ICANN Transcription

Transfer Policy Review PDP WG

Tuesday, 03 May 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/4BB1Cw

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, good evening. Welcome to the Transfer Policy Review EPDP working group call taking place on Tuesday the 3rd of May 2022.

For today's call, we have apologies from Owen Smigelski (RrSG), James Galvin (RySG) and Theo Geurts (RrSG). They have formally assigned Essie Musailov (RrSG), Beth Bacon (RySG) and Jothan Frakes (RrSG) as their alternates for this call and for remaining days of absence.

As a reminder, 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 view only chat access.

As a reminder, please select everyone when using the chat feature in order for all participants to see the chat and so it is captured in the recording. Alternates not replacing a member should not engage in the chat or use any of the other Zoom room functionalities.

Statements of interest must be kept up to date. Does anyone have any updates to share? If so, please raise your hand or speak up now. Okay. Thank you.

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. 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 CARNEY: Great. Thank you, Julie. Well, welcome everyone. Our first session post initial report. So hopefully everybody's gotten a chance to start reviewing the initial report. Again, the big homework over the next week or two here is to identify all those items that still need some clarification or work. And again, involving your stakeholder groups as much as you can in that process so that we can get a clean initial report out. But obviously, if something's not done in the public comment period, we can capture the rest of it and try to get as much work done prior to that as we can.

So again, so the next [inaudible] weeks, hopefully, everybody's already started looking at it. And it's a fairly easy read. So I think that that's good. I don't see any surprises in it. So it should be well known as you're reading it. So that's the big homework for the next couple of weeks. So, okay, Thanks, Jothan.

Other than that, I think the only other reminder is, we've got six sessions now. So [inaudible] diligently and again, [inaudible] we'll see how long it really takes us after flagging of any issues. But we're going to work diligently not try to pull up too much discussion of the past. Some new things we want to discuss, great. We can go through those fairly quickly. So again, stay focused, and actually Sarah's going to jump in here and to walk us through what the small group had done for a few weeks, looking at the NACKing and changes that they made to any of the NACKing rules.

Prior to that, though, I want to give the opportunity for any of the stakeholder groups that have any discussions they want to bring forward, any comments that they have or any concerns that they have at this point so we can get them addressed quickly. Any of the stakeholder groups have anything they want to bring forward?

Okay, so I'll turn it over to Sarah here. But again, on what this small group did, I think the key here is they've done some cleaning up for us, and some rearranging. I don't know that we'll need to get into too much detail, but Sarah will definitely be taking questions on anything that they've updated. So I will turn it over to Sarah now.

SARAH WYLD: Thank you. Hi, everybody. This is Sarah, I hope you can hear me okay. And you know, if it's zoom that was causing Roger's voice to cut in and out a bit, then maybe that's going to happen to me too. So please, somebody stop me if that does occur.

Okay, I want to thank the members of this small team who worked on this NACK finalization. And of course, also the staff team who put it together in the documentation for us. I was especially appreciative of the chart that you now see on the screen, because that will show you the section of the current transfer policy and the current text, what the revised text is, and in bold, it's the changes, and then the rationale. So those latter two columns are what came out of this small team's work.

I do need to perhaps gently apologize a little bit, I haven't looked at this in a few days. So hopefully, everything I say will not be distorted by my memory. Yeah. So and then just a reminder for the team, the focus here of the small group was really to finalize the input from the plenary team, not so much to come up with brand new ideas, but instead to take what the group had proposed and just figure out how to word it properly. So we're really looking for feedback specifically on anything that might be like really wrong, or we break things in some inappropriate manner. But I don't think that we'll encounter any of that, but hopefully everything here does really match the plenaries expectations.

Okay. So what I'm going to do is just really briefly discuss without reading the entire thing, each section, so we've got reasons we may deny, we've got some maize that were turned into musts, and then we've got must that were originally must and have been

updated. And in doing so, I will pause after each section rather than after each individual row. And we can discuss if needed.

Okay, so the first thing here that we have changed, and this was, I believe discussed in plenary, was adding into the evidence of fraud, also violation of the registration agreement. And of course, we do have some implementation guidance that we plan to include. And thank you, Owen, for drafting how that guidance could be phrased. So that's the registration agreement that I think was discussed in detail.

Scrolling down the next one, really, I think all agree that identity is not the goal here. The concern is that somebody requested the transfer who's not the domain owner. So that's what we made it say.

Next one down after that was payment issues. And one thing that was identified is that not every domain name is paid for by credit card, so there needs to be room for addressing payment disputes other than credit cards.

The other thing that we added into that one is the clarifying the current registrar of record is where the payment dispute would have occurred. And that just became, we think that'll make it more clear so that everybody can understand that it's a domain that has expired, and they haven't paid for it. And that's it for the remain mays. Has anyone any questions or comments on those? Great, thank you.

Okay. Moving down, the next thing that the group approached was mays that should be changed into must. So that's a little bit, I

thought, like an interesting change. And so we've got a [inaudible] objection to the transfer by the domain owner. Yeah, that should be a reason to deny it, we should must deny that. So most of the changes there were just taking out the admin contact and moving it to must.

Moving down. Thank you, Emily. Jothan, I'll take questions at the end of the section. Thank you. So the next one are the two different locks and we moved those here also and change the lock term. Jothan, your question is going to be on the must section that we're keeping must? Okay, so we'll get to that in a sec. Okay, great, Jothan, your hand. Please go ahead.

JOTHAN FRAKES: Thank you. Yeah, so I had a question come from a registrar after this came out about where—in order to afford a premium registry domain or a domain that was a premium, the domain may get renewed, and there'll be some sort of a payment plan or installment plan to afford that high premium of a registration across the span of a year. So it may fall outside of the qualification of this or fall within the qualification of this. If somebody has entered into a payment plan for the future registration, but the registry charges, let's say a domain name is $10,000 by the registry, I'm just going to pick an absurd amount, but they do exist. And the registrant determines to renew that domain name. The registrar renews it, but puts that registrant on some form of an affordable payment plan across the span of 12 months, in order for them to be able to afford to pay that domain name.

You would not want the domain name to transfer away during that time. So there was a question about if a domain was in a payment plan, if this would stretch to fit that element. That was the question that I received. And I apologize, because we're really putting a bow on this. But that seems like an important question, given the promulgation of premium domain names that are out there in the marketplace. Thank you.

SARAH WYLD: Thank you, Jothan. I do think that's a good question. I have a few thoughts as to what the answer could be. But before I get into it, I'd like to invite other members of the small team if they have opinions. I don't see hands. But if there are hands, I would take them.

Okay, so my thinking on this one is that would apply because I think this was intended to apply for registration periods that have been provided and not paid for. So maybe this is something for the group to take and think about, the plenary, and I'm sure that somebody is making notes from our wonderful staff team.

One thing that we could change at the very beginning of this sentence is where it says no payment, it could say nonpayment, which I think would include a partial payment in that kind of context. But yeah, so I think that's something for us to think about.

And yes, Steinar might be correct. Maybe this doesn't need policy to solve for it. Or maybe the policy is sufficient that it could cover. Yeah. Okay, so I think I'm officially suggesting we would say nonpayment instead of no payment. Any other thoughts on this

one before we move on? And also any thoughts on the musts which used to be mays and have transitioned to must? Rick, please.

RICK WILHELM: Just a quick comment. It seems like—I think that Jothan's yes was directed at my question about has the registry been paid. So it seems to me like in this case, the registrar has extended credit to the registrant. But the domain has been paid for but there's a credit relationship where the registrant is a creditor to the registrar, or the registrar could have been a creditor to some other third party that has a, for example, a credit mechanism.

We're familiar with these things where these days you can buy something, instead of paying directly with like Pay Pal or your credit card, you can pay in four installments or something like that, I forget the names of these things, where they do ad hoc credit.

And so it seems like that sort of a thing where there's a more complicated relationship, is a credit situation where the where the registered name holder is a creditor to the registrar. But that doesn't involve a more traditional grace period payment or something like that. So, but I don't think that the policy has to accommodate this situation is my initial reaction. Thank you.

SARAH WYLD: Thank you, Rick. Jothan.

JOTHAN FRAKES: Thank you. I think what we have here is a situation where the request was just that the registrar that asked about this wanted to know that there would be no opportunity for the registrant to make maybe one or two payments and then leverage policy to evade the rest of the bill.

And that was the only reason that this would fall into the realm of policy, or be within scope of policy. And again it's really the premium names that create this circumstance. And I think it's different from maybe when we were originally negotiating or discussing these transfer terms, premium names didn't exist. So it's kind of a new way to address some of that evolution. Thank you.

SARAH WYLD: Thank you, Jothan. Any other thoughts on this one or this section? Others in the section? Keiron, please.

KEIRON TOBIN: Thank you. Yeah, my understanding is that if usually some form of payment plan is kind of given, presented, then there's usually additional legal contracts where the individual would sign that would prevent that anyway. Jothan, I'm not sure in terms of which registrar you're referring to. But usually, from my understanding, and especially our registrar, if you take out some form of payment plan and stuff like that, there is additional kind of legal steps in there where you would normally put a lock on the domain to prevent a transfer in any way. Thank you.

SARAH WYLD: Thank you, Keiron. Good points. Seems that this covers this. Excellent. Any other thoughts? I'm seeing some agreement in the chat. Okay, Emily, if we can scroll back down a little bit. So we've talked about the mays. We've talked about the mays that moved to musts. And we've got the ones that are must and remain must.

So for the UDRP and URS that you see on the fourth row down, basically the same change, just adding in how exactly the registrant needs to get notified and that it needs to be notified by the provider in accordance with the rules. Yeah. Not changing the court order. Just really clarifying the language for the transfer dispute one. Not a meaningful change, just a language clarification, not even making changes to the 60-day lock. That's a bit lower down.

And we have may not, and must not. Any questions on the musts that remain musts, or comments or input? Okay, and then we've got changes from may not into must not. And so we're adding implementation guidance relating to nonpayment, taking out the admin contact, clarifying language around the inter registrar transfer lock. Scrolling down a bit more, Emily. Thank you.

This one, also time constraints, is just clarifying, instead of specifically saying how many days, it's referring to the requirements of the policy language for how many days and then we'll come back to the change of registrant later. Next one down, also just intended for clarity. And that is the end of our list. So any further questions or discussion are very welcome now. Jothan, please.

JOTHAN FRAKES: The payment plan issue kind of related to 3.9.1 also, that nonpayment for pending or future registration periods might be interpreted. I think there was a bridge between that and the prior discussion, but I do believe we've addressed that beforehand. I just wanted to make sure that this issue was raised related to payment plans for premium domain names, that those are for future or current registration periods, or pending registration periods, and could be interpreted here as grounds to may not, must not deny a transfer. Thank you.

SARAH WYLD: Yeah, Jothan, I'm not sure that I'm following you there. So why is it a payment for a future? Like, if it's for a future period that hasn't yet been provided, then why can't they just not pay for it or refund it and then transfer out?

JOTHAN FRAKES: Right, in this case, the domain has been paid for. And the registry has been paid. The registrar may have received maybe two twelfths or three twelfths of payments, and then the registrant decides to migrate out. So the registrar is left with eight or nine twelfths of the registration payment that they are stuck with.

So I do believe that this could be contractually addressed in the prior wording. But the concern was that this one might leave room for interpretation that it's okay that that registrant can't have their transfer denied while in that payment plan.

If we believe that that is not a valid concern, that is okay. So the domain name would have been renewed and paid for at the

premium price or at the standard price, depending on the model of the registry. And if it were in the premium price range, and there was, again, some form of an installment plan that the registrar was using to make it a monthly affordable amount or whatever model they would use in order to allow that registrant access to the domain name, that the registrant would keep the registration of that domain at the registrar during that payment term and that the wording of this might leave room for the registrant to migrate the domain name away.

SARAH WYLD: Thank you for explaining that. I think I understand better. I see Volker's hands up.

VOLKER GREIMANN: This is basically the same as nonpayment of the current registration term, or something like that. The question is, do we want to allow registrars to hold a domain name hostage for payment? That's essentially the question here. And for that purposes, I think it's irrelevant whether there's an installment plan or whether the domain name has to be paid at the end of the term in full or whatever the case may be.

And I think precedent with ICANN and most ccTLD registries as well is that a registrar may not hold a domain name hostage for nonpayment of current registration term fees because they have an agreement with that registrant and even if the domain name is transferred away, they still have that agreement for payment, and they have the right to collect for that from the contract. If they don't

have that, then basically, they have a very bad contract with a registrant and usually the next step would be to go to enforcement and collection services and make sure that the registrant pays in accordance with its contract. Thank you.

SARAH WYLD: Thank you, Volker. Jothan.

JOTHAN FRAKES: Yeah, and thank you, Volker. So the reason—I got a Skype message from the registrar in question, so what this would be is the scenario is that you've got a domain name where the registry has a model of a premium registration, but a standard renewal price. And the premium registration is something like $25,000, but the renewal price is standard reg fee, let's arbitrarily pick $25.

The registrar may take and work with the registrant to come up with a payment plan across a span of many years, let's say 5 to 10 years on that $25,000 premium price but the renewals have to occur at that registrar as part of that relationship. That was the example given.

So the payment plan might be a 10 year payment plan on that $25,000 premium registration. I think it may still be covered by Volker's scenario. But I did want to represent this in order to be inclusive of different registrar models that may not be represented in our representation by numbers. Thank you.

SARAH WYLD: Thank you, Jothan. And I definitely agree that it's important that we work through this type of question, so I'm really glad that you did bring it up. I don't see any further hands on this. I do believe that we have gone through all the different changes to the NACK, mays, musts, may nots and must nots. Any other input, questions, comments, discussion?

Okay, so in that case, I think I will turn it back over to Roger. Thanks, everyone. Oh, no, sorry. I'm seeing a hand from Steinar. Please go ahead.

STEINAR GRØTTERØD: Some time ago, I gave the example that the registrant had to pay a certain fee in assistance to get to a domain name transferred to another registrar. Is that something that we should kind of discuss and have it in this section of the policy? Or is it something that shouldn't be in the policy at all? Thank you.

SARAH WYLD: Thank you. That's a really interesting question. So the scenario here is that the registrar says you can transfer the domain, but first, you have to pay me $500 to provide tech support to you to get your auth code or something. I think that's not allowed, because it's not any of the reasons why the registrar may or must deny a transfer out. And so if it doesn't fall under those reasons, then it's not an option. So maybe they put it in their registration agreement. Right. But we have implementation guidance that says that's not allowed. I wonder if the implementation guidance on—

Emily, can you scroll up on the screen for me, just to the very top of this chart?

Yeah, thank you. Okay. So here in the implementation guidance, we refer to not intending that minor violations of the agreement could allow a blocking of a transfer. I wonder if there would be some kind of room for adding in text around you can't require crazy payments for things that don't need to be paid for. I'm not really sure how to write that. And I'm not sure if it's actually an issue that ever comes up in real life. So maybe this is something for the plenary to think about and ALAC or other groups can provide suggested text as to how to change it. Yes, please go ahead.

STEINAR GRØTTERØD: Actually, if I recall correctly—but I didn't make the notes—I think it was Keiron or someone else that gave some sort of reference in ICANN guidelines that it was possible to put certain fees into a certain task for a transfer. But maybe I'm having bad memory on that. But maybe somebody else has better memory. Thank you.

SARAH WYLD: Thank you, Steinar. Roger.

ROGER CARNEY: Thanks, Sarah. Yeah, and I think that that does happen today. The issue with the transfer policy is that the registrar can ask for that money, but they can't deny the transfer request because that money is not paid. So there's nothing that stops the registrar from

what you said, Sarah, okay, but there's $500 for technical support or whatever, but they can't deny that transfer, and they can't stop a TAC provisioning if that's not paid.

SARAH WYLD: Yeah, thank you, Roger, I immediately started to think like, maybe we can create educational materials for domain owners, but I'm not sure if that's the conversation we should have right this minute. Jothan, what do you think?

JOTHAN FRAKES: You know, I guess we just—and I put this in the chat, we just have to walk a delicate line between making sure that the freedom from a fee that Steinar described is not anything to support protections for the registrant so that should not give room for evasion of the scenario I described. Thank you.

SARAH WYLD: Thank you, Jothan. Volker.

VOLKER GREIMANN: Yes. Ultimately, I think it's the same as the fee for transfer out. I mean, according to ICANN policies, you may charge a fee for transfer outs. But if you charge that fee, nonpayment of that fee or late payment of the fee may not be used to stop the transfer. It's a contractual thing between the registrant and the registrar, but it cannot hold up the transfer. The registrar has other means to

collect on the contractual agreed upon fees, and I don't think we should make an exception here. Thank you.

SARAH WYLD: Thank you, Volker. Jothan.

JOTHAN FRAKES: So while a domain is at your registrar, you have the and attention of that registrant. And I think in many cases where you would have something in agreement, the desire to move the domain away might you be like as if you were in the process of purchasing a home, and you wanted to pay off your prior loan, you can accelerate all your payments and have a payout, immediate payout that takes you off of a payment plan. And that would be the mountain dew in a lot of those scenarios.

So what would be the difference here is the ability to leave without paying some sort of a transfer out fee is a different scenario, an entirely different scenario than the ability to protect from evasion of payout on that amount. And quite candidly, I think that we need to really look at that the domain name as collateral for payment, in this case, it could be quite a substantial sum, should really be possible. Thank you.

SARAH WYLD: Thank you. Interesting. Okay, we've got another thought from Volker. Go ahead.

VOLKER GREIMANN: Yes, I still think that in case a domain name registrant wants to move away in such circumstances where you have an agreement with certain terms, you as the registrar should make sure that those terms allow you to collect on those debts, no matter what the domain name is transferred away or not.

I think ultimately, the onus on that is on the registrar to make sure that they can collect on their fees. And offering that kind of service is ultimately a risk assessment of the registrar with the ability to collect their fees later if something goes south. I mean, the registrant could also sell the domain name to a third party. And they wouldn't be bound by those terms, because they haven't agreed to that. So would that also include prohibiting the registrant from selling the domain name to a third party? I'm very unclear on that. I think we're opening a can of worms here by creating an exemption that wasn't there previously. So I think this would be significant impact on registrant rights, we should be careful about those. Thank you.

SARAH WYLD: That's a good point, Volker. Registrant rights definitely need to be protected. I know for myself, I often just can't really think about whether I agree or disagree until I see it written down. Keiron, what do you think?

KEIRON TOBIN: Thank you. So essentially, the way I'm looking at this is that if a registrant hasn't fulfilled the full criteria, as you said, whether it be because of a premium domain, or whether it because it's taken out

over a subscription period, then because they haven't fulfilled the full criteria to me, then essentially, you could look at the section [1(a) 3.7.1,] evidence of fraud in terms of the fact that they are trying to take the domain without fully paying it, which also refers back to the violation of the registration agreement, which when it was taken out, it would be under that information, I would hope, from a legal stance.

SARAH WYLD: Very good thinking. Rick.

RICK WILHELM: I think that we're kind of confusing the difference between a situation where an item is like a car or a house or something like that, where the lender holds the title to a thing in a situation like a domain name purchase, where the payment plan is essentially an unsecured loan, because recall that if you have an auto loan, or a home loan, the title there is held by the bank that has loaned you the money for your car or for your house, you don't have the title.

And so that means that what's going on here with these domain names is not a similar thing to the situation that Jothan is raising, because in that case, the registered name holder for that name would actually be the one holding the lien, or the note or the loan, aka the payment plan for the $10,000 fee for the premium name. And then that entity would have a separate agreement to essentially lease the use or the DNS services out to what we would think of here colloquially as the registrant. But really, in that

situation, the registered name holder would be the bank or the lending entity. And then that works around this situation.

In the situation that Jothan's talking about, that essentially is the thing where the entity loaning the money has made an unsecured or otherwise secured loan where they're not using the domain name registration as some sort of a collateral where they can't prevent it. If they were doing it, then they would have to be the registered name holder.

And so our mechanism right now facilitates that situation, that if the registrar wants to do that, then they would actually be the registered name holder, and they would have a lease agreement on the side with what we would think of as the registrant to provide services of that name. So I think that this is, again, a red herring in the situation. And we don't need to complicate it because of the reasons I described. Thank you.

SARAH WYLD: Thank you, Rick. Those are some very good points. I think I'm going to give Jothan the last word on this topic. And then we're going to wrap up this review. Any further considerations, especially on how to adjust for this scenario, please send them to the mailing list, and we can discuss at that point. Okay, last word on this, Jothan.

JOTHAN FRAKES: Yeah, and thanks for the investment of time on this. And it's truly premium names that created this scenario, because that is what changed between the last time this happened and now, and it's

been a good way for registrars to give access to the Unobtanium that is those premium names in order to build websites and really help registry see the vision.

So for these domains, it's really bad, I see some suggestions that the registrar might be listed as the RNH. And so we get into the privacy proxy stuff or challenges related to where the registrar or the payment provider might be listed as the registered name holder. So this is the reason we're kind of splitting hairs. I realize this is a red herring edge case. But I do think that there's quite a lot of registrars out there that do provide this type of service in some form. And we'll be grateful that we had this discussion in a year or two. But I do appreciate people taking the time on this, I do think it's a different scenario, there's got to be a way that the registrar can keep the name until they have surety of payment, because it's such a great way to have the attention of the person who's taken the loan. Thank you.

SARAH WYLD: Thank you. And now back to Roger.

ROGER CARNEY: Great, thanks, Sarah. Great discussion. Again, as Sarah mentioned when she started, I think we proved it as we got through this, is this is great work by the small team here that they were able to get to some good wording for us. And I think the only thing that we agreed on was one small change to the very first one. So that's great. And I think [inaudible] this into the documents so that everybody sees it and knows it. Again, it's not new. It's

been out for a couple of weeks now. But I think now that we've had time to review it, and discuss it, again, it looks great. So again, thank you to the small team. And thanks to Sarah for presenting that for us.

Okay, let's go ahead and jump into Jim Gavin's e-mail, his proposal on not just recommendation seven because it kind of hit a few of them, but mostly focused on recommendation seven and some updates to a couple others that were needed.

I'm sorry that Jim wasn't able to make it. I'm sure he's not. But he said he may try to get on next week's call. So if anybody has questions for him, I would say e-mail him or put it on the list or try to catch him at the next call.

But he did provide some suggestions for recommendation seven. And some more, I guess I'll say technical representation of recommendation seven. So I think if we take a look at what he suggested—and I think here real quick, I'll read it so that everybody doesn't have to read it.

But Jim’s suggestion for recommendation seven was the working group recommends that the minimum requirements the composition of the TAC must be as specified in RFC 9154 and its update and replacement RFCS. In addition, where random values are required by RFC 9154, such values must be created according to BCP 106.

The salient point from RFC 9154 is as follows. Using the set of all ASCII printable characters except space and a required entropy of 128 bits, the length of the TAC must be at least 20 characters.

So yes, Thanks, Keiron. I mentioned that to Jim as well, it seems like a very nice technical response to a recommendation. And I wonder if this isn't better positioned as an implementation note or footnote on something closer to what Sarah had suggested a few weeks ago as well. And that was just my thoughts. And I mentioned it with Jim and he hasn't had time to take a look back at it.

But I wanted to bring this up and get any initial thoughts on this. And again, I see a few things in chat. But to me, it just seemed a little technical. We've gotten to this spot sometimes and then backed up a little and tried to get to more policy language, what we actually want instead of how to do it. But there's also the balancing act of making sure what we want is actually enforceable. So it's one of those lines that's hard to draw. So Sarah, please go ahead.

SARAH WYLD: Thank you. Honestly, I don't know why my hand is up, because I want to echo everything that you just said, Roger, this is indeed more technical than we often get in the policy recommendations. And that was sort of my first impression, was my goodness, this is technical.

On the other hand, I don't object to anything that's in here, it all seems very reasonable, seems to make sense, seems to be what we should be doing. And as you said, there needs to be something for Compliance to measure against.

So I'm not yet personally satisfied as to how to balance those things. But I do think it bears a bit further thought. I don't quite want to leave it as it is. But also, I can't figure out what to change or take out. So maybe somebody else can. Thank you.

ROGER CARNEY: Great. Thanks, Sarah. Okay, any other comments? It seems like it's pretty good agreement on this, and maybe we can find a way to, again, maybe backtrack and use some of what Sarah suggested a few weeks ago with this supporting that more directly. But how to do that, I guess, is a good question as well. So Rick, please go ahead.

RICK WILHELM: Just a couple of things. For those that don't know, RFC 4086 and BCP 106 are the same document. So that's sort of what is happening in that bracketed footnote.

In RFC 9154. If we just say that it needs to be compliant with what's described in 9154. That includes all of the stuff that is on the screen, especially the quote unquote salient point, which is the principal ASCII techno jargon stuff. It's just embedded in the document. So if the PDP wants to stay higher level and avoid having technical specificity and just refer to the IETF standards, then it could refer to RFC 9154 and BCP 106, the first sentence there, and we could just stop right there. And then that keeps it getting into the details of uttering that much language in the policy. It has the same practical effect as doing that in the document. And I'll stop there. Thank you.

ROGER CARNEY: Great. Thanks, Rick. That's great for clarity there. That helps. I think, Jothan, please go ahead,

JOTHAN FRAKES: And I'll go briefly because Rick covered some good ground. We did some review at the early onset of this. And this, I think, represents some of the best current practices and minimal type of uniqueness and printable ASCII characters and define things very clearly. At the onset of this group's work, I did go through and review a number of different registries, what their minimum maximums were, what sort of entropy or character set mixes were minimum requirements, whether you had to have combinations of upper or lower, you had to have numeric and special characters, what the string lengths needed to be, or could be as long as, and the balance of 20 characters and some of the other recommendations here really came at a lot of research cost, it did evolve in parallel with the definitions of these RFCs. So we had the RFCs occurring kind of in parallel with the work of the transfer policy review team. But all in all, Jothan's opinion is this is a good suggestion. Thank you.

ROGER CARNEY: Great, thanks, Jothan. Volker, please go ahead.

VOLKER GREIMANN: Yeah, my only concern is that it's very technical and very descriptive. And by referencing a certain RFC, I'm just wondering,

are we future proofing it enough? Or are we locking it in a place that might be outdated and maybe 10 years' time when we all have quantum computers and certain changes might happen that might make what currently seems like a secure passphrase or a secure token laughable in the future? So I'm just wondering if we are enshrining a set of requirements here, instead of leaving it open for implementation and having some room to let it evolve in the future, are we setting us up for problems in the future or is this sufficient for all times? Thank you.

ROGER CARNEY: Great, thanks, Volker. And that's actually—you're hitting back on how we kind of stumbled on to the original recommendation three to begin with, was, well, we knew we wanted that, but we wanted to make sure that it was somewhat adaptable, flexible for the future, as well. So Rick, please go ahead.

RICK WILHELM: Two things there. First, thank you Volker for that question. I would offer that to the extent that the technology evolves, the RFCs would be updated to adapt to those standards, as has been the custom in the IETF from long time historically, right. So to that extent, the IETF participation would update it. And so therefore, they would be adaptive of that. So hopefully that helps for Volker's comments.

Right now in RFC 9154, one thing I do want to point out is that it has a should around the 20 characters. It doesn't make it a must. And so I think that what Jim is proposing here with that bullet point

there is to make that be a must in the policy rather than allowing that to be a should as it is in the RFC. Because that particular bullet that Roger has highlighted there, that text does not exactly appear in the RFC, but I think that what he's doing there is he's proposing that into the working group text because right now the RFC in one, it has a should related to that level of 20 character entropy and 128 bits. Hope that's helpful. Thank you.

ROGER CARNEY: Great, thanks, Rick. And you bring up a good point that as great as reference to RFCs, it's a nice standard and easy to point to, to your point, most RFCs are built with flexibility into them. So as you mentioned, a should here or a may there or whatever it is, most RFCs are built with some optional features to it. So it's one of those where saying you have to follow RFC whatever doesn't mean that you have to do everything in it. The fact is the RFCs are usually written to be pretty flexible. So it's great to know, thanks.

Okay, so I think I'm hearing that this may be a little too technical or specific for specific recommendation. But it is great to have as a reference to this proposed recommendation. Is that what I'm hearing, thoughts? Rick, please go ahead.

RICK WILHELM: So this is a case where I think if the IRT does not make a recommendation to the technical requirement here, the IETF standard, purposefully—and this is the comment I put in the chat, when I was one of the co-authors as well as when this went through the regext group, there was very purposefully not a must

in this spot, but rather, it was a should, because if it had a must, that would have meant the IETF standard would have made policy in this area, where it was a technical thing that we would be talking about. That's why it's a recommendation.

And so if the group wants to impose a minimum on it, this would be the place, the group would have to do it somewhere. And because the IETF is not going to—the minimum that the IETF is going to put on it would be for a security standpoint, and it would be different. So I think that the group might want to make some sort of recommendation around this area, because making a length recommendation of that is—I don't think it's that radical, I would offer. Thank you.

ROGER CARNEY: Great. Thanks, Rick. Okay, any other comments? Question questions on this? So just to be clear, thinking about this, Sarah provided an alternative to our original recommendation three, which is now seven. And she provided some language to that. And now, Jim has also provided some language. So I think we need to take a look at that. And like Rick mentioned, is there a reason to make some things more static here or not? And again, are there suggestions that we can provide to the IRT in implementation notes? Or do we want to be somewhat specific on certain things? Those are the things we had need to think about.

I don't know that we'll get to that conclusion before the initial report, but we can at least provide some options to the public so they can take a look at what our thoughts are on that. So anything else on Jim's wording for recommendations seven? Thanks,

Steinar. And maybe I'll let Berry talk to that question real quick. Berry, did you want to talk to Steinars's chat question?

BERRY COBB: Thank you, Roger. I'm not in a position to speak for Compliance, and I believe they're on holiday. We'll take that as an action item. But generally speaking, and based on past experiences, when we're creating the consensus policy, I think it's general practice to avoid specific pointers to RFCs. I'm not suggesting that it can't be done here. But based on what I know, looking at Jim's kind of first paragraph, I think Compliance would be a little bit challenged with the pointer to RFC 9154 versus the bullet that is very specific and tangible that Compliance could investigate and enforce, but I'll leave the formal response to that team.

ROGER CARNEY: Great. Thanks, berry. And sorry, I didn't mean the Compliance part. But I noticed that you put in chat something similar to answering Steinar's question. So thank you for that. Rick, please go ahead.

RICK WILHELM: So I say this gently and curiously. There's a number of references to RFCs in the various contracts, whether they be EPP, or WHOIS or DNS, or something like that. Oh, I see, contracts, yes, consensus policies, very low. Okay. Sorry, Berry. Got it. Okay. Thank you very much.

ROGER CARNEY: Thanks, Rick. Okay, again, think about this, and again, Sarah's language is in here as well. So is there a chance to marry these? Or does it make sense to leave one or the other out? I think if someone can come up with that key and make it work, that would be perfect. Otherwise, I think we're going to kind of end up with a couple options here about being specific or not. Okay, Berry, please go ahead.

BERRY COBB: Thanks, Roger. Just real quick. And I think from a staff perspective, not picking one over the other, but trying to wear a Compliance hat, even though I never have worn that, I think they may be a little bit challenged as to under Sarah's suggestion there is no must there. So I think they would be challenged to try to figure out how they could enforce that as it being part of the consensus policy. Whereas Jim's suggestion is definitely more pointed in the must department. Thanks.

ROGER CARNEY: Great. Thanks. Yeah. And one of the things—and I think Jothan maybe will add to this, but when TechOps talked about this issue just a few weeks ago, and Sarah—and we talked about it on the call here to Sarah's suggestion about best practices, and what does that mean, and how does that happen?

And I think when I looked at it, I thought, oh, best practice meaning, okay, how do you use the RFC correctly? As we describe, RFCs are very flexible. But best practices is probably less flexible. And I was thinking, not a best practice, but how do

you actually use the RFC to achieve the goals that we're wanting, and this bullet is one of those. This isn't a should from the RFC, this is a must. And that's kind of how I thought of Sarah's idea of best practice can meld into something that's not a best practice but an exact, how to use this RFC. But Jothan, please go ahead.

JOTHAN FRAKES: Thanks, Roger, and you covered part of it, which was to identify that we had hashed this out in TechOps. I'm the co-chair of that group. What are the circumstances under which Compliance would come into effect? Is it where a name transferred away and there was concern over that? Is this where the registry or registrar is being reviewed for compliance with whatever the suggestion is?

I think we're spending a lot of time looking at this. As long as we're clear about how it can be implemented and that it's implemented in some consistent way across the various backend providers and registrars, I think that's really the objective here, is to make sure that we are providing registrants a reasonable amount of security for that TAC.

And when we go in and identify bullet points and be specific, as Jim has done, I think that there's a balance between ensuring that it's going to be implemented consistently, and the compliance work, but we do any kind of specificity like this at the cost of the forward-thinking flexibility to address Volker's concern about quantum, or other future evolving technologies. Thank you.

ROGER CARNEY: Great, thanks, Jothan. Okay, let's go ahead and take a look at the other updates that Jim thought would need to happen. If we scroll down, I think recommendation nine was the next one. And I can read this real quick, suggested changing 9.2 to when the registrar of record sets the TAC at the registry, the registrar must store the TAC securely, the registry must store the TAC securely at least according to the minimum requirements set forth in 9154 using a strong one-way cryptographic hash with at least a 256-bit hash function, such as SHA 256, FIPS 180-4 and with a per authorization information random salt of at least 128 bits.

Again, so I think that we went from a policy recommendation of 9.2 to a very technical solution of the same thing. I don't think it says anything really different. I think it's just being more specific and more technical about it. And the original 9.2 is just above that, if everyone wants to look at it. Rick, please go ahead.

RICK WILHELM: Sure. Thanks, Roger. Just sort of some additional comments on this. This text is copied almost verbatim, probably exactly verbatim from the 9154 draft. 9154 contains various suggested requirements for best practices on both registries and registrars related to what's referred to in the document, in the RFC as authorization info. Now, in this group, more commonly referred to as the TAC. You can see that in Section 4.3.

So this one refers to the mechanism by which the registry is required to store that. This stands in contrast—and just let me illuminate this briefly. This prevents the registry from storing TAC via encryption which would be reversible. So what this means is

that the TAC goes in, it gets hashed with a strong one-way cryptographic hash function, as you can see there, using a random salt. And that means that the registry can never—I'll say it slowly—can never recover the TAC. It cannot, it mathematically cannot be cracked.

So this stands in contrast to if the thing is encrypted, it could be recovered if you've got the other encryption key. But this is encoded using this mechanism. So you can compare them for equivalence. But you can never get the original one back. Correct. So that's just to clarify the difference here. So any registry is no longer going to be giving back the TAC to a registrar or a registrant. This is one of the big mindset shifts regarding the TAC, that they are relatively short-lived, disposable. That's a key thing here. Let me stop there. Thank you.

ROGER CARNEY: Thanks, Rick. And I'll just add on to that, just to make it clear for everyone, this stops the registry from being able to retrieve what the TAC was, but it does allow them to compare them. So that's the difference. They can only compare. They can't recreate the TAC. And maybe that's what the 9.2 really should say, is what Rick was saying. It doesn't even have to say one-way hash, just that it's non recoverable. And then we can even put Jim's suggestion as an implementation note, or again, we can use Jim's suggestion wholly. Just thoughts on how to make those things work. Steinar, please go ahead.

STEINAR GRØTTERØD: I must admit I'm not that technical survey. But I do understand that the TAC is extremely important, is some sort of a base of this, all the security instrument we have, we're proposing in this new policy. And the old wording, the 9.2, I don't think that kind of signaled the importance that the registry cannot display the TAC but he can just compare it with—in my mind, that's really important. So maybe it's getting too technical into the policy. But in one way or another, we have to kind of put that understanding into the wording that the critical elements here and the security elements here. Thank you.

ROGER CARNEY: Great, thanks, Steinar. And I was kind of thinking the same way you were thinking on that. It's like, how do you get from showing the importance of that, that it is considerably more secure doing it this way, without digging too deep into the details of the security. Jothan, please go ahead.

JOTHAN FRAKES: Yes, so some registrars use the TAC, I think, for things other than transfer, or this is at least when the auth info code was present. And there is going to be a change that comes, a rather sweeping change if the TAC, the artist formerly known as auth code, is transformed into being something that is a trigger for the transfer and only used one time for the transfer.

There is, in fact, under use right now, a validation of auth code that happens sort of, if you were to use a credit card analogy, when you check in with a hotel, they check your card has

appropriate balance, using what's called an open to buy command. But they don't actually take money away, they just make sure that the balance is there, so that they know that it's not a bad card, etc.

And then they later actually charge you. So there is something like a soft test for a transfer that works currently under the way that auth info currently acts. There is not just a test of if this person has the right keys to transfer the domain before actually issuing the transfer command that occurs in today's registrar world, but there are other uses of the auth info code that are being done in order to truly validate that the registrant is the holder of the name outside of using DNS or other needs. And those would be impacted by the way this will behave. And I think it's important to just represent that on this call and let people know that that's something that if there are strong feelings about, that those should be brought up rather quickly, because of the way that this will affect things. Thank you.

ROGER CARNEY: Alright, Thanks, Jothan. Rick, please go ahead.

RICK WILHELM: So I think that's a good point, Jothan. I would also offer, though, that whatever mechanisms people are currently using that TAC for that should be adaptable to determine if they're doing it, but I also agree with the point that Sarah's made for like the TAC is intended to be for transfer, for proving ownership. There's certainly other mechanisms that people can use.

We've all seen the way that you can have people enter a text record for like if you're doing Google workspaces or things like that. But the security around the auth info codes, the way it currently operates under the way we sit here today, pre this transfer PDP, it was actually—I would offer it offers a false sense of security because it's not as private as people think it is. And it can be misleading and more easily hijacked. The current thing that we've got the TAC set up for is going to be a much more secure mechanism for everybody involved. Thank you.

ROGER CARNEY: Thanks, Rick. Okay, any other comments? Okay, let's move on to Jim's last suggestion here, recommendation 11, Jim has updated to be the working group recommends that the tac must be a one-time use. In other words, it must be used no more than once per domain name. The registrar of record must meet this requirement by randomly creating a new TAC each time one is needed, as specified in recommendation seven, that registry operator must clear the TAC as part of completing the successful transfer request. And I think Jim added the third sentence there, just pointing, tying this recommendation to recommendation seven. Jothan, please go ahead.

JOTHAN FRAKES: Yeah, it's just a continuation of the prior comment. We used to have an auth info code that would sit there indefinitely that had other validation and other purposes that innovation had taken use of in order to create better validation of the registrant of record and the registered name holder.

The TAC being a onetime use and one-purpose use breaks those types of services or functionality that have been out there. The concern that was raised to me is that this may force people into using people's patented ways of addressing things where the auth info code may have allowed people to work outside of having to license or work with other people's patented processes. And that's what's being raised to me to represent here. Thank you.

ROGER CARNEY: Great, thanks, Jothan. And something else, it leads me off of what Jothan was saying, obviously, and I obviously I don't know that we need to say anything or fix anything here. But the IRT will have to work on a transition plan for sure. And that includes the fact that when this gets implemented, there'll be thousands of transfers in flight on a date. It's something they'll have to look at. And again, we don't need to solve for this. That's something that the IRT will have to address and come up with a solution for. So Keiron, please go ahead.

KEIRON TOBIN: Thank you. In terms of when we looked at the bulk function, I'm not sure kind of where we were with that. So I understand that every TAC must have its own single time use. But if we were looking at the bulk option, then would that mean that if one of them failed within that, then the entire bulk would fail?

ROGER CARNEY: Thanks, Keiron. And where we left the bulk was nothing different than today and that we were still planning to use—at least this is

what I remember anyway, use a TAC on a domain, not a TAC on multiple domains. We never got to a solution on that. So as of right now, it is just a TAC on a domain. To your point, does that cause a problem if that does get looked at? I think that that's something that would have to be addressed. Volker, please go ahead.

VOLKER GREIMANN: Yeah, I agree with what you just said. Essentially, even if you request the bulk of domain names to be transferred, these would probably be from a transfer perspective, the purely technical perspective of the transfer, looked at on an individual basis, as in each domain name is checked for whether the TAC is correct. And if it is, then the transfer is processed. If it isn't, the transfer is not processed.

And therefore, if you submit a bulk, and there's errors in that bulk, then those errors would only affect those domain names where the errors are. That's unclear, we might want to clarify that. But I think that's the status quo. And that's how it should be in future as well.

ROGER CARNEY: Great. Thanks, Volker. Any other comments? And again, the wording that Jim suggested and again, all he added was that third sentence tying this to recommendation seven. Otherwise, he left everything intact as far as I see. Thoughts on is this a better recommendation 11, Or does this need to be in here? Does it

cause confusion, or does it actually help clarify things? Keiron, please go ahead.

KEIRON TOBIN: So when looking at the bulk function here, if for example, we saw, let's say you use 100 domains in a bulk, and 99 of them fail, and just one of them feeds through—sorry, I'm still rereading it.

ROGER CARNEY: That's okay.

KEIRON TOBIN: Let me put my head down on that. I need to reread this. Sorry. Thank you.

ROGER CARNEY: Thanks, Keiron. Yeah, I'll just kind of feed off of what you said there. If 99 fail, to me, the last sentence of the original recommendation or this one says, only on a successful transfer will the TAC get reset. So if you had 100 of them, and however it is, 100 different TACs, if 99 fail, only one of them's going to get reset to null or blank or whatever it is. Reset by the registry. The other ones, because it's a failed attempt, I wouldn't expect that to happen. And Sarah, for your question, bulk right now means if you have 100 domains, you have 100 different TACs. Oh, sorry.

Again, so my big question here is, does this middle of sentence help or hurt? And I'm not sure the suggestion of must meet this

requirement ... I don't know how that feeds into the one-time use, specifically, but that's just my thought.

Okay, no questions. To me, recommendation 11 is still valid without the addition of this new sentence that Jim is providing. And again, I don't see the connection to the one-time use versus the meeting the random part. So I don't know. Rick, please go ahead.

RICK WILHELM: Let me just elaborate just a little bit. I think that one of the things that the current wording does not specify that who creates the TAC in the current wording that is unhighlighted. So the inserted sentence does specify that the registrar of record is creating the TAC. And it also links that to happen as needed. And it links it to recommendation seven.

If Jim were here, I would offer the friendly amendment that we could do without the word randomly there on the third line, because as long as you adhere to recommendation seven to create a new one, then you don't need the concept of randomly in this sentence, because that's over-specifying it, because if recommendation seven had some other means of creating the TAC, do you want that recommendation to specify?

But I think that the key thing that this sentence does is link the creating of the TAC to the registrar of record and links it to recommendation seven. So I think that that's partly the thing that we should focus on, is what the insertion does here. So maybe that would help. And maybe there's an amendment that someone

could offer to modify the suggested text. I see a comment from Keiron here, but I just want to offer that that's kind of what's going on with this thing. Thank you.

ROGER CARNEY: Thanks, Rick. I do like the fact that where it's appropriate, the recommendations can be tied together. So I think that that's useful. And your suggestion of randomly makes sense, because it's randomly random the way it is. But I guess I don't understand must meet this requirement. To me, the registrar of record meets this requirement by creating a new TAC each time one is needed as specified in recommendation seven. To me the must meet seems odd here, again, because it's talking about the one-time use versus the TAC. Rick, please go ahead.

RICK WILHELM: Sure. So maybe the sentence could be edited that the working group recommends that a TAC created by the registrar of record as per rec seven must be one-time use.

ROGER CARNEY: I think that makes sense. Yeah, something along that line. Can you make that suggestion, Rick?

RICK WILHELM: Yeah, let me see if I can remember it while I type real quick. Thank you.

ROGER CARNEY: That's okay. Yeah, I was trying to think of it as I was doing it. I couldn't think of exactly how you said it. Okay. No, I think that's good wording. Again, I like the fact that when a recommendation is interconnected, that there is a direct tie in the recommendations. Any other comments on Jim's three suggestions here?

And again, I think the big suggestion here is recommendation 11, I don't think is too specific, but the one in recommendations seven and nine are very technical and very specific, which obviously, there's some benefits to but also early on, recommendation seven, we were talking about needing the flexibility for ongoing changes, which we know will happen, security will improve and things like that. So I think there has to be a balancing of that specificity, versus something that's flexible enough going forward. So, Jothan, please go ahead.

JOTHAN FRAKES: Yeah, so again, I'm saying that the one-time use of the TAC, it is certainly servicing this transfer purpose. However, we are breaking how folks have been using the auth code for validation of domain ownership, or doing a soft validation of the ability of a registrant to transfer at certain registrars. So if there is a change like this, we may want to look at having something that replaces the functionality that is being deprecated that the auth info code had represented. Thank you.

ROGER CARNEY: Thanks, Jothan. Yeah, and I think that, again, I don't think that this one breaks it any more. And I think the example you're providing is broken in several spots, as you mentioned, when it's hashed, and assuming the hash is going to break it as well.

But this group is not going to be responsible for coming up with a solution to some other issue when it's not an issue of already documented contractual or consensus policy. So I think you're right. And I think that needs to be called out, that there are uses for this that are going to have to change. But I don't think this group is responsible for coming up with those recommended changes. So just my thought. Keiron, please go ahead.

KEIRON TOBIN: Thank you. Yeah, I do have a quick question. Maybe Jothan can kind of give me a bit of an answer. It's just in regards to the National Institute of Standards and Technology in the US. Obviously, we have a lot of registrars out there that are maybe in Africa and Asia. And I always hate kind of listing different jurisdictions in terms of this kind of criteria. How standard across the board is this? Is it something that is easy to implement? Are we asking a lot in terms of this? I don't know the answer, which is why I'm hoping one of you guys can kind of lead me towards exactly what it is. But yeah, just kind of [inaudible] just so I kind of get a bit of an understanding. Thank you.

ROGER CARNEY: Thanks, Keiron. Rick, please go ahead.

RICK WILHELM: Sure. So they're the NIST standard there that Keiron references—and thank you for the question—relates to FIPS 180-4 which describes the SHA 256. SHA 256 is a wide global utility in computer algorithms and encryption and security. And so this is extraordinarily well known. And while it's referenced here as a FIPS standard, it's something that has a high degree of—SHA 256 has a high degree of global acceptance. I don't have any real concerns about that one, but I certainly appreciate the question. Thank you.

ROGER CARNEY: Great, thanks, Rick. Okay, any other comments on this? Again, I think 11 is the easy one to get through. And Rick did provide that language in chat. And I think we can use that, balance that with Jim and see what his thoughts are, and maybe tweak it.

But I think the bigger discussion here is that level of granularity on recommendation seven and nine, how do you get to something that's enforceable, that will be carried through the IRT that actually makes sense that will provide security, which is our goal here in these recommendations.

So I think that that balance in a policy recommendation needs to be figured out, again, so that we can get that through all the way to the actual policy language at the end of it. So just keep thinking about that and see how we can get to that spot.

And now, I think we are only a couple minutes away from ending. Any other further comments from anyone? Okay, great. Great discussion. And again, Thanks, Sarah. Thanks, small team, for the

work on the NACK for the few weeks that you spent extra time on that with us, for us. So I appreciate that. And we will talk to everyone next week. Thanks. Bye.

JULIE BISLAND: Thanks, Roger. Thanks, everyone for joining. This meeting is adjourned. Have a good rest of your day.

[END OF TRANSCRIPTION]