exposed. I think that moving the ACK/NACK functionality to this pending state after the gaining registrar submits it solves those few outliers there.

Rick, is that a new hand? Thank you, Rick. Owen, please go ahead.

OWEN SMIGELSKI: Thanks, Roger. I just kind of want to add on to what Jim put in the chat about how it's kind of a warm, fuzzy option but people don't really necessarily understand. And yes, I understand for a lot of the public comments we received, these are people who, for a long time, this is what they've experienced. When there's this type

of change, there can be some unease with the unknown, especially when for them, this is something that has always been there, has always done that. If what we're trying to do is make something more secure, Roger, you mentioned this was for some outliers. This is going to represent a significant effort in terms of adding, changing, updating already as it is and adding more stuff in there. There's even going to be more development costs for registrars, registries. And if we're going for what are outliers, I don't think that necessarily justifies the work for the handful of times this happens. We're looking at something that's 30%, 40%, or 20%, a significant chunk of things that I can understand that the basis, this is something that you may not necessarily be a cost center for registrars, and so it's kind of something you've got to do just to do, you're going to lose money on it. It's hard to justify that when if this is solving 0.2% of transfers out there—I'm just throwing numbers out there—but if we're going really for extreme scenarios, I'm not sure that really it's worth the efforts that we've got to take care of. I mean, if we're doing something to improve security, make sure your accounts are secure so that there's less chance of hacking, require two-factor authorization to log into a registrar panel. Something like that could actually solve these problems of not having access to it. But I think just having an FOA for the sake of having the FOA to keep people comfortable is kind of silly, in my opinion. Thanks.

ROGER CARNEY: Great. Thanks, Owen. I think Rick kind of touched on it last week as well. Really, if we ended up pulling this functionality in and placing it between the gaining registrar submitted and in the

registry putting it in pending, it's really no different than it is today. So honestly, if this moves to pending cycle, post gaining registrar submitting it, the dev cycles, the communication cycles, and everything like that to registrants will be considerably small compared to if we move this to the first five-day window. Again, I think Rick didn't have a whole lot in that and doesn't as a registry, but you're right on if we decide to move this, to me, there's a bigger impact system-wise and education-wise to moving this forward than to leaving it basically where it is today. Just my thoughts on that. Catherine, please go ahead.

CATHERINE MERDINGER: Thanks. Maybe I'm not totally understanding the conversation we're having, which is very possible. But are we able to really come to a conclusion here without seeing what the small team gives us? Because my understanding is we can talk about this but the answer is still like, "Well, small team, try and figure it out for us and come back and tell us what do you think." So are we just a little bit beating a dead horse? Unless I'm misunderstanding, which is again, very possible.

ROGER CARNEY: Great. Thanks, Catherine. The small team is really tasked with looking just at the different threats that can occur in a transfer process, and maybe just a little wider in a transfer process. We're not talking about necessarily the small team making a decision here on this, not at all. They're just documenting what threats this group sees and what we are trying to solve and what we're not trying to solve, so that when someone says, "Well, you're not

solving the problem with half the account," it's like, "You're right, and we're not trying to." But we are trying to solve the problem of if someone breaks into someone's e-mail, the TAC gets used that the actual registrant may have a chance to NACK that. Again, I don't think that the small team is purposely looking at where this should go or if it should be at all. They're more looking at it more general, "Okay, what are the threats, and are we trying to solve them or not? And if we're trying to solve them, how are we solving them? And if we haven't solved them yet, okay, where's that gap?"

CATHERINE MERDINGER: Thanks for that explanation. I think I was confused.

ROGER CARNEY: Great. Thanks, Catherine. Theo, please go ahead.

THEO GEURTS: Thanks, Roger. I am not completely sold on the accidental authorization code that somebody is accidentally looking at some screen and then captures like 84 characters arrive into their mind, somebody with a photographic memory, and then goes out doing bad stuff. In my mind, that doesn't happen. If you're dealing with stuff like that, you shouldn't be posting your boarding ticket of your flight on social media. Bad things can happen. If we go into these edge cases—and they are edge cases in my opinion—then we keep adding additional security features which they'll always be bypassed. So the idea of having a risk assessment, that is not a bad idea. But I think what you will find if you make a risk assessment—and we've seen a couple of cases in the past where

some high profile domain names were being hijacked and where the attackers took a completely different route than the regular process that we are looking at here on our screen with FOAs and that kind of stuff—they just went for social engineering. Because that threat profile for those domain names, those guys had a completely different idea on how to make sure the transfer happened, and that was through social engineering. If the risk of a domain name is high enough then you are going to face are going to be text, you will be facing a text that are highly complex which no policy can account for, and that is what I've been saying all along. If somebody really wants your domain name, he is going to get it regardless. I mean, a skilled actor will get it. The policy, regardless what you put in there, it's public. So any threat actor, any criminal can work around those issues. It's never going to eliminate the issue. As long as the domain name is very, very valuable or it has a very important function, it could be used in cyber warfare to disrupt some kind of service. I mean, if the target is valuable or important enough, all bets are off. Thanks.

ROGER CARNEY: Great. Thanks, Theo. I agree. I don't think that someone looking over someone's shoulders, it's going to happen. But obviously, someone could e-mail the code to somebody and say, "Take care of this. I'm on vacation or whatever. I don't have time to do it." So I think that there's still possibilities where this can occur. Again, someone just has your e-mail or access your e-mail, whatever it is. Again, are these numbers, as Owen says, small? I think they're very small. To me, it's a little hard. If we move this to the front, everyone has work to do, including education, and we lose that

measure of that even a tenth of percent or whatever it is, maybe smaller, I don't know, of transfers, we lose that measure. Or if we leave it where it's at, we still get that measure—and again, no matter how small it is, we still get it—and no one does any work and there's no education needed, to me, it just seems like it solves itself. But again, I'm not here to make that decision and the group is here to make that decision. So I think that, again, it's up to the group. I don't remember who reminded us last week or week before, if there is no consensus on change, we will stay with what we have today and make no changes to it. So if we can't decide on this, if some people in the group want to move it forward into the five-day window, when some people want it in the pending window, it's really going to default back to the current losing FOA. Notice that has to be sent and it's going to be in that pending window. So just my thoughts on that.

Okay. We've had great discussions. The Registries have jumped in on this. The Registrars have voiced their opinions on it. I don't know if anyone else, BC, IP, any thoughts on this? Any comments you want to share? Steinar, please go ahead.

STEINAR GRØTTERØD: Hi. I'm not 100% sure about how At-Large will address it, but one of the initial ideas we had and my way of understanding the discussion in the CPWG is that we want to have a secure, safe, and reasonably fast transfer process as possible. I think that however how much we discuss it, I think the security doesn't necessarily lie. Or, at least in my opinion, privately it doesn't lie in the policy. It lies in the registrars and their way of securing their customer data two-factor, etc., etc. I think it's maybe not the

correct word, but it is a shame that we cannot agree upon something that doesn't take that much time, the 60 days window, etc., like it is now, the waiting for the TAC and all these things. I think we have to identify that, that what we initially said in the working group was definitely a great step forward. We have made the process in securing and getting a more secure TAC in the TTL on the TAC and we have a process of NACKing or sorting out if there is there an [altered] transfer. I think that is much, much better than it is today. So I sincerely hope that we can get on to some sort of agreement that kind of mirror something what I just said, that it must be a little bit faster, not too complex. We have to teach the end users, the community, about it one way or another. Thank you.

ROGER CARNEY: Great. Thanks, Steiner. Okay. Any other comments? Zak maybe. If Zak has anything, BC comment on this? If not, no big deal. I just want to make sure everyone has a chance.

ZAK MUSCOVITCH: Hi, Roger. Thanks very much for the opportunity. I'm afraid I'm just getting back up to speed after missing a couple of weeks due to COVID, etc. So let me get back up to speed and circle back after I consult with BC. Thanks very much, Roger.

ROGER CARNEY: Great. Thanks, Zak. Again, anyone? It sounded like the last two weeks and even since ICANN, the idea of this functionality should be pulled back. So I think the issue is not if this functionality

should exist or not, it seems to be well. And even if some people think it may be a little fluffy, I think it does solve some out there. Again, we're doing it today so I think the important part is—and I think Rick brought this up last time—is the smaller changes, the better on these. Give it some thought and I think we can move on from this today. Obviously, the functionality we're looking here, it's just where that functionality should lie in the process. I think let's go ahead and move on from this and jump into Recommendation 3, which I think we started last week as well. Yeah, let's pull up the Rec 3.

EMILY BARABAS: Sorry, just one moment.

ROGER CARNEY: No problem. Great, excellent. Thanks, Emily. Again, this is on the TAC revision, which we've kind of touched on a bit. Obviously, it's one of the gates that we've been talking about here. But there's a few comments we should work through and see if we can either answer the comments or incorporate any suggestions that makes sense. Emily, please go ahead.

EMILY BARABAS: Thanks, Roger. Hi, everyone. This is Emily from staff. As we talked about last week, one of the considerations regarding Recommendations 3 and 4 about the notification of TAC revision and notification of transfer completion is whether these notifications will be kept on the recommendations regardless of what the working group recommends regarding losing FOA. So I

think that that's still a question for discussion. But if it's helpful at this stage to move forward with the comments under the assumption that these two recommendations will stay in place regardless of the outcome on Rec 2, we can dive into some of the specifics. Is that the path you'd like to take, Roger? Or do you want to talk a little bit more about whether these notifications make sense in combination with the other elements?

ROGER CARNEY: No, and definitely. Thanks, Emily. I think we can take that path. And not only that, but I think that obviously Recommendation 3 to me it's not really a question if we take the path on the losing FOA or not. But to me, Rec 3 has to exist. Now, is there something that if a losing FOA is in there changes it? I don't think so. But we can obviously cover those. But I think Rec 3 is one that it has to live on, even if we decide not to do a losing FOA or if we do decide to pull it in somewhere. I think yes, let's go along with the assumption that these need to reside in and let's try to either update them with appropriate comments or at least answer the comments with our deliberations before or now. Emily, please go ahead.

EMILY BARABAS: Thanks, Roger. Would you like me to then just walk through the issues one by one and we can—

ROGER CARNEY: Yeah, let's go ahead and do that. Yeah, please. Thank you.

EMILY BARABAS: So the first few comments are actually more applicable and we went over them on the last call to the conversation about the elimination of the losing FOA. Since we did review those, I think we can more or less move forward and will be covered there. There was a question or a suggestion that the notification should be sent to additional contacts, and in particular that tech contact would be an important recipient. It's worth noting here that this notification was envisioned to potentially be combined with the actual provision of the TAC. So obviously, that would not be the case that you would be e-mailing the tech to all of the contacts. So if it were to be the case that this notification that the TAC has been provided was to be sent to more contacts, it would have to be split out from the provision of the TAC itself by e-mail. But I did want to note that suggestion and see if there were any inputs on that. Thanks. Okay. I'm not seeing anyone. Is it possible that folks have reasons that they'd like to share that they think it's not beneficial to send to additional contacts? It's helpful to have that in our discussion as documenting that we've discussed these comments. Thanks.

ROGER CARNEY: Great. Thanks, Emily. I agree either way, if someone supports sending it to additional. I think the tough part is if the communication is generic in form, sending to other contacts doesn't seem like there's a big harm in that. I suppose there could be a time. But if you're including the TAC in that communication, to me, that's where it gets difficult sending it to multiple people, again, because it being the key. Theo, please go ahead.

THEO GEURTS: Yeah, I'm actually struggling with that language. I mean, the ideas need additional contacts. But my first question is who would those contacts be that contact admin? I mean, they are all going away, at least in our system. At the moment, we are allowed to remove the admin contact. It's going to be gone. The same goes for the tech contacts. The billing contact is no longer utilized so we don't even collect that one anymore. So that is basically the big discussion is do you want to have your database full of additional contacts, which can be a risk when your database is being breached, because now you're going to have multiple issues versus the discussion, is it actually that useful to contact multiple persons? That is, there's definitely a trade off there. Then there's also a little bit the question of when—okay, I'll just leave it here. I think it's already complex enough to make a decision. Thanks.

ROGER CARNEY: Thanks, Theo. I agree, I think that it does get a little complex when you start. To your point, Theo, really, you're only talking about the possibility of the tech contact here, if it's even collected, which is an optional thing to do. So I think that gets a little difficult. Again, I don't know sending notice to the tech. I mean, obviously, you do want to make that known up front when the request is made or even prior to that that if a transfer is requested that the other contacts may be contacted or notified of it just for other reasons. Maybe it's legal reasons. There was no reason to notify them. Again, get back to, is it required to make the transfer happen? I don't know. I agree, Theo. I think it's a little tough to add additional contacts, but it seems like it doesn't hurt in the general sense, but

I think there's specific areas where it could be. Keiron, please go ahead.

KEIRON TOBIN: Thank you. From the registrar perspective, you'll find that a lot of contacts are usually the same in instances where there may be different. It may be because of companies or corporate companies. But I would have no issue in suggesting that if the registrant name holder wanted to forward it on to the tech contacts, then they couldn't do, it was different. But that is probably about as far as we go without going into kind of the complexities like Theo just discussed. Thank you.

ROGER CARNEY: That's interesting. Thanks, Keiron. Jim, please go ahead.

JIM GALVIN: Thanks, Roger. Just a comment, I guess, for consideration here, as you're thinking about must versus should, and how much from a security point of view, it's important to keep in mind that the principle of notifications is essential. It's an important part of the overall security of the system. So the question of whether to notify at request time versus provision time, what I would offer is it depends on how far apart those two steps are. If you are provisioning more or less in near real time with the request, then one notification is fine. If you're going to have a request and you're going to have a review period before you actually provision it, then you probably should have two notifications, quite honestly. Because you just need to make sure that each of those events are

covered. It's an important part of the overall security profile that those events, which are significant security events, are available and observed by the party. So that's one point.

The second point is should you tell more than one person? I think that given some of the larger activities going on with the presence or absence of contacts and roles and whether they're there, certainly at a minimum, the registered name holder must be notified. We already have that up above. I think from a security profile point of view, it's good to notify more people than less. But I would think that rather than being prescriptive about must notify the tech contact or something, I think it would be an advantage to say that you should notify whatever other contacts you have available to you. But I don't think it would need to be required. There's no additional security advantage to doing that. But it is helpful to do that since you never really know if they're different or the same. And making that distinction is probably something if they're all the same, then there's really little point in doing this. On the other hand, maybe that's part of the recommendation. If they're different, you really should because it is an enhancement to the overall security profile to do it, but I don't think it needs to be required. So that's just an observation for folks to consider. Thanks.

ROGER CARNEY: Great. Thanks, Jim. Volker, please go ahead.

VOLKER GREIMANN: I'm basically on the same level here. I don't think sending around hundreds of thousands of e-mails for one transfer is beneficial for the community or for most registrants. If I look at the database or registrations for our registrants, for example, a lot of registrants use our data as technical contact by default. A lot of resellers do the same. I'm asking myself what the benefit would be to send ourselves or our resellers this notification.

I think what could be interesting is if we allowed the registrant to specify a transfer contact that is not part of the registration data, basically, that could be associated with a domain name and then notify. Simply because of the fact that, in many cases, the compromise of an e-mail address results in, A, the transfer of the domain name not being noticed and, B, also all notifications that happen afterwards being caught by the hijacker. So having an additional contact as a suggestion, I wouldn't call the best practice, but as an additional contract that's not part of the registration data as [inaudible], that might be an interesting idea. But using the contacts that we have currently on file I don't think adds anything. Thank you.

ROGER CARNEY: Great. Thanks, Volker. Any other comments on the additional contacts? Theo, please go ahead.

THEO GEURTS: I just struggled to see how you're going to make that work. Because if you would allow such a contact, it's not a bad idea on its face, but it assumes that a registrant makes a very conscious

decision, is very security aware, make sure that everybody he sets up the data for all those contacts, that all those people are informed, that there's a legal basis there to do so. Those are all assumptions. I think in reality, people are usually not very security aware and they just enter some data from a friend or an uncle or an aunt or whatever. And all of a sudden, you have all these contacts in your system which I think you might not have a legal basis for and maybe you weren't aware of it as a registrar. But I see a complex security mess coming up due to the reasons I just mentioned before. But I also see legal issues coming up. Thanks.

ROGER CARNEY: Great. Thanks, Theo. Volker, please go ahead.

VOLKER GREIMANN: I tend to I agree with Theo to an extent. I think it would have to be an alternative e-mail address of the same person, that if they have a separate account with a different mail provider that they could use for that. I also see some use for that for corporate registrations, where this could be an additional service that we provide where we have an additional notification against transfers. Although I think that those domains should be protected by domain lock anyway, but that's a different story. I think it might make more complicated and I just think we shouldn't preclude it and I don't think we do so. If we specify that the registrant being contacted that we just say, at a minimum, the registrants that allows a registrar to offer different venues of notification but does not require it, I think that could be something that is worth considering. Thank you.

ROGER CARNEY: Great. Thanks, Volker. Steinar, please go ahead.

STEINAR GROTTEROD: Hi. One of my day jobs is actually working for a corporate registrar and I do see some sort of benefit in having a transfer account or transfer agent or something like that. But don't we end up in a scenario that could create problems if an e-mail is sent to the registered name holder and to the transfer contact and one of these NACK the transfer in a way and the other one approves it? Who will have the right to do so? Both or only the registry name holder? Thank you.

ROGER CARNEY: Great. Thanks, Steinar. I was trying to think down those paths, Steinar, as well. I mean, it seemed to split off that, obviously, the actionable ones could only go to one direction, a notice, a non-actionable list of, "Hey, transfer was requested" or whatever it is. It could go into multiples. But I guess what I'm falling back to is should it be policy driven? I mean, I think if we say it must go to the registry name holder, okay, that's fine. But let the rest of that up to the registrar's business model dictate if they're sending it to a tech contact or if they want to create a transfer contact or a transfer agent, let that live with the individual registrar. "Does that need to be policy?" is I guess the big question to me. Thanks, Rich. It's kind of the way I was heading down. Rich's chat on authorized agents and things like that.

Again, I think, when I summarize what I think I've heard is let's leave this as a must to the registered name holder and let the other contacts fall outside of this policy. Again, if a registrar decides to notify someone else, I think that they would have to be able to support that reasoning. But that's not necessarily a policy thing. Okay. Emily, let's move on to probably the bigger topic. We've got about 22 minutes. Emily, please, let's go through this.

EMILY BARABAS: Thanks, Roger. As you'll recall from last week's call, we had a number of comments on the language of Recommendation 3 raising concern that the recommendation language doesn't sufficiently take into account cases where the customer is using a privacy or proxy service. Specifically that, in such cases, it should be clear that, as is the case with the losing FOA where there's access to the underlying customer data, the notice should be sent to that underlying customer as opposed to the service provider.

What we've done here is drafted some draft text for an implementation note for you all to shoot down if you think it's wrong or add to if you think it's on the right track. This actually combines both that concept. Also, we got a number of comments that it seemed to be confusing this clause here that says, "As listed in the registration data at the time of the TAC request," which is referring to the snapshot of what data should be used in terms of contact information for sending the notification. But I think when people were seeing that in the context of the notification of TAC provision, it was creating confusion. So what we're suggesting to do here is to take that out and add the text about where the point in time in which the information should be used for

sending that notification. For the purposes of sending the notification, the registrar of record should use the contact information as it was in the registration data at the time of the TAC request and then adding a sentence, “In cases where a customer uses a privacy/proxy service, the registrar record should send a notification directly to contact information associated with the underlying customer where it’s possible to do so.” So that’s where the registrar is also the privacy/proxy service.

One question for input that we’re hoping to get from you all, we noticed in some of the comments that they reference both privacy and proxy services, but it was our understanding that the proxy service would be the RNH. Whereas for a privacy service, that’s the underlying customer, that’s CRNH. So our question is, should this actually just be referring to those specific cases where a proxy service is being used? I will pause there. Thanks.

ROGER CARNEY: Great. Thanks, Emily. Again, this brings up a lot of old memories in the privacy/proxy policy that was being worked on from years ago. I think important things to tease out here, and especially getting answered. Theo, please go ahead.

THEO GEURTS: I think this is an interesting one. I think it’s even a little bit more complex and yet it is more simple. I hope I’m not going to be proven wrong, but we of course offer a proxy service. And never in my mind I would use that data to send the registrar of record a notification or a TAC. I mean, that’s not how you set up your

databases. Unless a registrar does that, I would love to hear it. That registrar must have some really operational problems there from time to time, because I don't see how you can make that work if you use your database that way. So my initial reaction was like, "That doesn't happen." That entire privacy/proxy services, if that is operated by the registrar, then this language is a complete non-issue because you will be sending it directly to the registrant. Because no registrar in his right mind will send it to the proxy service, which he runs. That is just ridiculous. You already have that information. And if the recommendation says you need to send it to the RNH, then you send it to the RNH and not to the privacy contact you have on file. That is just plain silly.

However, there are also third-party proxy services that are operated by third-parties where you as a registrar have no control over. That data is actually your registrant data as a registrar. I mean, if somebody says that anonymous proxy service A, B, C and provides that as the registrant data, yes, then we, as a registrar, have that data as the registrant data. Now, I don't see that as a problem because that is already happening right now. I mean, if we need to provide the current authorization code to such a service, then it's done. And if there is a problem with contactability or whatever, then usually the registrant or the reseller remove that surface and replaces it with the registrant data, and then everything is well again. Thanks.

ROGER CARNEY: Thanks, Theo. I think how you started that conversation was what Owen was saying in the chat as well. The proxy service would not be initiating the transfer, it would be the underlying domain

registrant. But making that request to transfer, it wouldn't be the proxy service initiating that. I think Owen and you were saying the same thing at the beginning there. Yes, it is, Owen.

Any other comments or questions? Looking at the possible steps here, removing the as listed in registration data TAC request, I think that's fine. I don't think that that diminishes the recommendation we're making here. I think it is useful to have an invitation note or some kind of note here that specifies and calls out when it is unknown, privacy or proxy service, what should occur. Again, to Theo's point, proxy services aren't going to send the transfer or the TAC provision to the proxy service. They're going to send it to the underlying customer of the proxy service. Owen, please go ahead.

OWEN SMIGELSKI: Thanks, Roger. I'm kind of responding to Emily's question in chat where I had referred about how the proxy service is not the one doing the transfer, etc. As I was thinking, there's a little more clarification. We're referring to privacy and proxy services here and that we should send the TAC to the underlying customer of that. Then there's two different reasons for that. One, the proxy service, although the registrant is not the one who is seeking to initiate the transfer or do anything about administering the domain name, that's the licensee underneath the customer who's doing that.

The other reason why is because if we're requiring that the registrar use the information that's in the public RDDS, then they're going to be sending it to whatever information would

appear in the data output. Some sort of anonymized type e-mail address, they could do that. Or because the registrar has access to this, they can use the underlying data for either the customer licensee of the proxy service or the registrant who's using a privacy service. I think when it's a privacy proxy, the registrar can do an end run around needing to use that public data. It goes out to an e-mail service which then forwards it. The registrar could just skip that process and just send it to the underlying customer information in either case. Thanks.

ROGER CARNEY: Right. To Owen's point there, I think that's how most registrars—and to Theo, as he said earlier, registrars do that. To me, I'm not sure that the privacy or proxy, the distinction between the two matters. Again, you're talking about the customer of that service would need to be the one that's notified. Again, I think that's how it occurs today. Theo, please go ahead.

THEO GEURTS: I think a little bit of the confusion maybe from the commenters. I'm just assuming here, it's maybe because in the past when we still had a gaining FOA, privacy/proxy service would sometimes delay the request for whatever reason. But if you talk about strictly from a database point of view, the privacy/proxy service where you display that info that is usually on an RDAP server or a WHOIS server, which is completely separate I hope for everybody, completely separate database which is not tied to your registration data directly, especially for a WHOIS service which has open pores. You'd never ever want to have that database and somehow

connected to your registration database. Those are strictly separated databases. So what you see on the outside on a domain name that you look it up through the WHOIS, that is a completely different beast when you are sending notifications or a TAC to the registrant, which is a completely separate database. That's why I was a little bit puzzled about the comments to begin with, because in my mind, what is on a WHOIS database service is completely detached from all the other databases that we have, and there's no correlation there. You never would use that data to begin with because that doesn't make any sense.

ROGER CARNEY: Thanks, Theo. Thanks, Owen and Emily, for continuing to chat there. I haven't heard anything, but if anybody asks, I think what we're saying is for this recommendation, the language itself, we can strike out the as listed in registration data at the time of the TAC request and live with the wording outside of that. Again, I don't think that changes anything. If we have an implementation note, I think that maybe that second sentence could be improved in that maybe it starts out with where—or in the case of privacy/proxy service being used—I think that the important thing is where it's the customer information is known is maybe more important than—I don't know. Again, I think this language works but I don't know if we're hitting the right importance of the two issues of it being known to the service or the requestors there.

I think that's the important thing, Rich, what I was trying to get at. I think Theo brought it up. Obviously, there's times where we don't know where our registrar wouldn't know but the actual underlying customer information. At that point, the registrant data is the

registrant data and that service would have to handle that process on their side. But if it is a controllable or known—not even control but just known—who the proxy service is, I guess, representing, then that should be where the notices are sent. Again, I don't think it's just this notice, it'd be all notices that we're sending.

Again, I think that what's on this screen here works and I think that it solves the questions asked about it. I just don't know if we can't make the implementation note a little better, and we can work on that over time. But I think the point is we can remove this language out of the exact text of Recommendation 3, and then include an implementation note as this covers it. Unless anybody disagrees with that, I think we'll move forward with that and this answer those few questions about it.

Okay. I think we've got about eight minutes. We at least touch on the next topic, Emily, if you want to bring that up. And at least introduce it if we can't dig into it.

EMILY BARABAS: Sure thing. This next comment was from ICANN Org. It was recommending additional elements to include in the notification of TAC provision with a focus on making sure that there's enforceability about some of the specific requirements associated with that notification. So the suggestions were to include an element that explains that the TAC will enable the transfer of the domain name to another registrar. I believe the goal there was to make sure that it's clear the function of the TAC for people who may not be aware. So it's more of a customer education element.

The deadline by which the RNH must take action if the request is invalid, so that the registrar has enough time to NACK the transfer where applicable. Now, if we keep the recommendations as they are, it would be important to note that sometimes the RNH would receive the notification of TAC provision and a TAC may have already been provided for the transfer, so that maybe somewhat dependent on what the group lands on in terms of the steps related to approving the transfer. Then any required actions that the registrar needs to take and by when upon receiving the notification by the RNH of an invalid request.

You'll recall that later on the recommendations, we do have a recommendation. There's currently an item under reasons that transfer maybe not, that is about the RNH not wanting the transfer to take place, then that's been changed to a must. So it is now a requirement for registrars to take action in accordance with the RNH's position on that. But I think from a compliance perspective, understanding what those required actions are will help Compliance enforce them. Thanks.

ROGER CARNEY: Great. Thanks, Emily. I don't want to dig into this too much. Maybe this is a good spot for us to pause on it and start back up on, not next week but the following week. Thinking about do these extra things make sense in the provision notification? I think it's worthwhile to provide as much information at the time. That makes sense. So let's take a look at these and think about them, and I think we'll start back up here on our next session. But I did want to cover some timelines and work plan with the group. So I think maybe I'll have Emily go over that real quick before we end the

call so we can see what we're planning to do for the remainder of the year. Emily, please go ahead.

EMILY BARABAS: Thanks, Roger. Hi, everyone. There we go. What we've done is tried to sketch out what we're trying to do in terms of getting through the public comment review with our newly enhanced twice a week schedule through the end of the year. What we've done is tried to sketch out based on how many comments are and the complexity of the comments, how quickly we can get through clusters of comments that logically fit together. What we're suggesting is that we do go in sequence because the recommendations build on each other pretty logically.

We'll share this with the notes. I encourage everyone to take a look at it. But it gives you a sense of as we move ahead, what we're hoping everyone is prepared to talk about so that we can get through these discussions as efficiently as possible. But the goal here is Meeting 63, the next one. Unfortunately, Meeting 63 is today. So we did not get through 2, 3, and 4. This will indeed be adjusted as necessary. We'll continue to work through this but it was envisioned that 64, we would continue discussion on Recommendations 3, 4, and the question for community input on Recommendation 4, which was about including getting registrar's IANA ID in the notification of transfer completion. So this is a plug for everyone to please review those comments. It's not a heavy lift, but making sure that you're familiar with the comments on Recommendations 3, 4. And that question for community input will help us move efficiently through those comments. Thanks.

ROGER CARNEY: Great. Thanks, Emily. Again, this will get posted on the wiki. So just take a look at—Emily, did you say you were going to send this out as well to the group? Anyway, again, good work plan. Hopefully, by the end of the year, we'll have public comments being wrapped up or closed wrapped up. We'll be making good progress. As Owen points out, yes, 63 was on this. And we have a little cleanup from to-do but I think we're moving on along that. And 3 and 4, I think we make good progress on 3 today so we should be able to wrap that up the next meeting as well.

Okay, two minutes left. Thanks, Julie, for the next two calls, Tuesday, November 8th and Thursday, November 10th at 16:00 UTC. Hopefully that makes it easy. Same time, same channel for everyone on both days. But I will open the floor for any last comments. Otherwise, we can give everybody one minute back on their day. How efficient. Great. Thanks, everyone.

[END OF TRANSCRIPTION]