ICANN Transcription

Transfer Policy Review PDP WG

Tuesday, 15 November 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/8QnVD

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: All right. Good morning, good afternoon, good evening, everyone. Welcome to the Transfer Policy Review PDP working group call taking place on Tuesday the 15th of November 2022.

For today's call, we have apologies from Richard Wilhelm (RySG) and he has formally assigned Beth Bacon (RySG) as his 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 emails. 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 functionality.

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 so it'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.

Seeing no hands, please remember 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 multi stakeholder process are to comply with the expected standards of behavior. Thank you. And over to our chair, Roger Carney. Please go ahead.

ROGER CARNEY: Thanks, Julie. Welcome, everyone. Looks like we have a busy schedule here today. So we'll jump into a couple of early updates here. And first off, since our last meeting, when we were discussing, and I think kind of tripping over designated representative—and I think we were kind of confusing that with the designated agent and that change of registrant policy.

I was giving some thought over the weekend to it. And I wonder if we should rename designated representative to something different so that we're not making that correlation there that we can [inaudible] The only thing I came up with was authorized representative. And I don't know if that makes sense or not. I just thought about it just to try to come up with something distinctly different than designated agent.

Again, I know that when we talked about designated representative way back last year, we talked through a couple of different—and I don't remember what they were, a couple of different possibilities and settled on designated representative but I just wonder if [inaudible] making that a little confusing. So I thought I'd throw that out there and see if that makes sense. Oh, sorry. Sounds like I'm cutting out a little bit. Oh, sounds good, Sarah. Emily and Caitlin are having issues. Okay, let me know, others, if I'm cutting out and I can move to a different mic if we need to.

Okay, great. Thanks. Maybe I'll just keep talking and I'll keep the ... going on my side here. Yeah, Keiron, let's not make any more acronyms. So again, give it some thought. I just think that maybe it'll make it better to make a cleaner distinction between the two concepts. And we're not trying to hijack designated agent as a use here, we're actually thinking of something completely different.

Okay. Thanks, Emily. Thanks, Sarah, for that. Don't need to formally define it. I agree. We don't need to define it. I think it makes sense. It's fairly straightforward. I just wanted to try to create a line between the designated agent and this representative. So there we go, Owen. Do another “RAA, RRA, RAR.” Yeah. So that will make it much simpler.

So just think about it and if authorized representative works, or—it just seems like makes it cleaner line for me. But please let me know if anybody has thoughts, mail list or you can drop in here as well.

Other than that, I think staff has been working on the red line so far that we've talked about, red lines to the initial report that we've talked through already through recommendations one through six now. And they're starting to redline the initial report up for our review. That'll be coming out shortly.

Once it comes out, I think that we're going to try to stick to roughly a two-week window of feedback on that, and flagging anything of concern or providing alternate text if it is a concern. So we'll try to wrap it up two weeks after it's posted so that everybody gets a chance to do it, and we get it out efficiently. So be on the lookout for that. It should be coming out soon. And again, we'll be doing that as we go through these recommendations.

So, again, we're going to try to stick to the two-week window just to move this along as well as we can. So other than that, I think that's about it. As we try to do every week or every call, is open up the mic to any stakeholder groups that may have had some conversations that they want to bring forward. So I'll open up the floor to anyone that wants to bring up anything they'd been talking about or want to address with the group or get answers from the group. Holida, please go ahead.

HOLIDA YANIK: Thank you, Roger. I had a conflict last Thursday and missed the conversation and opportunity to clarify the confusion within the group relating to designated representative. So I'd like to take a moment and provide some clarification.

Basically Compliance's recommendation to update the definition of designated representative by including the term to request is made to prevent scenarios where a representative may obtain the TAC that an RNH never intended to request. This is pretty straightforward.

And the rationale why we recommend it, to be more clear about the representative's authorities, is based on the Compliance's experience with enforcement of provisions concerning designated agent authority for change of registrant that can also serve as an analogy. And as you know, per definition, designated agent is an individual or entity that the prior or new registrant explicitly authorizes to approve a change of registrant on its behalf, but not to initiate or perform COR that was not requested.

However, when we investigated some transfer and unauthorized transfer cases, we saw that abusive resellers completed COR that the RNH did not request or initiate and we saw that this was usually done right after the RNH requests AuthInfo code, the TAC, and it appears that the reseller changed the RNH information to their own to avoid allowing the transfer.

So from such cases, we saw that the resellers usually included a general clause in their terms of service or agreements that granted them blanket authority, like authority to manage the domain name. And we also saw provisions like RNH authorizes reseller to modify its contact information as opposed to only approve or confirm change of registrant request.

And on top of that, we also recently had couple of cases where reseller included a clause authorizing them to transfer the domain

name which did not mention anything that this transfer would be done or performed upon RNH's request. And with the provisions that we had within the current policy for designated agent, Compliance was able to request remediation, and the contracted parties corrected this noncompliance and committed that this was will not be committed, that they will be preventing the reoccurrence.

So, I guess this will respond to the deliberations why we need to include the definition within the policy. So, we believe that more clear the policy specifies what actions the designated representative or however we call it can do on RNH's behalf concerning the TAC and more efficiently Compliance will be able to enforce the requirements and help prevent occurrence or at least repeated occurrence of similar scenarios that I had just described.

Additionally, I'd like to note that, based on the currently proposed TAC definition, in recommendation six, TAC can be provided to the designated representative and also per recommendation 9.1,. the TAC must only be generated by the registrar of record upon request by the RNH or their designated representative.

So meaning that representative can both request and obtain the TAC and Compliance's input for inclusion of request element in the definition is also in line with the currently proposed recommendations.

Further, Compliance's—so our recommendation to include this definition into the body text of the policy is also, again, consistent

with the current transfer policy language that provides designated agent definition as a separate policy section.

So based on my own experience, so this is me talking personally, based on my interaction with contracted parties, I would also like to note that footnotes can be usually regarded by registrars as an optional guideline, and not requirement for consistency and clarity and also for ease of enforcement. So Compliance recommends, again, that this definition would be a part of the body text of the policy. Thank you.

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

VOLKER GREIMANN: Thank you. It's an interesting point. But I think that the designated agent and maybe also the designated representative, they do have a very important role to fill, especially in those cases where the registrant does not directly engage with the registrar to register and manage the domain name and has no interest in doing so.

I mean, this is basically every situation where somebody else does the work for the registrant, and the registrant either does not care or wants the third party to act on behalf of the registrant.

I'm not quite sure what we gain by making the requirement explicitly. The terms and conditions that designate the reseller as the designated agent or representative that is authorized to make such changes are a binding contract between the parties. And as such, I think it's legitimate that if the registrant agrees to these

terms in their contract with the reseller, or the registrar, as the case may be, then these terms should be binding on the registrant.

It's the obligation of the registrant to read the terms and conditions of the agreement that he signs on to and ultimately, it is important that a registrar and also a reseller is able to manage the domain name in the best interest of the registrant and sometimes that involves making changes or modifications that would otherwise require the explicit permission of the registrants.

But as the registrant has given that permission in the terms and condition, it is simply not feasible to do it on an individual basis. And therefore, I think we should leave the current language in place. Thank you.

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

THEO GEURTS: Yeah, thanks. And I agree with what Volker just laid out there. I think that it's very essential that we have such language that sort of allows it. I also make the observation that ICANN Compliance was able to nail this registrar down. Not going to speculate who it was, but I was quite reasonably surprised to receive a newsletter from a certain registrar who was apparently engaged in the tactics that Holida described and that sort of explained to me in my mind that the usual NACK requests coming from registrar was certainly explained in my mind—So I was like, okay, that's maybe the reason why we saw higher levels of NACKs coming from

registrars because the resellers just go like, “Oh, we don't like a transfer out, we’re losing the customer, we’re going to NACK it.”

But again, the observation is also that ICANN Compliance did some good work here and made sure that all the actors—at least that actor, there's always some actor abusing some kind of stuff—that this actor is now brought back into line, and it's doing what policy requires to do. Thanks.

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

EMILY BARABAS: Thanks, Roger. I just wanted to follow up on Volker’s comment to make sure that—because I think Holida’s clarifications of the Org comments actually covered a few different elements of the comments. So I want to make sure that we understand the impact of some of the comments in response to her explanation.

So going back to a few of the elements that we talked about on the last call, just very briefly, there was some agreement on the last call to add language specifying that in the event of a dispute, the RNH’s authority supersedes that of a representative.

There was some support for the edit to adjust the definition of the designated representative to include the term “request and” for the reasons that Holida described.

And the third element was a suggestion to take the definition of designated representative out of a footnote of the

recommendation. Now, it's important to clarify that the recommendation is not the same thing as the policy language. So the policy language will be written in the implementation phase. And right now we're just writing recommendations from the working group.

So Holida was talking about that the important definitions in the policy are not typically included in footnotes, but are included in the language of the policy. So it is still possible that there's a footnote in the recommendation that becomes language in the policy itself. But if it really is a concern that this is going to get buried—and noting the concern last week that if we make it its own recommendation, it may not be read in the context of this very specific sort of situation or set of circumstances in which we've created this definition.

Another possibility is that we simply add like a sub bullet to recommendation six, which includes that definition. So it's in the recommendation, but it's also contextualized and only applies to this recommendation itself. So maybe that's a potential middle ground. And I see Sarah says that maybe inside the rec is better than as a standalone.

So just going back to Volker, I just want to make sure if he's opposed to any of the edits that we went over last week, that's clear, and we can address those specifically. Thanks.

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

VOLKER GREIMANN: I'm not necessarily opposed in this context. I think the edits are in and of themselves are fine. The only question that comes to my mind is, are we overcomplicating things by having two different terminologies for what is essentially describing the same role, albeit in a different circumstance? Designated agent is for owner changes and things like that, whereas the designated representative is for transfers. These are related issues. These are both in and of themselves concerning the management of the domain name on behalf of third party, and I feel that essentially, as they described the same role, they could use the same terminology as well.

ROGER CARNEY: Thanks. And I kind of said I think in the last meeting, and I think why Emily suggested the context here, and why Sarah—it's important that I think is—this designated representative or authorized representative—I'm going to start using just to see if people hold on to it or not—is specifically just in the context of being able to request a TAC and get a TAC. And it doesn't go beyond that.

And then I think that that's why it seems more appropriate, as a footnote, or as Emily suggested, maybe just a bullet under six where a designated agent is a bigger concept in the core, and, to me, has a true overarching ability for the change of registrant.

So I still think that there is a separate—and I agree, Volker, I think there's a fine line there. But to me, it is two separate use cases. And really, when we came up with designated representative back last year, we were trying to fill that known real-world scenario that

occurs every day where the account owner can do certain things, the web pro can do certain things on behalf of the registrant. And it's not defined as the designated agent, it's actually something separate.

And again, I think that's why we came up with it last year, because we know that there's a real world use that's been occurring for years. So I think that we're just kind of contextualizing that real world example. So yes, one ring, Crystal.

Okay, so it sounds like then—let's propose that we move this in air quotes here, this not necessarily definition, but description of authorized representative to a bullet in six, and we can move on from there.

Okay, thanks for bringing that up, Holida, we can get that cleaned up. And again, as I mentioned, all these edits will be coming out in a redline version. So we will get a couple of weeks to look at them, and we can flag them. And if it doesn't fit for someone, they can propose alternate language.

Okay, let's go ahead and jump into item three, the strawman for recommendation two. And I'll let Emily go through this, but I'll lead it off as staff and I worked on this as a—I don't want to say compromise, I just want to say a possible solution here to where the discussions have been going.

Again, I think there was some discussion—obviously, our recommendation was to remove that losing FOA functionality. We have public comments back that suggest keeping it. And actually,

as you read through the rec comments across recommendations, that kind of keeps coming back up as well.

But along with that are discussions starting back in ICANN 75, the working group seemed to formulate around, okay, this does provide an additional use for the registrant. It gives some power back to the registrant. And it does go against our efficiency model that we had hoped for in our recommendations, but it does provide solutions that we remove.

So I think that, again, that's where the discussions kind of fall, is, okay, the functionality does make sense. And I think even Sarah and Rich were kind of talking about the functionality, but maybe that functionality upfront. And again, I think that functionality is important. And I think most people see that it's important.

But where it goes, I think, is also important. When the TAC is provisioned and provided and before it gets used, there's a chance of misuse there. And if this functionality is put at the end, that misuse can be contained to a certain degree. And again, I'll let Emily get into this but I'll let Theo go first before Emily takes us through the strawman. Please go ahead.

THEO GEURTS: Yeah, thanks, Roger. And maybe I'm going to try to save us all a lot of time and remove a couple of barriers here. I was thinking like last week when I was in Brussels and not on the calls, I was thinking about the entire process, how we get a little bit stuck, sort of bogged down through the details, because we got some real detailed provisions within the current draft language.

So I was going back to the TAC provisioning. And in my opinion, that is going to be a problem in the future. It is way too detailed, it is way too granular on how the registrar must provide a TAC, and there's a NACKing process available to the registrant there and approval process there.

And last week, apparently, there was also some discussion if a notification is done by email by providing the TAC through email, is that secure enough? And I think if you ask me, that is not really secure.

So went back to the original transfer policy that we have now. And it simply states like registrar must provide the auth code within five days. It doesn't mention how that is even being done. So it skips all the complexity that the wholesale registrars have with APIs going through resellers, going through control panels at resellers for the registrant where they can obtain their auth code. It isn't there in the current policy, and I think that's with good reason, because it's very complex stuff.

So my thinking was going like, okay, maybe we should just make the current TAC [provision] less granular and move the entire NACK or agree to the TAC, let's take that out and—I think the word replacement is very bad. But let's not do away with the FOA, at least have the registrant keep that valuable sort of control in place.

So we're going to move then a little bit faster with the entire group, if we make the TAC provisioning more basic, we remove the entire complexity of registrars sending notifications, because in a lot of cases, as a wholesale registrar, the only notification that I can

send is email. So that is going to be problematic. So I rather have a less complex provisioning system.

And if we can also make sure that the FOA is still there, I think it goes [along in the] community to have it there, it will remove a lot of concerns. And I think we can move much, much faster through the comments there. So that was my attempt to speed things up. Thanks.

ROGER CARNEY: Thanks, Theo. I think you're in support of the strawman then. And I think keeping that five-day provisioning window flexible in the sense that it's up to the registrar to decide what they need to do in that first five days to provide the TAC or to provision the TAC and provide it. But I think you're also suggesting that keeping the losing FOA makes sense.

And I think that's what this strawman is doing, is keeping it with some slight changes, and really slight changes. And to your point, I think it keeps it simplified. Yeah, Theo still wants all the security mechanisms, he just wants that first five days to be flexible, and maintain NACK, ACK at end.

Okay, let's let Emily go through this strawman of recommendation two so that everybody gets onto the same page. And again, I think this was just a proposal about bringing the TAC back in but because of public comments, and because the discussions were leading that way. So let's go ahead and let Emily go through this. Please go ahead.

EMILY BARABAS: Thanks, Roger. Hi, everyone. I'm not going to read through this. And I'm not going to go through every detail because folks can read it on their own and will have some time to do so. I believe Roger mentioned in the opening that the idea here is that in addition to the redline, we'd give folks two weeks as well to review this and provide—coordinate with their the groups they represent and provide feedback on behalf of those groups about whether this path is acceptable.

So the idea here is basically that we are, as recommendation two, essentially affirming the world losing FOA requirements, and following with some potential small adjustments. These are all bracketed because they've been mentioned on previous calls, but have not been agreed upon by the group, but allows folks to review them and think about whether those additions makes sense.

We'd include here a rationale that would explain what these adjustments seek to do. And then the revised response to charter question A7, regarding the losing FOA, would instead provide a summary of the initial rationale that the group had for removing the losing FOA in the initial report.

This includes some of the discussions that have happened in review of the public comments for those who were in support of continuing to keep the listening FOA out of the recommendations. So this summarizes the arguments that were discussed there.

The next section summarizes the concerns that were raised in the public comment and in subsequent discussions and reviewing the public comments about the elimination of the losing FOA.

The next section talks about the alternative proposal to make the notification of the TAC request mandatory with that option to accept or reject. And the pros that were presented for that proposal, followed by the concerns and reasons that some oppose the proposal. And concludes that because the working group did not come to a conclusion on an alternative to the status quo that appears to be able to reach consensus, that the by default, the losing FOA is expected to be maintained.

So that's the summary of the language, and I encourage everyone to review that. And again, coordinate with your groups, and come back with feedback through—we'll set up a process for providing that input in a structured way so that it's easily reviewed by the group. Any questions? I'm happy to respond. Thanks.

ROGER CARNEY: Great. Thanks, Emily. Yeah, and again, I don't want to get into this here, I want to let us get into the other work. But this was just a proposal to pull all this together. And I think that, as Emily mentioned, I want to let the group have the next couple of weeks to digest this, and think about it and provide any feedback on it as well.

And I encourage discussion on the mailing list here about the pros and cons here. Again, I think this is laid out here to explain the group was somewhat not all agreeing on bringing the losing FOA back or removing it completely, so I think what we've settled on here is, okay, let's go to the default and keeping the functionality as it exists today.

And again, it's a proposal. I'd like to hear feedback from everybody that has concerns with it, or people that are in support of it, great, on the mailing list so that we can work through this.

And again, I want to give everybody a couple of weeks to think about it and put their words together for it. So I think the plan is let's take the rest of the month until November 30th, get everything down, written. And then our meeting on December 1st, we'll cover it and get up behind us and move forward on recommendation two either way, whichever way we ended up going. But again, take the next couple of weeks. Let's chat about it on the list. And then we'll get on to these other items that we need to clear out. Steinar, please go ahead.

STEINAR GRØTTERØD: I'm a little bit confused, because my understanding was that when we created the workgroup, we decided upon when we published the initial report was some sort of set of processes that we [believed] was improving the security and also improving the time spent on the transfer.

And what I also understand is that based on the comments from the public comments, we have to revert something, and particularly the losing form of authorization.

[But so, are there more elements?] Is that the only thing that we're kind of reverting? Or are we back on more or less the skeleton of the present transfer policy?

And I'm not sure whether this is—let me phrase it this way, I'm representing At-Large. I don't know how this will be taken,

because At-Large, some sort of have their initiative, idea that we should make a transfer process safe, secure, and also an element of more speedy than the existing one.

I hope we can at least keep the safety element and the improvement of the safety element and also reduce the length of a normal transfer. So I'm really looking forward to particularly the comments from the registrars, in the changes that we have done to the initial report, and whether this is purely the losing FOA that is the critical element, or if there are other implementations methods that will kind of revert back to the present policy. Hope that was some sort of a signal that I'm a bit disappointed. Thank you.

ROGER CARNEY: Great. Thanks. Yeah, and just to be clear, we're only talking about one recommendation, all the other ones staying the same. Recommendation two, what our recommendation was to remove the losing FOA, and now we're suggesting that that may be maintained in that pending transfer spot at the end.

And I think again, none of the other things are changing, no one's suggesting changes to TTL or anything like that, all those other factors. And to your point, Steinar, on trying to be efficient, I think that's exactly what I tried to mention earlier was, yes, we were losing on the efficiency gains that we were hoping for when we made the initial recommendations. But again, it's out of the functionality, recovery, I guess, of the registrant having the ability to acknowledge or deny it, and providing that possible—I don't know if it's a security mechanism or not, whatever you want to call

it, but the fact of once a TAC is provisioned, if it gets misused, this proposed strawman helps in that possible misuse with the ability for the registrant to still stop that transfer after that.

So, again, just recommendation two. All the other security features, the standardized TAC, the storing of it securely, the only provisioning it when it's requested, TTL, all those things are going to remain. And one thing to think about, we talked about it now, I think, several weeks ago, is when we were talking about if the losing FOA functionality made sense, there was some discussion around the duration. And today's current policy, it's five days, the registrant has five days to acknowledge or deny it.

And there was discussion of if that should change, if that should go to a shorter time period or not. There were some public comments around that saying that a shorter time period didn't seem like it would matter, it was just that ability was more important than how much time they were given.

So maybe that's something ALAC can think about as well, does that make sense? And again, not just ALAC, but everyone. Does that make sense for it to be five days still? Or should it go to a shorter period or change period? So just something to think about. Theo, please go ahead.

VOLKER GREIMANN: Yeah, I think that's an important point that Steinar raises there, because it basically touches upon the process that we are on and the decisions that we made in the earlier phase.

Now like you said, Roger, many times, nothing is set in stone. And I think just then we were looking at the strawman revision so to speak, I think that is just adding an extra element to it. Or not even adding but just moving up some security piece, which was there, what's currently written down as a security feature, is just moving up the chain a little bit like you just said. Instead of doing it in the beginning, we do it at the end. But that also will affect the recommendation itself on the TAC provisioning, which needs to be changed in some shape or form. Because currently, that is not working for wholesale registrars when it comes to the notifications.

Like I said before, our only notification is email to the registrant. And that is the only way to communicate to the registrant. And that is not workable, at least from a security perspective sending a TAC code, I mean, that is sending like a unique key in plain text, like a password in plain text. So that is something we need to avoid. And the current language is way too strict in how we should do that as a registrar.

I know, I'm completely aware, if you're a retail registrar, you don't really care because you've got all these other means through control panels or God knows what to communicate with a registrant, but for a wholesale registrar, our options are extremely limited.

So there is going to be some change, in my opinion, in detect provisioning also. And that is going to be interesting when we talk about process, how we walk back a little bit.

But like I always say, it's better to have clarity during the process than at the end of the process, because then it's usually said and

done, and then we have a problem. And I apologize that [I come with that] now. I should have done it month ago, but it didn't dawn on me. I think breaking away from the process last week gave me some clarity like, okay, we need to do this differently, because we're on the wrong track here. Thanks.

ROGER CARNEY: Great. Thanks. Yeah, and I just suggest, again, as you mentioned, the sooner the better. And it's good that you're bringing it up now. I'd suggest—you pinpoint exactly the language that doesn't quite work and maybe put that on the list, and just make a suggestion as to a better language there. And then we can work from there.

So, again, thanks for bringing it up to your point. Yeah, the sooner the better. It's better than when we get to—even flagging it in in a few weeks. It's better that we know now than then. So earlier is better. Great. Thanks, Theo.

Okay, so again, let's plan to talk about this on list for the next two weeks up until November 30. And then December 1 meeting, we'll pull this back up. And we'll get this closed and behind us, and we can continue on. All right, let's jump back to our agenda. Let's jump to recommendation seven.

EMILY BARABAS: Hi everyone. On our last call, we went over at a high level some of the input that was provided on recommendation seven. So we'll dive today into some of the details. Roger, shall we just go through one by one?

ROGER CARNEY: Yeah, let's do one by one. Thanks.

EMILY BARABAS: Okay. So as a reminder, this is about the composition of the TAC referencing RFC 9154. So starting with the concerns, there's a cluster of concerns that are all connected to RFC 9154. But each is a little different.

So the first one kind of refers back to some of the vulnerabilities of the TAC and refers back to the [inaudible] proposal that we discussed under recommendation one. So where these have come up previously, we've sort of referred back to this deliberation. So of course, let me know if we need to dive into that further here.

The second comment references section 4.1 of the RFC and suggests that, as I understand it, the group of permitted characters is restricted even further than the RFC specifies. So this would sort of be narrowing further some of the requirements around the permissible characters for the TAC.

The third comment is similar to one that was previously discussed from Org but this is not from Org, this is from another commenter about the fact that the RFC says that the TAC should be provided over a secure channel, and that, for example, email or SMS would not meet that standard.

The group previously discussed a couple of calls ago under recommendation three, that, folks, at least at the time, were not

interested in moving forward with a specific recommendation to require an encrypted channel, for example, for provisioning the a TAC.

And then there's one additional comment here that says that the RFC has a weakness in audit trail capability, but doesn't make a specific recommendation regarding the working group's recommendations on that. So Roger, shall I pass it back to you, and you can facilitate any further discussion on these items?

ROGER CARNEY: Absolutely. Thanks. Theo, please go ahead.

KEIRON TOBIN: Yeah, thanks. So the way I'm looking at things right now is I think the RFC 9154 is very handy for the implementation of several sections regarding the TAC, regarding security, and how it should be set up and defined, etc.

But it will be a guiding principle, because when we talk about the actual security requirements that will be upon registrars and every company within Europe, and basically every company that deals with Europeans as a customer, the NIS2 is almost there. I mean, the final text is almost agreed upon. I mean, all the drafts have been sent out to everybody who's interested in the NIS2, and the NIS2 will be de facto leading throughout the entire industry.

So when it comes to something like audit trail capability, that is already covered within the NIS2, it's not there like written language, like you need to have an audit trail capability. But it sets

very high requirements on how you set up security as a company within the EU, which is also applicable to registrars in the EU.

The NIS2 will set up major requirements to beef up your security as a registrar, yourselves, but also for your customers, because that is basically what the NIS2 is driving at, increased security on every level.

Since that will be a law in every member state, it is going to be the law and everybody has to comply with it. So I'm not too worried about any weaknesses of the RFC. It will be a guiding principle, but you as a registrar will still need to do a lot more, like adding audit trail capability. So we don't have to include all of that. Thanks.

ROGER CARNEY: Great. Thanks. Yeah, and I don't remember—I have had a couple of discussions about 9154. And I think that one of the keys was, there's a lot of good things in there, and we're not going to use everything that's in there. I think that that's something important to recognize, is yes, they've identified a lot of good things, and we're going to pull those out and use them. But they've put a lot of stuff in 9154 that we're just not going to use at all.

So I think that 9154 is great. And I wish Rick was here to at least support his own paper here. But maybe I'll make Beth pretend to be Rick today and stand behind his paper.

But I think again, 9154—and it's every RFC, there's a lot of good things in them, and you can use pieces of it, you don't have to use the whole RFC to make things better.

And the audit trail? Yeah, I thought, okay. I don't know that Rick and Jim's purpose was to create an RFC that worried about the audit trail. They've got that, as Theo mentioned, that's handled elsewhere. So I don't know if it's a shortcoming of the RFC, or if their intent was not to include it anyway. But anyway, yeah. Thanks for that. Keiron, please go ahead.

KEIRON TOBIN: Thank you. Just on the second note, where they've mentioned, don't use SMS and email, didn't we specify that that would be a notification and that would be down to the registrar to decide?

ROGER CARNEY: Correct.

KEIRON TOBIN: Yeah, I thought we did. So just on that point, we can kind of clarify that it will be down to the individual registrar that it's a notification and not a specific kind of email or something that they've identified there. Thank you.

ROGER CARNEY: Thanks, Keiron. Yeah, and we purposely left it as notification and didn't try to describe the mechanism to allow for future mechanisms. And as you mentioned, the choice by the registrar. So, Jim, please go ahead.

JIM GALVIN: So thanks, Roger. Just a couple of observations to think about here. 9154 does not have an audit requirement. But I'll observe that no security standard in the IETF has an audit requirement. Because an audit requirement is really a policy consideration. It's not a technical consideration in that you need it in order to achieve interoperability, which are generally [inaudible] in technical specifications unless it's a higher level best current practice of some sort, is a statement about what you need in order for two parties who want to achieve the same goal to work together. Audit is a higher-level function, and it's not part of the technical standards.

So I wouldn't call it a weakness per se. And I think it's entirely appropriate, if not mandatory, for us to add in this work here some audit requirements, whatever you want those to be.

The other thing that I'll say is 9154, taken in total, obviously, is a proposal for how to do things in a secure manner, trying to provide an answer for all of the security elements that are relevant for the context in which that works. Okay, so that's a lot of buzzwords in there.

Listen, I personally tend to lean on the side of practical security, as opposed to always wanting to achieve full security overall, that's just sort of my alignment in this space. And with that in mind, although it would not be perfectly aligned with 9154 to suggest this, and Rick is likely, if he wanted to defend his work fully, he would disagree with me, and that would be appropriate from that point of view.

I think it's reasonable for the registrars to kind of step back and think about what is the minimum that they want to achieve, from an interoperability point of view, what is the minimum that you want to make sure is present for everybody that gets you towards this more secure goal? Maybe it doesn't get you everywhere you think you probably ought to be. But that's a distinguishing characteristic in some sense. From a business point of view, you can do more if you want to be more secure. But you want to figure out how to—I think making choices about which elements are mandatory and leaving the rest as things you might do is not an unreasonable posture to take. And that's just my opinion about this. Just an observation here. Thanks.

ROGER CARNEY: Great. Thanks, Jim. And I don't know that—you stated it as your opinion, but I think we're hearing that from multiple people, is some of these items can be left up to the business model to decide. And again, all registrars aren't the same, all registries aren't the same. So they do have their unique business models that they work down.

And some of these, as you mentioned, Jim, some registrars may pull in more of 9154 if they feel like that that's something they want to do. But again, we have different business models across registries and registrars that we're not going to force all of them to do the same thing, because it just doesn't make sense.

Okay, and the one I wanted to comment on was the second one under A which is talking about maybe reduce the group to even more. And I specifically remember the TechOps group, when they

were writing the white paper, had talked about that. And they decided specifically about the zeros in the Is and things that get confusing. And I think it came down to—and maybe it's even in the white paper—that people aren't going to type this out. They're going to copy and paste it somewhere. So the confusing zeros and O's I think disappear. And I'm not sure that it's—again, I remember the conversations and I just remember that it wasn't worth the effort to go through that. So, Jim, please go ahead.

JIM GALVIN: To frame this a little bit differently, from a security point of view, from a technical point of view, you can't just start eliminating characters, okay, because that changes the [entropy] of what you're trying to achieve here. And it reduces your randomness. And that's obviously contraindicated to the goal we're trying to achieve here. And you would need to have some discussion with some cryptographers about making sure that you're still achieving your goal.

We have here a stated algorithm which has been accepted and reviewed and put into a standard from security experts, which includes some crypto people who have had the opportunity to look at this in the IETF. We can't go changing that for user interface kinds of reasons. And that's just a technical comment here that people need to take on board.

If this is the goal you want to achieve, where you're worried about being able to actually hand write these things or speak these things, as opposed to looking to other mechanisms of transmission, that's a different problem space, and we need to

look for a different technical solution. 9154 doesn't cover that. So that's what I would say there. I think we need to not try to solve the problem of handwriting and hand understanding them. We need to look for other mechanisms for moving this thing around, unfortunately. Otherwise, we need a different solution. Thanks.

ROGER CARNEY: Great. Thanks. Okay, so I think we're good on this. Emily, if you want to take us to the next one.

EMILY BARABAS: Thanks, Roger. So the next set of proposed edits were about adding additional elements to the TAC. So embedding for example the TTL of the TAC or the gaining registrar's IANA ID. And what we've done here is captured a few of the points that were discussed in the TechOps group about this issue that Roger relayed at a high level a couple of calls ago as well. And it seems from those discussions, like the group was trending towards not recommending that these things be included. But of course, everyone should sanity check these bullets that they're captured correctly. And of course, if there are additional points to raise, we'll capture those as well. Thanks.

ROGER CARNEY: Great. Thanks. Yeah, I think that at this summit, and even prior to that, I think there were discussions around what can be embedded and what do you gain, what do you forfeit out of that? So I think that the simple answer here is we're not going to try to make the TAC any more cumbersome ownership, whatever you want to call

it, onus. And I think we're going to leave it as it is. Again, some of these ideas seem to make sense. But once you dig into them, they start to lose their value, especially against the cost of implementing them. So unless anyone has any comments, we'll move on to the next one. Okay, let's go ahead and move on.

EMILY BARABAS: Thanks, Roger. So the next one is a bit of a language puzzle. And your input is very much recommended and needed here. ICANN Org provided some strawman edits. But again, these are just a suggested formulation to solve a particular problem and not prescriptive. So please take a look at that.

So the RFC 9154 talks about—or in Section 4.1 says that the implementation should use at least 128 bits of entropy as the value. And what is being pointed out here is that our recommendation is that the working group recommends that the minimum requirements for the composition of the TAC must be as specified in RFC 9154. But the RFC itself uses the term should instead of must.

So the request here is to clarify that in fact, the working group is recommending that this element about the entropy value is in fact a must as opposed to a should. So if the working group agrees that that is the intent, which from the staff side it sounded based on the deliberations was the intent, then we need to figure out a way in the language to reflect that effectively. Thanks.

ROGER CARNEY: Thanks. Yeah, interesting. And maybe I can call on Jim Galvin to give us a quick lesson on the meaning of should. My understanding, in IETF, should is it's not as in normal language should, as in it's optional. Should is, yes, you're supposed to do this and you have to have reasons not to do it. But I'll turn it over to Jim. Thanks.

JIM GALVIN: No, you're doing great there, Roger. I was going to take my hand down. But yeah, obviously, using must makes it an absolute requirement that in order for the protocol to function correctly, the goal that you're trying to achieve, this is something that you have to do.

Should is exactly as you said, it is a recommended usage, and strongly urged, if you will, but it's okay if you don't do and you've got good reasons not to do it, then that would be a thing that you would be able to back off of.

But you have to keep in mind that if you choose not to do a should, then you are risking certain interoperability issues. So I just want to say I think this is a great call out by ICANN Org, this inconsistency. I think that if we stick to the recommendation as it was originally intended, as I understand it, and certainly some discussion here might want to see that differently, we should put a must in the recommendation here. And I want to speak a little bit to this comment at the last sentence there about BCP 106 Being a normative reference.

Also, in IETF parlance, a normative reference is actually a big deal. So it does mean that it is a requirement within the standard, the fact that it's normative means that the standard itself, the rest of the text depends on it. And therefore, it would be duplicative for us to have to say it in the recommendation, which we did up there. So that's another nice call out there. It just suggests that we could in fact delete that second half of the sentence there in the recommendation, it would not be unreasonable to remove the phrase "Such values must be created according to PCP 106," because that's already required in 9154, as it's a normative reference. Just something to think about. Thanks.

ROGER CARNEY: Alright. Thanks, Jim. Okay, so the thought from ICANN—and Jim is concurring here—is that we do change the should of 9154. Again, the logic behind should still, to me, supports this modification, but change the should to a must in our recommendation. So must use a minimum of 128. So I think that that makes sense. And again, it's a good call out. And if anybody has any issues—Steinar, please go ahead.

STEINAR GRØTTERØD: I don't have any issues. I'm just trying to avoid that we have to go back due to the NIS2 recommendation. So [kind of a clear] question, when we in this policy and our proposals only referred to RFC 9154 and not add some sort of wording that there might be other security requirements that is more secure—I'm using a very [inaudible] word but more secure than RFC 9154 but the policy kind of states that you have to go to the old stuff and not to the

new one, will we end up in that kind of scenario? If so, then I think we should try to twist that wording into something that gives the opening for whatever comes in the future. Thank you.

ROGER CARNEY: Great. Thanks. How I saw that was obviously 9154 and its successor, so if 9154 is updated. But to your point, if it's even outside of that, to me, we're saying the minimum requirements and the minimum bits of entropy here. So I think that no matter how you look at it, the forward looking—you just can't go backwards. So you can't use 64 bits or you can't use less than what 9154 is saying, but you can always improve on those. So that's at least my read in the language. So, Theo, please go ahead.

VOLKER GREIMANN: Yeah, I don't think we need to sort of cement that kind of language. The RAA already forces us to comply with applicable law. So there's that. I do have a question, though. I'm totally not an expert when it comes to encryption. But assuming that a baseline is 128-bit and a registrar implements 256 bits, or 512, I'm not sure, isn't there a chance that if a registrar goes beyond the baseline, and implements something like a TAC that is encrypted with 512-bit—I'm not sure if it's even possible—isn't that going to break stuff at some registry level, other registrars? If anybody knows.

ROGER CARNEY: Thanks. I don't know that it would break anything in another registrar, but good point on [inaudible] for the registries, and I'm not sure if that would bother them, either. Jim, please go ahead.

JIM GALVIN: It should not break anything. The only thing that happens is what you're getting here with the entropy is a quality of randomness. And so the should here is sort of giving you a minimum quality of your randomness. But ultimately, if you choose a higher quality, then you're just allowing for that thing to exist and be more secure, without getting into details of how it all works.

The only issue that really matters to the registry is going to be the length overall of the actual TAC itself. And the syntax has that specification, and registrars and registries are subject to the same rules there. So if you try to do something there, you're going to break yourself as well as the registry.

ROGER CARNEY: Great, thanks, Jim. Thanks, Theo. Okay, I think we can move on from that one. Emily.

EMILY BARABAS: Thanks, Roger. So just to clarify, it sounds like we'll use the Org strawman as a starting point for the language and the revision. And if Jim or others have suggestions to make that a bit more clear or simple, or whatever else, they can provide those in their review of the comments. Does that work?

ROGER CARNEY: Yes. Great. Thanks, Emily.

EMILY BARABAS: Thanks. So the last proposed edit on this one says that RFC 9154 and BCP 106 require reference for further clarifications regarding the difference between current and previous RFC BCP. It sounds like this is a call for further kind of clarification of the text. But I don't know exactly what the comment is looking for. So maybe the next step is just to think about if the language is sufficiently clear and precise in the way that it's referring to these standards and the relationship between them. Thanks.

ROGER CARNEY: Thanks. Yeah. And I think that the IETF process already handles this. And I don't think that we have to get into it. I don't want to get into this policywise, this is something technical that the IETF can handle and does handle continuously. So I think that we'll leave it in their hands and not mentioned anything about it in policy, but I'll open it up to see if anyone has any concerns on that. Jim.

JIM GALVIN: I think that from a technical level, I agree with you, Roger, be interesting to understand what this comment is really getting at. Something that occurs to me is that we are both subject to clauses in our contracts. Well, I know that registries are, I guess I shouldn't say we both. I don't know how far this goes with registrars, honestly, in your contracts.

For when there's a specification for a standard, there's usually this interesting phrase when you get down to contractual language for this kind of stuff about you are obligated to comply with this standard, and its future updates and successors. So there's some little phrase in there about that. But I don't know how to translate that into previous in this comment here. But I don't know if anyone has any thoughts about this future business. Just wanted to call that out. Thanks.

ROGER CARNEY: Great. Thanks, Jim. And I don't know if Volker or Theo want to say anything. But yeah, registrars have similar language that they have to follow the successor paths down there. Okay, I think we can call this one good as well. and move on to number eight.

EMILY BARABAS: This is recommendation eight. This recommendation is about the registry verifying at the time that the TAC is stored at the registry system, that the TAC meets the requirements specified in preliminary recommendations seven. And there are just a couple here.

So the first one is a proposed edit adding the word syntax to the text of this recommendation to be prescriptive about the requirements that the registry is to verify. And I believe that this came from the Registries Stakeholder Group. So I think it's pretty self-explanatory what the suggestion is, but if folks want to provide additional flesh around that, please do.

ROGER CARNEY: Great. Thanks, Emily. Any comments from anyone? And maybe I'll just pose this to registries. Is all of seven just syntactical? Jim, please go ahead.

JIM GALVIN: Well, no, I think the critical thing here to observe is that there's no way for a registry to verify that you used 128 bits of entropy, for example. That's clearly an operational thing, which is not visible in any external way. And if you look at the results, when you look at a TAC, you have no idea exactly what mechanism was used to create that value. And I just think that that's the point being made here. So there's just limits to what's actually possible. And just calling that out.

ROGER CARNEY: Thanks, Jim. So I think that the suggested text should work out then for us. Alright, let's move on to B.

EMILY BARABAS: B was another comments from Org. And I think that this was actually just an oversight in drafting because this was probably an earlier recommendation that we drafted before we were being as consistent as we should be with the shirt and muster and so forth. But it's basically saying that if this is a requirement, that it shouldn't just say that the working group recommends that the registry verifies the TAC syntax, but that it must verify. So I do believe that that was the intent, but I think it was just sloppy drafting on staff's part. If everyone agrees, we can correct that. Thanks.

ROGER CARNEY: Thanks. Any thoughts on that? Seems to make sense. Yes, that they must verify. Okay, I think we can close that one.

EMILY BARABAS: Okay, next up is recommendation nine. So this is about TAC generation, storage and provision. And 9.1 is that the TAC must be generated only by the registrar of record upon request by the RNH or their designated representative. 9.2 is that when the registrar of record sets the TAC at the registry, the registry must store the TAC securely, at least according to the minimum standards as set forth in RFC 9154.

And 9.3 is that when the registrar of record provides the TAC to the RNH or their designated representative, the registrar of record must also provide information about when the TAC will expire. Just a couple of items on this one.

The first comment notes that 9.1 doesn't contemplate the registry being the one to generate the TAC, instead of a registrar, and notes that there should be logging of failed requests at gaining registrars and that information should be shared with targets and perhaps trigger enhanced security measures.

ROGER CARNEY: Thanks, Emily. Yeah, and I think that we kind of talked about this at one time when we were trying to figure out if we could put limits on number of attempts and things like that. We didn't look at it from the gaining registrar perspective, we looked at it from the

registry perspective of tracking that, because the theoretical is the gaining registrar, if they're tracking it or not, that wasn't a concern. It was more of the registry. But I think we decided that that wasn't all that useful. Theo, please go ahead.

VOLKER GREIMANN: NIS2. I mean, it's going to apply to the law. I mean, we don't have to have policy around this. And that is the beauty of NIS2, when you have actual regulation which forces you to think about all these kinds of things, either when it comes to logging, how to deal with some kind of brute force on any level, not just the level that is in this comment here. But you need to take it all, you need a complete holistic approach when it comes to implementing NIS2, and for some companies, it's going to be very dramatic, because they haven't done anything for years. For some who already are on top of the game, it will be a continuation of what they're already doing. But you need to review everything within your company over and over again. Especially stuff like this. Thanks.

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

JIM GALVIN: Thanks, Roger. An observation here about how to think about this. Certainly, one way in security practices is to account for all kinds of attempts to access. So you could make requirements about failed access attempts as well as valid ones.

What I want to call out here is the way I view this total picture of what we have here, we account for the TAC itself is one-time use. And that's mandatory and required of all parties. So from a registry point of view when a TAC comes up, if we get a TAC that matches what's stored, then that automatically means it can't be used again. So now we're going to see if the rest of what's necessary here is successful.

And if the rest is not successful, well, it still can't be used again. And what I mean by that is we have this transfer confirmation, the new word, instead of losing FOA, that we're talking about. So once a valid TAC is accepted, if the transfer confirmation fails then obviously, you can't use that TAC again.

On the other side, rather than counting failed requests, the TAC has a TTL. And so it has a lifetime which is defined and has to be managed. So you can either provide for making it ineligible for use after a certain number of failed attempts, or put in the TTL instead to take care of that.

I could go either way. But some other considerations here, the value of the TTL, let's go back to the previous discussion we had about whether or not the TAC itself should be something which is readable or pronounceable, or something I can write down.

One of the advantages of, well, gee, if I'm entering it wrong, or giving it to the gaining registrar wrong, I want to have a lot of options for being able to put that in there. So the balance against any potential denial of service attack is the TTL. And you allow the registrant multiple opportunities to do that.

I'm sure we've all experienced passwords where you get X number of failed attempts, and whatever fat fingering is going on. Surely you've experienced getting it wrong when you know it, but nonetheless, and isn't it just hateful that you have to now go through a password reset process?

These are all user interface and user interaction issues. I just want to call them all out and say that I think that we have two mechanisms in place. It's one-time use and TTL. And let's make sure that we hang on to those as being responsive to this issue of failed access attempts. I'm not saying that we shouldn't do something different if you want. But that is the solution in place at the moment. Thanks.

ROGER CARNEY: Great. Thanks, Jim. And I remember the discussion we had on trying to count and things and we even talked about the bad actors that could come in and try to stop a transfer by purposely just sending in a bunch of wrong TACs, and if we put limits on them, then we're going to stop it and things like that, or maybe there's a rogue registrar that's losing transfers, and they start doing that themselves, just to stop the transfers from going through. So I think that there's both sides, as Jim mentioned, but I don't think that we need to get to that. And as Theo mentioned, the logging aspect of this, that's going to be not just by NIS2 itself, but other laws that require [inaudible] log these events anyway for security reasons. So, Keiron, please go ahead.

KEIRON TOBIN: Thank you. Just a quick question for Jim. So, Jim, if it was to fail on a registry side, I take it you guys would be able to investigate that when it came up.

JIM GALVIN: Well, I mean, you're asking me to—certainly a registry, I would think that registries could make the choice of as an ordinary security feature for their own services, to take note of repeated failures on a transfer attempt. And they certainly could, if they chose, choose to investigate that and look into it.

Whether or not registry would do that? I don't know. Different people have different reasons. Different business models, different concerns. So it's something that could happen, but I certainly don't want to speak for all registries and say that they would.

KEIRON TOBIN: So I'm trying to work out the definitive point is to—for example, if a registrar blocked it, would you guys be able to identify that as opposed to just someone using an incorrect character, for example?

JIM GALVIN: Well, now you're getting into what registries would log or not log. Certainly, registries that are doing a full complement of security protection would have rather complete logs. And when they investigate, they kind of see what's going on. It could be interesting that you get a lot of failed attempts over here, and then

suddenly, it's successful over here. That might be something that somebody wants to look at and compare.

Logging requirements, again, as we've said here before multiple times, we there's a lot of audit requirements that we don't have here. If you think that's important, then that's something that we should talk through and see what we want to do. And then of course we would have to ask our registry, other colleagues here how far they want to commit in terms of logging and processing.

KEIRON TOBIN: Okay, thank you.

ROGER CARNEY: Great, Theo, please go ahead.

VOLKER GREIMANN: Yeah, and the amount of logging that a registrar does, that is also somewhat dependent on the business model. We can't do without it. We need to log everything, for legal reasons to start with. We need to prove that this and this happened on this in this time, on the second, because there's a dispute about whatever. And that could be a legal dispute, but also like basic stuff, our technical support staff answering a reseller, like this transfer happened on this and this day, and was approved by this and this and this, it was yourself or you logged into the control panel, you deleted all your domain names so that wasn't an incident, we got pre-approved like it was this user, etc. So it kind of depends on your business model. But I think in general, registrars log a lot,

because customers have a lot of questions about all kinds of things that happen to their domain name. Thanks.

ROGER CARNEY: Great. Thanks. And I think that you'll see that. I think even if you wrote logging requirements, you're probably going to be [inaudible] the basement of those requirements, because most registrars, registries log more than you realize. Steinar, please go ahead.

STEINAR GRØTTERØD: From my experience with all the transfer from a corporate registrar point of view, what I think will be very handy is when there is a failed transfer and whether this is caused by an incorrect TAC, or is that just the fact that the TAC has expired? If possible, if this in some way could be communicated to the guy that's requesting the transfer, this will be very handy. And I'm talking about quite normal situation where there is no compromised account, etc. This is just a regular workflow that we need to find out. And this is very useful information. Thank you.

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

VOLKER GREIMANN: Yeah, so while Steinar's example is very clear, it also is very clear that we already have logging to go with that. I mean, we can't operate without logging. I mean, if somebody needs to know what

happened with a transfer, then our staff needs to answer. “Well, the authorization code you provided was incorrect. We got to denial from the admin contact, or the registrant contact, the transfer went wrong for this, this and this reason.” We can't go without it.

We can tell a customer, “We don't know. It failed.” That is not enough nowadays. Maybe 20 years ago, you could barely think that is an option back then, but you need to tell your customers what happened. Because if you don't, they keep making the same mistakes. They will keep providing the wrong authorization code.

So when somebody enters the wrong authorization code, our system already pings back that's the wrong one. We don't want to have any emails or phone calls dealing with invalid authorization codes. We want to avoid as much questions as possible, because it's just overhead, costs money. So we try to make our systems dummy proof as possible. So we can explain to them what's happening real-time, what went wrong. But if we get questions, we certainly need to have the logging and have our tech support team going like, “Okay, this is what happened,” so people can learn from it and know exactly what they’ve done wrong.

ROGER CARNEY: Great, thanks. Okay. So I think on this one, as Sarah mentioned, this is a good idea. And people should be doing this and as Theo mentioned, our legal requirements make us log certain things and most things. So I don't think that we need to add any policy language around this from a gaining registrar perspective. It's going to happen because of the legal constraints that they have.

And so I think we can move on from that. And we've got one minute, but I wanted to try to close nine out if we could, Emily.

EMILY BARABAS: Thanks, Roger. I think this is a pretty straightforward one. It just notes that 9.2 references RFC 9154 but neglects to mention the potential for successors and include those as well. So I think that that's a logical addition, unless anyone has concerns. Thanks.

ROGER CARNEY: Great. Thanks. Yeah, I think that makes sense to add that. If anybody has any issues, let us know. Otherwise, we'll consider nine done and we'll pick up on 10 Thursday. But again, just a reminder, redline changes for the recommendations will be coming out shortly. And we'll try to stick to a two-week window of getting those redlines flagged and up for discussion or approved. And also on strawman for recommendation two, let's take that to the list and make sure we get those discussed by November 30. And on the December 1 call, we'll get that closed out for us.

Okay. I think that we're at time now and I want to thank everybody. Great discussion. Great work today. Great progress, and we'll see everyone Thursday. Thanks, everybody.

[END OF TRANSCRIPTION]