ICANN Transcription

Transfer Policy Review PDP WG

Thursday, 08 December 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/b4IFDQ

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

TERRI AGNEW: Good morning, good afternoon, and good evening. Welcome to the Transfer Policy Review PDP Working Group call taking place on Thursday, the 8th of December 2022 at 16:00 UTC.

For today's call, we have listed apologies from James Galvin and they have formally assigned Beth Bacon as the alternate for any remaining days of absence.

As a reminder, the Alternate Assignment form must be formalized by the way of Google Assignment link. The link is available in all meeting invites. All members and alternates will be promoted to panelists. Observers will remain as attendees and will have access to the view chat only. Alternates not replacing a member should not engage from chat or use any other Zoom Room functionalities. If you have not already done so, please change

your chat selection from host and panelist to everyone in order for all to see the chat and also to be captured on the recording.

Statements of Interest must be kept up to date. Does anyone have any update to share? If so, please raise your hand now. Seeing or hearing no one, if you do need assistance, please e-mail the GNSO secretariat.

Please remember to state your name before speaking for the transcription. Recordings will be posted on the public wiki space shortly after the end of the call. As a reminder, those who take part in ICANN multistakeholder process are to comply with the Expected Standards of Behavior. With this, I'll turn it back over to our chair, Roger Carney. Please begin.

ROGER CARNEY: Great. Thanks, Terri. Welcome, everyone. Before we jump into our agenda, we don't have anything major to share. But I just wanted to open the floor up for any stakeholder groups that might have had some discussions or want to bring anything forward that they've been talking about or been pondering within their stakeholder groups. So I'll open the floor up to anyone that wants to bring anything forward.

Okay. Let's go ahead and jump into our agenda and work our way through here. I think we'll jump into number three here, review of the small team on the MAY Deny reasons. A group of people met right after the call, maybe some stuck on the call, stayed on the call and listened in to the discussion. But it was a good discussion, it actually resulted in a fairly quick language update to Rec 19 item

one there, which today, obviously, is just evidence of fraud. In our initial report, we expanded that to domain use and abuse policies and a lot of comments came back that that was too broad or could be possibly abused. So the small team on Tuesday quickly went through some language and came to this language here. So let's go ahead and just read it. I think this was supplied. But let's go ahead and just read it and see what everybody thinks and see if we can move forward.

The update that was suggested and agreed upon in the small group was evidence of a fraud or B, the domain presents an active DNS security threat as defined at this URL, which is maintained by ICANN. Here's the URL location. A couple comments on this. It was suggested, well, it's just a URL and it could change, which is true. I guess, the pro to it was as things change, this can be updated without having to go through the policy and update for a new security threat. It was kind of the good … As we know, this can possibly change. It'll have to be watched by those that are interested in it and are affected by it. But it did allow the flexibility of ongoing future security notices or changes. This is what the small team came up with.

Good question, Sarah. If it's clear enough, that evidence is for both. It's evidence for fraud or it's evidence for the domain presents. Access, it's clear to him just because of the way it's set up. Maybe a comma after fraud. To me, marking it as an A or B option. The lead of the sentence to me always goes with that. But yeah, it's obviously something we want to make sure that's clear. So is it better if we do put any punctuation or if we just say evidence of fraud or evidence of domain presents an active DNS

threat? Do we just move for clarity, add evidence in twice? Thoughts?

BERRY COBB: Roger, if I may interrupt. I see Mike Rodenbaugh has his hand raised in the participants. Mike, you want to accept the upgrade to panelist, please?

ROGER CARNEY: Thanks, Berry.

MIKE RODENBAUGH: Sorry about that, Berry. Thank you. This is Mike Rodenbaugh for the IPC. We had a couple of questions come through from our group on this one. The first one, I think I know the answer. This is a MAY NACK, not a MUST NACK issue.

ROGER CARNEY: That's correct. That's correct, Mike.

MIKE RODENBAUGH: My constituency, we're wondering why this is not a MUST NACK rather than a MAY NACK. We had a couple of comments to that effect from corporate domain name registrars, actually, wondering why that's not a MUST NACK instead of a MAY NACK.

The other question that came through was what has happened to the proposed revision that we'd made earlier to Rec 19 about

violation of the registrar's domain use or anti-abuse policies? Is that now gone? Are we keeping that somewhere else?

ROGER CARNEY: That is gone now. This language replaces that old language. For your first question, I'll let people answer that. We kind of talked about it on the last call in the small group. So I'll let anybody talk to that, your first question on that. If anyone from the small group or anyone wants to—why is this a MAY and not a MUST? Anyone want to chime in on that? Zak, please go ahead.

ZAK MUSCOVITCH: Reading it, Mike, it would appear that, why shouldn't it be MUST? If there's evidence of fraud or evidence the domain presents an active DNS security threat, shouldn't it be that the registrar must withhold transfer the domain name? The reason that it's MAY is that there's a question about what level this evidence rises to.

So for example, a complainant writes into the registrar and says, "I allege that there's fraud in connection with this domain name. My evidence is A, B, and C." A registrar then would be in position to receive that and review it and say, "You know what, I agree. There is sufficient evidence of fraud such that I'm uncomfortable in preventing the transfer out of this domain name." But on the other hand, a registrar could receive that complaint and say, "Hey look, I see that you think that there's evidence, but you really haven't been clear. You haven't cited it, you haven't given us examples. And I don't consider that sufficient evidence." That's why there's

this residual discretion that's left to reside with the registrar. Thanks.

ROGER CARNEY: Great. Thanks, Zak. I don't want to speak for anyone else. But the other issue came up is wherein a certain jurisdiction that may be considered fraud, but if they moved it to another jurisdiction, then it may not be fraud. So you wouldn't want to deny the transfer if they were moving it to a possible other one. So I think that's just a few reasons why it stayed in the MAY. Hopefully that helps, Mike.

MIKE RODENBAUGH: I appreciate the explanation but I don't buy either of those explanations. Roger, what you just said makes no sense. Fraud is fraud anywhere. That doesn't change amongst jurisdictions. That's just not true in my experience as a lawyer for 25 years. And of course, now that we're defining DNS security threats very specifically, that's not true. Those are the same for every registrar everywhere in the world as clearly now defined. So I just don't buy that one at all.

As for what Zak was saying, registrars should maintain discretion. I also don't really believe in that. I mean, maybe we can change it to say, "Presented with clear evidence of fraud and make it mandatory." Otherwise, we're allowing registrars too much discretion to transfer a name even though it's been identified as having fraud or a DNS security threat. The other thing we could do is split the baby there, if the real main concern is around evidence of fraud, and that may not be clear enough, okay, fine, then that

can be different. But for DNS security threats, that is either is or isn't. There's not usually an IF there. So in those situations, it should be a MUST NACK. That would be our position.

ROGER CARNEY: Okay. Thanks, Mike. Keiron, please go ahead.

KEIRON TOBIN: Thank you, Mike, for your insight, knowledge into global jurisdictions, very useful there. But just to let there are some countries out there that do have just different jurisdictions. For example, India doesn't allow any form of pornography on the website, whereas actually in the U.S. and other states it does. So, different jurisdictions, different laws, which is why it should stay in the MAY. Thank you.

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

OWEN SMIGELSKI: Thanks. I see Mike put the chat, "Porn is not fraud." But yeah, it is considered illegal, and under the definition that we had for fraud, that could be used as a way to block or deny a transfer for, say, an India-based registrar. Other examples could also be insulting the Kingdom of Thailand. A registrar in Thailand might have some concerns with that, but they might want to let a transfer out someplace else that could do that. Mike, I'm not going to argue what that is. But I'm just saying defamation is not fraud. However,

fraud, if you look at the definition, can be a very broad term that can be applied to generally pretty much all illegal activities out there, and that's kind of an approach that ICANN has been taking and that's what registrars have been taking as well, too. So that's why I'm very hesitant to do that. Because there may be a registrar based in Russia that has an anti-Putin website that's hosted there, and they might want to let it go away, because for whatever reason, they're feeling altruistic and that could be considered fraud in Russia. So they have the option to let that transfer if they want to. So I think that we should keep the definition here at the MAY and not really make a massive, drastic change here even after the initial report because there would probably be a lot of community feedback in here. I think this is kind of the wrong time to be doing that. Thanks.

ROGER CARNEY: Thanks, Owen. Zak, please go ahead.

ZAK MUSCOVITCH: Thanks, Roger. Just to pick up on Mike's points, which I get, they're well taken. But, Mike, my question is if a complaint comes in from a concerned party or an IP owner, for example, that makes the allegation of fraud—and we'll leave the DNS security threat for a moment, push that to the side—but if the allegation comes in that a fraud is taking place and the complainant makes references, some evidence of the fraud, who determines whether that evidence is sufficient? Suppose the registrar takes the position that that evidence is insufficient but the complainant says, "Well, it is sufficient in there for you," you breach the Transfer

Policy provisions which require you to withhold a transfer based upon the existence of a fraud. So this is the question, Mike, is that if it's actually MUST, if a registrar must withhold the transfer, wouldn't that be putting registrars into a breach situation if they didn't believe that the evidence rose to the level of evidence of fraud?

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

MIKE RODENBAUGH: Zak, I hear you. I think there's different levels of fraud. So if it's very clear, for example, phishing, but that would come in through the DNS security threat. So that doesn't bother me so much. I think maybe the way to do this is to split it, to make fraud a MAY and to make DNS security threat a MUST. Because I'm not hearing—maybe someone wants to chime in, explain to me whether there's any vagary around whether it is a DNS security threat or not.

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

STEINAR GRØTTERØD: Hi. I do understand that—well, let me rephrase. From a practical point of view, I think that very often the registrars and the registry operators use data from the different reputation blocklist in defining whether there's suspicious behavior also within the DNS

abuse area that is connected to a certain domain name. One quite regular situation that I experienced is that even though the registrant or those who can mitigate had taken the action is not being removed from the reputation block list. So, there might be a period where the domain name, by looking at the data from the reputation block list, is seen to be suspicious but impractical, it may be sold to the best.

In this period, if we have that scenario, there will be some problems for the two parties, to losing and the gaining registrar, exactly to kind of prove that things are okay. Because the reputation block list is not updated accordingly. Also, adding to that is that my experience is that these reputation block lists can be seen as trustworthy in different ways from the different registrars. So I feel it's very hard to put a MUST on this for a DNS abuse point of view. I think it solves the rationale and solves the IDs if we put a MAY, and I think that's the best way to do this. Thank you.

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

ZAK MUSCOVITCH: Thanks. What Mike had been suggesting in terms of splitting these off, I think what he was saying is that evidence of fraud can remain as made, but he was suggesting that if there's an active DNS security threat is defined in that link, then it must be disabled. So my question is, looking at the list of DNS security threats in the definition—botnets, malware, pharming, phishing, spam as it's

used to propagate other DNS security threats—do registrars, in their experience, have difficulty in ascertaining whether these things are taking place upon a complaint, or is it the fact that once a complaint is made alleging one of these DNS security threats, that they're generally able to definitively identify that this threat is taking place, and therefore, there's no reason to leave it discretionary and not make it mandatory?

ROGER CARNEY: Good question, Zak. Steinar, please go ahead.

STEINAR GRØTTERØD: This is touching the problem that we have that in the Registry Agreement and also in the RAA, there is no reference to a use of certain reputation block list. Meaning that you very often have a scenario that if a blocklist kind of monitor both for using phishing as an example, one block list will identify a certain domain name connected to phishing, but another block list provided that to also have it within the system. Monitoring for phishing doesn't recognize this domain name for phishing. Since the registrars do not have, they can choose how they want to monitor and mitigate abuse. Then we have a scenario saying that, "Well, my feed doesn't say this domain name is connected to suspicious behavior," in this case phishing. And the other part saying well, "My feed says it clearly is." That's the problem we have with this. Thank you.

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

ZAK MUSCOVITCH: Thank you. I get the point, Steinar. My question to you or anyone else is this is that if a complaint comes in that's relying on inclusion in an RBL and registrars understand that that might not be definitive of anything because, as Sarah said, it's hard to get off that list in some situations. In other words, just inclusion on such a list isn't proof of anything necessarily, although it could be a good indication in most cases, would the registrar be in a position to say, "Well, your provision of this domain name on that list doesn't prove that there's inactive DNS security threat. We actually would need to be provided more evidence to show that that's in fact the case. And if you are able to do that, then yes, we shall remove it."

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

THEO GEURTS: Thanks. I just noticed that Steinar just made a comment that it's a good indication when you're talking about reputation block list. These block lists are often completely without context, it's just a list of a domain names that are supposed to be bad. But it doesn't say why it is bad or there's no info at all about it. So as a registrar, you always do your own due diligence and check it out why it is bad. And based on that evidence, which is still circumstantial at best, then you make the decision not to suspend the domain name and usually make sure that the thing cannot transfer out to a different registrar. Though in my experience, 99%, maybe it's even

a little bit higher than the 99% of the cases, you suspend the domain name and there's no transfer hopping going on anyways, because these guys just move on to the next target. They set up a new account, add a registrar or a different registrar, and start doing whatever they are doing. Thanks.

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

MIKE RODENBAUGH: How do we stop the notion that if a registrar just doesn't want to deal with a security threat for whatever reason, that it still has discretion to push it, even though it knows that there's a threat going on? I just feel like there should be no discretion in that situation where the evidence is clear there's a DNS security threat, the name cannot be transferred. I don't see how it's really defensible to argue otherwise.

ROGER CARNEY: Thanks, Mike. I think one issue on that is that it's clear and who's making the decision on clear. That's obviously always an issue that comes up. Zak, please go ahead.

ZAK MUSCOVITCH: In regards to Mike's point, I think what you're suggesting there, Mike, with clear evidence is a higher standard of proof than just evidence. So it's akin to saying if there's proof or it's self-evident that there's a DNS security threat, then the registrars should be

required on a MUST basis to prohibit the transfer out. Maybe that's language for the group to consider because that's a very high threshold.

What Mike's essentially saying is that if you know that this is an active DNS security threat, then you must prohibit the transfer. I don't think that registrars would take issue with that. A complaint might say, "Well, you do know," and a registrar might say, "No, I do not know." And then if the if the registrar has a good faith belief that they haven't been provided with the level of proof that's required for them to know, then they are off the hook.

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

MIKE RODENBAUGH: I'm suggesting that in the chat. Basically, we could bifurcate this and say that where there's clear evidence, you must. Where there's just evidence, you may.

ZAK MUSCOVITCH: Sorry, Zak again. I don't think clear evidence is the appropriate threshold, Mike, because evidence is just an indication that it's not necessarily equivalent to proof. I think what you're saying is that if it's indisputable fact or self-evident or the complaint has provided proof.

MIKE RODENBAUGH: I guess we would we would say in the U.S. clear and convincing evidence.

ZAK MUSCOVITCH: That might be workable. I'd like to hear what the registrars say.

ROGER CARNEY: Owen, please go ahead.

OWEN SMIGELSKI: I think we should keep fraud again as a MAY because one definition of fraud is "Wrongful or criminal deception intended to result in financial or personal gain." Under the porn example that Keiron raised earlier, a person in India setting up a porn site, I think meets that definition of fraud. However, my registrar has no concerns with that. So we would possibly want to allow that transfer out, we have no concerns with that, again, just speaking hypothetically. I don't want to take a position on this one way or another. So I think that is one of the things where we want—and then I see Keiron put in there, LGBTQ and a number of jurisdictions, that is 100% illegal. But I think we're for free speech, we might want to allow them to transfer out if they're at a registrar where they're feeling threatened or something along those lines. So I think there are some things where this is permissive. It's not 100% completely, fully illegal activities such as phishing or a type of security threat where it's well established that these are bad things that we don't want to allow to propagate. But certain things may be allowed there. So I think we need to give the flexibility to the registrar to decide when are they going to essentially break

the contract with their customer and not force them to do it in every situation. There need to be some leeway. Thanks.

ROGER CARNEY: Great. Thanks, Owen. I think Zak put in chat. I think everybody seems comfortable with evidence of fraud. I look at it in today's policy. That's the only reason we have. Obviously, there was a lot of discussion about today if a registrar locks a transfer because of DNS abuse but they actually get in trouble for that, a complaint can come in saying, "Why didn't they allow my transfer because there's no reason not to?" ICANN Compliance will call the registrar and say, "Yes, you have to allow the transfer," even though in today's world, even if there is convincing evidence, they have to allow the transfer and just because the policy doesn't allow for it.

This wording here again gets to the point of expanding that so that it can be enforced that "Hey, no, we're not going to allow this." To Mike's point, should it be a MUST? I don't think I can make that decision. But adding it in to the fact of it is a huge step forward, I think, for registrars that are trying to work within the DNS abuse constraints and functionality. So I think adding this into that MAY is a huge step. Should it go to a MUST? I think that's up to the group. Owen, please go ahead.

OWEN SMIGELSKI: Thanks, Roger. I just wanted to clarify about denying a transfer for DNS abuse. I don't know if in all situations ICANN Compliance would necessarily require a domain like that to transfer out. I know we've had complaints about that and we've told the registrant to

go fly a kite. If we've got a clear abuse on our platform, we're blocking that domain and not letting it transfer out, disabling it. But again, I don't want to speak on behalf of Compliance. There may be some scenarios and situations, a fact pattern where a domain name may need to be transferred out or allowed to be transferred out. But I just don't want to give the impression that all abuse of domain names have to be transferred out and ICANN Compliance is telling registrars to do that. Thanks.

ROGER CARNEY: Great. Thanks, Owen, for that clarification. Steinar, please go ahead.

STEINAR GRØTTERØD: I'm not supposed to argue for this in too many ways because with At-Large, I think this is definitely more in the hands of the registrars. I do like to say that I like all the processes that the registrar and registries, the contracted parties had done in the work of both defining DNS abuse, the processes to mitigate DNS abuse, etc. But we're still in a situation where the contracted wording both on the registry and the registrar side is kind of diffused in what sort of things shall be done. What I feel now putting the DNS abuse in the MUST category regarding transfers, my gut feeling is saying that we're going for too much and we'll most likely end up in a huge debate about one policy, inter-registrar Transfer Policy is more restrictive purely in one particular situation. But the other policies connected to the contracted parties in DNS abuse mitigation is not that restrictive. I think we will solve the problem with having this in the MAY category. I think

the good registrars are doing all the best. The registry operators, they are not in fact in the transfer stuff, but they are also doing the best. So, congrats to all the work that has been done in that area. So thank you very much.

ROGER CARNEY: Thanks, Steinar. Crystal, please go ahead.

CRYSTAL ONDO: Thanks. Crystal Ondo, Google. I 100% agree with Steinar. One thing that I think we're overlooking here is that sometimes transferring out is what is in the best interest of securing the Internet. A lot of times, especially when you're dealing with botnets, we get requests to transfer domains to the registrar of last resort. There are also instances where huge phishing scams or other takeover scams are similarly requested to make that transfer happen. So I think making this a must just ignores those cases. Again, to Steinar's point, this is not where we have these discussions. There are other places when we can talk about how we handle DNS abuse, but this policy should not be where that happens.

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

ZAK MUSCOVITCH: Thanks, Roger. Yeah, those are good points by Crystal and Steinar. I have a question for Mike, just try to see if there's a way

of resolving, notwithstanding the other points. Or it's just me. Mike, my sense is that registrars if they really, truly, unequivocally knew that there was DNS security threat going on that they would transfer out the domain name subject to the considerations like Crystal mentioned. Sorry, I got the exact opposite. They would refuse to transfer the domain name as subject to considerations that Crystal mentioned, if they unequivocally knew. What I think registrars are concerned about is that if they do not believe that there's been a proper complaint or if there is insufficient evidence made and they refused to allow the transfer out, would they become liable for a breach of the Transfer Policy or at least responsible for breach of the Transfer Policy? So my question, Mike, is what can be done to satisfy registrars that if they act in good faith and they make a decision one way or the other that someone's not going to say you're breaching the Transfer Policy, because it turns out that it was a DNS security threat, even though that may not have been sufficient evidence in your view? It seems that it puts registrars in this tough spot of forcing them to either stop the transfer and be liable to their registrant customer or allow the transfer and be liable for the breach of the Transfer Policy vis-à-vis the complainant.

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

MIKE RODENBAUGH: Well, I guess the easy answer there is that—what's the easy answer there? Sorry. I just lost my train of thought. There's no easy answers to this. I don't pretend that there is. But I think the

way to fix it is by clear definitions. If something is a DNS security threat or it's not, I don't think that it's realistic to think that someone who's a DNS security threat is going to sue their registrar for in fact complying with the policy. And I don't think that making it a MAY or MUST helps or alleviates that potential liability in any way.

ROGER CARNEY: Okay. Thanks, Mike. Any other comments, questions, concerns here? Thanks, Mike, for bringing this up because I think it really touches on the fact of the need for this to be in our policy. Again, we're talking about if it's a MAY or MUST, but to me, the win here was actually getting it in the policy so that's it's actually usable. I understand Mike wanting it to be a MUST when it's clear. When this one was brought up, I kind of thought the same thing about Zak. It's like, okay, so if a registrar doesn't think it's clear and then moves it or allows it, then what's the responsibility? I don't know. It's one of those hard things. Again, Mike, like you said, it's not an easy topic to solve. I think the key here is it's a great win that we got this language in here and that we agree that the language makes sense. If it's a MAY or MUST, again, I think it's up to the group. But having it here and being able to use it I think is a huge win for our policy update. Zak, please go ahead.

ZAK MUSCOVITCH: Thanks, Roger. Okay. One last stab at seeing if there's a way of bridging the gap before I get back. How about this? How about a registrar must refuse the transfer if the registrar satisfied that an active DNS security threat exists? I'll repeat one more time. A

registrar must refuse the transferring—just reword it—but the registrar must refuse the transfer if the registrar is satisfied that an active DNS security threat exits. So it's a must but only if the registrar is satisfied. It works for both sides of the equation.

ROGER CARNEY: Okay. Thanks, Zak. And you're saying leave what we have on the screen here as a MAY, but you're making a suggestion of adding a MUST in the MUST list.

ZAK MUSCOVITCH: Just to be more clear, the highlighted portion on the screen, I would say evidence of fraud. The registrar may refuse the transfer for evidence of fraud. Then I would say the registrar must refuse the transfer if the registrar is satisfied that the domain name presents an active DNS security threat.

ROGER CARNEY: So you are suggesting the change that this is no longer a registrar discretion.

ZAK MUSCOVITCH: No. It's a word game, really, because I'm saying the registrar must refuse the transfer but only if it is satisfied. So there's where the discretion exists. In other words, it pushes this into the MUST category but it still is within the realm of the registrar's discretion because the registrar must be satisfied.

ROGER CARNEY: Okay. Thanks for clarifying, Zak. Catherine, please go ahead.

CATHERINE MERDINGER: Thanks. My concern with that is if I'm a bad registrar, I'm just never going to be satisfied. Oh, sorry. Well, I didn't think that met my standard. So it doesn't prevent that. If I know something is a botnet security threat, now I can't transfer it to say [RALER] or a different registrar that's doing something similar where we want to sequester those names. I'm prohibited from doing that because I know that it is a security threat. So I think we've heard from a few people that they're not satisfied with this being a MAY, but I think we've overwhelmingly heard from everyone else that it needs to be. I'm not sure what we get out of continuing this conversation. Thanks.

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

VOLKER GREIMANN: I absolutely agree with Catherine. This is better if it's a MAY or a MUST. I also agree with the previous comment that there should probably be some discretion for the registrar to make that determination. So the gold standard of making the determination should be what the registrar believes or has determined in its investigation of the domain name previously. So basically, we are looking at giving the registrar a tool here that did not exist in the past to deny transfer, but I don't think we should make that an obligation. We're not here to police bad registrars. We are here to enable registrars that feel that they have a moral obligation to

prevent certain behavior to cease existing to stop that, and if we have a MAY paragraph here, then we actually also allow those cases where domain name is better transferred, for example, to the registrar of last resort or similar organizations.

ROGER CARNEY: Great. Thanks, Volker. Any other comments on this? Okay. So I think, to move forward on it, again, I'll just reiterate what I said before is I think this is a huge step in adding this language into the Transfer Policy. It gives a lot more meat to be able to handle any DNS abuses. So I think it's great that it's in here. A MUST or MAY, to me right now, I agree, I think that we're talking about the MAY here. The MUST is a higher level. I suggest that Mike, and whoever else wants to, maybe put a suggestion on list. I think, to me, this makes sense here and I'm hearing the group say it makes sense in here. Mike is looking for a higher threshold of evidence and action. So I would suggest maybe Mike puts that on list, and then we can talk about that.

The other thing—and I don't know if Owen is up to this or not—but the other thing is we know that there's ongoing discussions—and maybe I don't know that it's ongoing or if it has started yet and Owen could probably clarify—about adding in contractual language on DNS abuse. So I think that we may get some of that and we may have to review again. I assume we're going to review this once that contractual language comes through because that should be well in advance of us moving this policy through. Owen, please go ahead. Sorry, I missed your hand.

OWEN SMIGELSKI: That's okay, Roger. Since you summoned to me regarding DNS abuse negotiations, I can't give any particular things because these are still internal Registrar Stakeholder Group discussions. However, I might be able to be coy and say I can provide an update later today.

ROGER CARNEY: Okay, great. Thanks, Owen. I think Mike brought up a great point. Obviously, everyone's looking at abuse. To me, it's great that we get a win that we got this carved in here. Obviously, it couldn't be better. If Mike had some good language that he can suggest for a MUST, I think let's put it on list and see how that works out. To me, I think we're going to leave this here because it does add in functionality that didn't exist before and it will help on the DNS abuse side.

Okay. Let's jump into our agenda four. I think Caitlin was going to walk us through some of this.

CAITLIN TUBERGEN: Thanks, Roger. This is Caitlin Tubergen from ICANN Org for the record. The rest of the agenda is devoted to going through the comments that we've received that are not specifically tied to a policy recommendation. So we're going to start here. This is about additional topics or proposals for the working group to consider. As with all of our public comment review tools, we expected everybody to have read all of these comments in their entirety before we begin this discussion. But for the sake of the discussion, we'll bring up each comment. I propose to do so in

small groups just to get through them, and then I'll pass it back over to Roger to see if anyone has any further comments or thinks the idea or comment needs to be considered further.

So to begin with the additional comments, the first three comments include number one, and this commenter is suggesting that there should be an introduction to limit the amount of times that a domain name can be transferred and a new rule about that.

The second comment is about a TAC being provided in bulk. So if a registrant wants to bulk transfer their names from one registrar to another or has more than one name, there should be a bulk TAC for that purpose, noting that a bulk talk were to be introduced, that there should be enhanced security around that, and this commenter is suggesting two-factor authentication could be something to consider.

Then the last comment in this group is kind of a three-part comment. The first is that a domain name transfer should be allowed free of charge and implement some sort of domain push to the new registrar. The second comment from this commenter is about allowing a specific expiration date or allowing the registrar to choose that expiration date. So, for example, if the registrant wants to renew it for six months or five months, that should be allowed, and the commenter is arguing that it should be allowed. I presume their names all expire on the same date for easier management for the registrant. And lastly, at the end of Comment 3, there's a suggestion of an enhanced security, is that when a domain name transfer is requested, the losing registrar enables a webcam to take a picture of whoever is requesting that transfer,

and also verifying users with a government-issued ID to enhance the security of that transfer.

So, Roger, if anyone has any comments on those first three comments, I will turn it back over to you.

ROGER CARNEY: Great. Thanks, Caitlin. On the first one, it just doesn't seem to make sense for something that can be around for multiple decades to limit the number of transfers. To me anyway, I don't know if anyone else has thoughts on if that's good or not. To me, it just seems like it's restrictive, not productive, I guess. Owen, please go ahead.

OWEN SMIGELSKI: Thanks, Roger. Are we addressing these one at a time? Or can we go for number one—

ROGER CARNEY: No. I think that's why Caitlin put them as a group so we can talk about all three of them.

OWEN SMIGELSKI: Sure. I agree that we should not control how many times a customer can transfer a domain name in a lifetime. Like I said, people have a domain name registered for years. I registered my personal domain name in the year 2000 and I've transferred it a number of times. If I find a registrar that I like or get a good deal, there shouldn't be any reason not to limit me from doing it. I don't

know what the concern or the risk is there, what problem it's solving.

As for the bulk TAC, I can understand the benefit that might be helpful for somebody who has a large portfolio. Somebody's got a thousand domain names that they want to transfer, trying to get an individual TAC for each one is a lot of work. I've done some volume transfers myself and it's a pain in the butt. However, if we make a multi-domain TAC, that makes it a lot easier for somebody to then hijack an entire portfolio. I think that's a big security risk, especially for domainers and others who have large portfolios, corporations as well too. I think that's just an unnecessary risk.

As for webcam verification, I don't think we should really be solutioning how we do verification here because while that might be one option to do today, five years from now, when we all wave our hands and magically send DNA or whatever type of method of verification we have in the future, we'd still be stuck in that old way. For now, registrars are still required to provide ICANN with fax numbers for contractual purposes even though nobody has really a fax machine in the last decade or so. So I think it's a bad idea to tie it to a very specific technology like that. Thanks.

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

THEO GEURTS: Thanks. Limits on how many times a transfer is done in the lifetime of a domain name, that's going to be a operational issue for certain resellers, registrants, and it doesn't add anything to the

security of the domain name or to the transfer process itself, so I'm not in favor of that.

Talking about a TAC, I think Owen covered a lot there, but I would suggest that we move this discussion to a the later phase when we are going to talk about bulk transfers in a broader setting so that's maybe a suggestion to have the discussion there.

On the screenshot or a webcam, taking a picture, I think we're going to hit GDPR issues really, really quick. Can you scroll down a little bit on what the other comment was? We have based on the 2FA, we already got it covered. NIS2 will be in effect at some point so everybody will require 2FA anyways.

Setting the Renew for like six months or shorter periods like one month, I actually like that. However, we do that in the Netherlands for .nl. We see a lot of issues now, let me put it diplomatically. I mean, people transfer the domain name, they are under the complete impression that they transferred it for a year, but they selected a month, and then the domain name expires, and then all hell breaks loose. I don't like that solution from an operational point of view where the registrant actually forgets a lot of things there. Thanks.

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

VOLKER GREIMANN: The first point, I absolutely agree that this would be problematic, simply because it would also decrease the value of a domain

name. If a domain name has maybe 10 charges left, it may not be as valuable as a domain name that has 30 charges left and domain names exist for quite a long time in some cases, some, I think, approaching or have reached 30 years by now. If we only had 10 lifetime transfers, that would lock in a registrant at some point in his career to a registrar that he might feel is no longer up to the standards of the times and would like to go to a registrar that is more up to the challenges of modern times. So I think having a domain name that becomes more static over time, I think, is a big problem and it will increase stickiness to the detriment of the registrant. I don't think there's any benefit to that.

Bulk transfers, everything has been set to that. I would also like to say something about the registration fees suggestion or renewal fees suggestion. I don't think as part of our Transfer Working Group, the fee structure and renewal structure of a domain name is even up in our scope and that should end the discussion right there. But I think also it would drastically change the expectations of a registrant. It would increase the risk for the registrant. If you, for example, transfer a domain name without renewal that is quite short before expiration and the domain was transferred in maybe five minutes before it expires, so that they never have a chance to renew and it expires based on that. I think it would generate a very bad user experience and I would hesitate to change anything with renewal in this PDP, at least. I don't see a reason for that. Thank you.

ROGER CARNEY: Great. Thanks, Volker. I'm not sure what problem one is trying to solve. I think that our 30-day lock solves, to me, the possible issue

of frequent transfers to avoid identification or whatever it is. I'm not sure that an overall transfer thing is solving a specific problem.

I think that on these three—and as Theo mentioned, two kind of leads us into some discussions that we have earmarked later on. But I think we have some good input that we can respond to these. Caitlin, if you take us through the next section of comments, please.

CAITLIN TUBERGEN: Thanks, Roger. So the next three comments, the first is from the Non-Commercial Stakeholder Group. This comment raises concerns about transfer fees and noting that this has a restrictive effect on non-commercial users, there should be some recommendation about restricting high transfer fees, inter-registrar transfer fees. There's also a note here about sanctions, and noting that even if the group decides that these topics are out of scope, if they could document it as such in the rationale of its report, the NCSG would welcome that.

The next comment is also by an individual about a registrar and post transfer fee away should be restricted. Comment 6 is from the At-Large Advisory Committee. And this comment is noting that specific language should be added into the Transfer Policy to make clear that registrars are responsible in regards to the updated implementation or updated Transfer Policy requirements vis-à-vis the resellers, noting that although ICANN doesn't have a direct contractual relationship with resellers, registrars do, and that there should be some sort of explicit language that there needs to

be some acknowledgement that registrars will ensure their resellers are in compliance with the Transfer Policy.

Just as a note, for those who may not have been on the call on Tuesday, the group did discuss at least Comment 4, which is a repeat of a comment that we discussed in relation to the fees and sanctions. Staff does have an action item to draft language about a rationale as to why the group did not believe that it was appropriate for it to weigh in in terms of the Transfer Policy on any sort of fees for sanctions. So I just wanted to remind everyone of that if you hadn't been on the call, but I'm going to pass it over Roger in case anyone has any additional thoughts, comments about fees and/or the comments about reseller's activity. Thank you.

ROGER CARNEY: Great. Thanks, Caitlin. I appreciate that the NCSG brings this up. Not that we can solve it here or that we're going to try to solve it here. I think that it's definitely an education that the registrant should have that. Hopefully, our language and our policy is clear enough to recognize that they don't have to pay those fees to have their domain transferred. It's very clear that the transfer has to go through for any forward-looking fees. Theo, please go ahead.

THEO GEURTS: Sanctions—go back to the transcript of Tuesday, all covered there. When it comes to the reseller part, I'm not against it but I would like to point out that every wholesaler registrar has

contractual obligations that any ICANN policy will also be applicable to the reseller. It's not like these resellers, while they do not have a contract with ICANN, they are certainly responsible that those policies of ICANN are carried out correctly. If that weren't the case, it would be a total Reddit conversation. I mean, come on, that would be total chaos. Again, I don't mind it but I don't think it's necessary. And on the renewal fees, I don't have any comment. Thanks.

ROGER CARNEY: Great. Thanks, Theo. I agree on the registrar part of that. I think it's in our contract that the registrar is responsible for the reseller. So I don't know that we have to say anything additional. Obviously, all policies are enforced all the way down. Thanks, Crystal. Volker, please go ahead.

VOLKER GREIMANN: Crystal just typed into the chat what I wanted to say as well. It's already the obligation of the registrar to pass on all obligations to the reseller. So maybe ALAC should reread the contract that we have in place before they comment. That being said, I think there is some consideration to be had with regard to that responsibility because a registrar cannot act upon something he doesn't know. So if, for example, a transfer request is directed as a reseller, it should not necessarily be counted against the five days that the registrar has to respond and provide the Auth-Code. There's some complications in there and I think that's better handled in a separate policy that's not necessarily due to the Transfer Policy because ultimately the inter-business interaction between the

registrar and the reseller applies to so many other policies than just the Transfer Policy. If that has been looked at, then it should probably be looked at on a grander scale, not just on the Transfer Policy bit. Thank you.

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

STEINAR GRØTTERØD: This time in my only At-Large hat on. When we discuss this and the way we put it in the wording and our intention here is to get some sort of understanding that the clear obligation, even though we do know this in the Registrar Agreements, etc., but a kind of a clear understanding to put all the elements that we have discussed in this working group for the new policy into the line of the resellers and make sure that these are being understood correctly. We don't necessarily want to have clear wording saying that the registrars has to put this forward and prove that they put this forward. It's just underlying the pure fact that we are operating in a market where we have registrars, we have resellers. There's not the simple model of registry/registrars, etc. That was the intention. The thing is that the registrar members of this group, you are the good guys, you know exactly what to do. But there are elements in this world that might be needed to put some things in blocked letters. Hopefully that is something that I will survive next time we meet face to face. Thank you.

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

VOLKER GREIMANN: With regard to the fees, I'm a bit on the fence here. On the one hand, I don't think we should regulate fees and what fees can be charged and can't be charged, because for some registrars, I know that transfers or provision of Auth-Codes can even be a manual process simply because they're not automated as much as other registrars, and therefore, they wants to be paid for their trouble. Other registrars have certain security precautions where they check various authorizations, which is manual work, all to the benefit of the domain name of the registrant to secure it more. That's an optional service that is charged as part of the transfer out process. So I can see why registrars would want to have the ability to charge for transfer out, and that would also apply for the resellers, obviously. However, on the other hand, we've also seen cases where small registrars tried to basically chain their registrants to them with ridiculously high fees. That kind of market practice, I think, is to the detriment of the registrant and there should be something said against that. Again, that's probably something to be addressed more on the field of business practices in general, not just transfers. However, I see the argument here and I see that there is a case to be made, but I'm not sure if it needs to be made now. Thank you.

ROGER CARNEY: Great. Thank you, Volker. Owen, please go ahead.

OWEN SMIGELSKI: Thanks, Roger. Like Volker, I'm not 100% for it and also not 100% against it. I can see some scenarios where that may be there. I want a scenario that happens quite a bit with some registrars and a lot with resellers is, that there's a contract or something to do web design services or something along those lines. Then two months later, the person wants to transfer out. Then a lot of time and effort was involved to getting stuff in advance in there and they're counting on that being there as a reoccurring revenue stream for a while. And so losing that domain name is actually going to hit the bottom line. So I don't want to keep playing with all sorts of different scenarios but I don't want to preclude that.

Also, another concern is ICANN really doesn't anywhere else set what types of fees or charges can be done. Yes, I know it's done to a degree. In Registry Agreements, for some TLDs, there are price caps but not all of them. This would be a really big departure for ICANN community to start saying, "You can or cannot do prices here or there or whatever." I saw Mike's suggestion in chat that needs to be prominently displayed. I know there are some requirements in the ERRP, which is the—oh boy, I don't even recall what that acronym stands for. But it does make some requirements that renewal and redemption fees must be prominently displayed in the Registration Agreement. Then there are some other web hosting obligations for those as well, too. So that can be something where we might want to make that requirement where it's visible in advance conspicuously prior to entering into the agreement so that it's not a sudden surprise later on down the road when somebody wants to transfer and suddenly they're hit with a fee.

I would also like to note that transfer fees are not a reason to deny a transfer. In fact, I know that ICANN has pushed back to registrars who said that a transfer fee must be paid prior to authorizing a transfer. The transfer fee can always be done and then they can argue about the transfer fee after the fact. It's not as much of a concern because while it may be onerous, it's not something that's going to block the transfer. Thanks.

ROGER CARNEY: Great. Thanks, Owen. Mike, please go ahead.

MIKE RODENBAUGH: Sure, thanks. I guess, that's nice. Owen and I are agreeing on something that maybe we could do something here for registrants and at least make registrars prominently disclose transfer out fees rather than bury them in Terms of Service. That happens today. And people get surprised when they try to transfer out and they realize there's a fee for that that they must have agreed to 10 years ago because it was buried in TOS. So I think that that's a strong idea that we should look to the Renewal Policy and use the same sort of language here around transfer out fees.

ROGER CARNEY: Great. Thanks, Mike. Any other comments on this? Okay. I think we can continue on. Volker, you have your hand up. Please, go ahead.

VOLKER GREIMANN: Just one thing, if the fees have to be disclosed at the time of registration, could for a very long term Registration Agreement—say the registrant wants to transfer out after 10 or 20 years, that would prohibit the registrar from increasing those fees based on inflation, for example, the costs that he has with performing the transfer process, the Auth-Code provision and everything that is included in that. I'm assuming a legitimate fee here. Then he has higher staff costs and whatnot and would not be able to pass those on. So that might be disadvantaged, so we would have to have some kind of leeway to increase those fees down the road.

ROGER CARNEY: Great. Thanks, Volker. Okay. Caitlin, if you can take us through the next section.

CAITLIN TUBERGEN: Thanks, Roger. Moving on, you'll notice that Comment 7 is quite lengthy. This has to deal with record keeping, and it's actually a comment from our ICANN or colleagues. Unfortunately, Holida, our liaison to the Contractual Compliance Team had to leave the call early. So if you don't mind, I'd like her to speak to this comment when she's able. So perhaps we can table this one until next week, because I think she wanted to provide some further color on this one.

Moving to Comment 8, this was a comment provided by GoDaddy. The comment is in reference to privacy/proxy, noting that privacy/proxy issues should be considered holistically and it's not an issue that the Transfer Policy Review Working Group should

be resolving as it's not in scope. And here, the commenter is suggesting that the use of registered name holder is the appropriate mechanism.

The next comment from Newfold Digital is about the transfer dispute process. As we know, I believe that's an issue that will be further considered in Phase 2. However, this commenter is noting that the further discussion on transfer dispute should be aligned with all of the recommendations in Phase 1A, that they're a bit interdependent, in other words. I'll turn it back over to you, Roger, if anyone has comments on privacy/proxy or how the TDRP relates to Phase 1A recommendations.

ROGER CARNEY: Great. Thanks, Caitlin. I would say I think that #8, we went through with some earlier comments that wanted to change the privacy/proxy. So I think that 8 may have already been handled in our individual discussions or recommendations.

For 9, I think that we've all stumbled on this and that we recognize that Phase 2 has considerable impacts on the Phase 1 stuff and we're already working on ways to accommodate that. But any comments on 8 and 9, from anyone?

Mike, to your point in chat, no, we left that. As we have, we're not going to pull it out into this transfer discussion right now. Unless someone gets some good traction on this, I don't think that there's anything that we can do right now to address—I don't know how you would say it—other fees. I think that it was clear that other

fees are not in jurisdiction for ICANN or anyone else. Mike, please go ahead.

MIKE RODENBAUGH: Again, we're not talking about whether or not the registrar can charge a fee, just how prominently it needs to be disclosed, which I think is within scope of ICANN's remit and this group. And I didn't really hear any opposition. I heard agreement from Owen that transfer out fees, for example, could be required to be permanently disclosed in a DN RA rather than buried in text. I thought we had look to the example of renewal fees. We already have a policy on that. Why can we not impose the same policy on these sorts of fees, which today are hidden and do cause problems for people in the real world?

ROGER CARNEY: Great. Thanks, Mike. I guess my point on that was we don't have any language to address that and we didn't have any language to address that. That was my point on it. I don't know if Theo's hand was up but he put it down. There's nothing suggested on our initial report about it. If we missed it, we missed it. We talked about fees and sanctions a year ago and we moved past that. But if someone wants to bring that up, I think that it's important to be bringing it up when we were talking about it, not after the initial report goes out and it doesn't show up. How that happens? I think that that's something that could be presented to the group and see what their thoughts are on it. But again, we have nothing to look at right now. Caitlin, if you want to take us through the next section.

CAITLIN TUBERGEN: Thanks, Roger. The next comment is from SSAC. SSAC is re-highlighting a comment that it made in SAC119, specifically feedback that was provided to this group. Mainly, a registrant's domain name is at risk of experiencing a discontinuity of DNS resolution, and when DNSSEC is in use, a discontinuity of validation during a registration transfer if the transfer of DNS services is not considered during the process. So the SSAC is requesting that if the working group has determined or will determine that this particular risk that they noted is not in scope, then they're requesting that a rationale and description be included in the final report just to have that on record.

The next comments are quite detailed and refer back to a comment that was received from Leap of Faith Financial Services. I'll touch on these briefly. But as noted previously, I hope that everyone read all of these in their entirety earlier. The first was about an X-prize style competition to improve domain name transfer security. In other words, allowing people to submit creative solutioning and seeing what comes back possibly from folks that are not as intimately involved as this working group and allowing some outsiders that might have some good ideas. The breakthrough proposal of generating a domain name transfer transaction ID at the gaining registrar to input at the losing registrar. I believe a representative presented this idea or proposal in detail at the last ICANN meeting, but feel free to correct me if I'm wrong on that.

The third comment here, I believe we discussed at one of our last recent meetings and that was about retaining the losing FOA and

making it an ACK to the transfer rather than NACK only or a passive losing FOA. I believe the group has discussed that. And again, for some who may not have been attending the last couple of calls, the proposal on the table is to put the losing FOA back into the process, but have the NACK model, basically status quo from today.

The next comment is about improving the losing FOA by making visible the before and after WHOIS information. Next, embedding the gaining registrar into the Transfer Authorization Code. And lastly, here, a time lock access for the TAC generator, aka vacation mode or lockdown mode. I think that was also discussed during our last meeting.

Then lastly, here, the same comment where Leap of Faith noted that the report really needs an impact analysis. There needs to be a systematic review of potential attack scenarios to make how ineffective these recommendations are in securing against potential attack scenarios. I think that is all.

Again, the Comments 10 through 12, we have the SSAC proposal, and then we have the comments from Leap of Faith. So I will turn it back over to Roger for those who have comments on these. Thank you.

ROGER CARNEY: Great, thanks, Caitlin. I'll open it up to the floor. I know that we talked through the SSAC stuff on DNSSEC. Steve actually sat in and talked to us about that. We did come to that determination that this was out of scope for the Transfer Working Group. It's

beyond the name and talking about the transferring of DNS information along with it. So I think that we determined that it was out of scope, DNSSEC specifically. I don't know if anybody has comments outside of that. Okay. Staff can correct me, I think we have rationale to explain why we feel that it's out of scope for that. So I think we're good on 10.

As far as 11 and 12, the idea of making this a call out asking for ideas on it. One of the things I'll say is I did bring this up in our TechOps meeting at ICANN75, if I'm right, and put this out on the table for the TechOps group to look at this. The same idea of not just looking at the Transfer Policy and improving it, but tipping it upside down and looking at it from a new and different perspective. I did present that at the TechOps and I don't know if TechOps is actually going to pick up on any of that. Again, I think that a lot of the updates to our current policy were driven from the TechOps' ideas. Maybe not finalized, but some of the high level ideas. I thought that was appropriate to take to that group and see if we shook it up as Leap of Faith suggested. Looking at it from a reverse view of moving it from the losing to the gaining, I don't know where that's going to go, but it's something that was presented.

For 12, specifically, there is a small group that did take a look at threat vectors and they are working on providing a write-up for us. Thanks, Jothan. Any other comments on these items here, 10, 11, 12? Keiron, please go ahead.

KEIRON TOBIN: Thank you. In regards to 12, I think we need to iron out quite a few more details first. But I'm definitely not against pen testing. Hopefully, we can catch everything in the round of comments, that people believe that there are potential issues. I have lots of faith in the TechOps group and Jothan and the team. I'm not completely against that but I just think we need to iron out a couple more issues first. Thank you.

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

THEO GEURTS: How does this work from a process point of view? Let's assume TechOps goes like, "Okay, this is a good idea to analyze." And at a certain point, after much debate there, the proposal is being flagged as a possible solution with many benefits. How do we go about that if it comes back to the group and the breakthrough proposal is dissolution to do transfers that way? How are we going to toss away everything that we have? I'm just looking for the process here.

ROGER CARNEY: Thanks, Theo. Like everything else, the TechOps group took several years to come up with the last whitepaper they wrote on transfers. I think that this would probably even take longer, because it's again a greenfield kind of thing where they're looking at it from a different perspective. So I don't expect any of the TechOps stuff to impact this group. It would probably impact the next review. If TechOps two years from now said, "Hey, we've

come up with a great new understanding," then they're going to have to work that through Council and everything else to get it that way, it's not going to affect the work of this group.

I think we're good on these. We're six minutes from time. I don't know, Caitlin, if you wanted to introduce anything else or if we're in a good stopping point here.

CAITLIN TUBERGEN: Thanks, Roger. I think there were two comments received on the charter questions. I can quickly touch on those, if we all don't mind.

ROGER CARNEY: That sounds good. Thank you.

CAITLIN TUBERGEN: These two comments both housed in the same box. The first, I believe, we did already discuss in previous discussions. But specifically, the commenter here is noting that the term lock, particularly in the UDRP rules, should be made more precise. Specifically, the registrant should be able to update its name servers during the UDRP. That was the concern there.

The second one was the swim lane seems to incorrectly state that the TAC is securely stored by the registry, but it's actually the hash of the TAC that is securely stored, not the TAC. So if there aren't any disagreements with the second comment, staff can make that update. Of course, if folks want to digest that a little bit

longer, we can come back to it on the next meeting. But I did want to quickly bring up the definition for a lock under the UDRP rules, which states that lock means a set of measures that a registrar applies to a domain name, which prevents at a minimum any modification to the registrant and registrar information by the respondent but does not affect the resolution of the domain name or the renewal of the domain name.

So registrars might implement this differently and I believe we did discuss this. However, I think the conclusion the group came to earlier is that definitions within another policy aren't really within the scope of this group's work. Therefore, we would flag it to RPM Phase 2, who will be dealing with the UDRP. But I just wanted to flag that we did receive a comment on this. And if anyone had any questions, concerns, or further insight on this, we obviously would welcome it. Turn it back to you, Roger.

ROGER CARNEY: Awesome. Thanks, Caitlin. Owen, please go ahead.

OWEN SMIGELSKI: Thanks, Roger. I agree with Caitlin on both points there. It's not within our scope to change other policies like the UDRP rules. I also agree with it that I think it's a plain meaning under the UDRP rules that name servers can indeed be changed. The registrars are not allowed to impact the resolution of the domain name during the pendency of the UDRP. The caveat, if a, say, WHOIS inaccuracy complaint or an abuse complaint comes in, there's actual abuse, the domain can be suspended, that can override

that, because we don't want to allow those things to continue. But the registrant can certainly change the name servers if they want to go to different hosts or something like that. I don't think that lack of concern is something that we really need to address. Thanks.

ROGER CARNEY: Great. Thanks, Owen. Keiron, please go ahead.

KEIRON TOBIN: Sorry. Owen stole my words. Thanks.

ROGER CARNEY: Great. Thanks, Keiron. I think that on the first part here—I guess, to me, that's the easier one. I suppose I'll leave it to the team to think about the wording in the last spot here. Should it be changed to the hash of the TAC or is TAC securely stored? Again, it'd be good if Jim was here and he could do his security speech for us. To me, the TAC securely stored hashing is just one feature of securely storing it. But I can understand the slight difference here. Rick, please go ahead.

RICK WILHELM: Thanks, Roger. I think that's a difference without a distinction. And I also think that it also over specifies. Because in the future, the mechanism for that secure storing may be something different than hashing as technology evolves. So I think that securely stored by whatever means necessary, as the saying goes, is a

better way to state it and not over specify it in the policy. Thank you.

ROGER CARNEY: Thanks, Rick. I think that's a good explanation of it, is not trying to get too specific because of the potential and the likelihood of it changing in the future.

Okay. Thanks, Caitlin, for taking us through this because that was quick. We have one minute left. Anything anyone wants to add? Okay. We will pick up on Tuesday with continuing to review these other comments here. Everyone, have a great week. We'll see everyone Tuesday. Thanks. Bye.

[END OF TRANSCRIPTION]