ICANN Transcription

Transfer Policy Review PDP WG

Tuesday, 04 January 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/aYHOCg

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

JULIE BISLAND: Good morning, good afternoon, good evening, everyone. Welcome to the Transfer Policy Review PDP Working Group call taking place on Tuesday the 4th of January 2022.

In the interest of time, there'll be no roll call. Attendance will be taken by the Zoom room. For today's call, we have apologies from Barbara Knight (RySG) and Owen Smigelski (RrSG). They have formally assigned Beth Bacon (RySG) and Essie Musailov (RrSG) as their alternates for this call and for remaining days of absence.

As a reminder, an alternate assignment must be formalized by way of a Google assignment form. The link is available in all meeting invite e-mails. All members and alternates will be promoted to panelists. Observers will remain as an attendee and will have access to view chat only. As a reminder, when using the chat feature, please select everyone in order for all participants to see your chat and so it’s captured in the recording. Alternates not replacing a member should not engage in the chat or use any of the other Zoom Room functionalities.

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

KRISTIAN ØRMEN: Thank you. I've updated my SOI earlier today to reflect that I'm going to change job in May and I'm going to change to ccNSO instead. So just wanted to be fully open. I'm going to continue in this group until RrSG replaces me, and I'm not sure when that will happen at the moment. Thank you.

JULIE BISLAND: Wonderful. Thank you so much, Kristian. All right, if you need assistance updating your Statements of Interest, please e-mail the GNSO secretariat.

Please remember to state your name before speaking for the transcription. Recordings will be posted on the public wiki space shortly after the end of the call. And as a reminder, those who take part in the ICANN multistakeholder process are to comply with the expected standards of behavior. Thank you. Over to our chair, Roger Carney. Please begin.

ROGER CARNEY: Thanks, Julie. Welcome back, everybody. To me, it seems like it's been longer than just one week off, but happy new year to everyone. The one-week reprieve hopefully allowed everybody to do some fun things that they were looking forward to. As far as any updates, I think we don't have any right now. The only thing I would do is ask any stakeholder groups that may have had some discussions. Again, I know a lot of people took a break. But if there were any discussions or any continued discussions from prior that any stakeholder groups want to bring forward to talk about, I'll give time for that now. So if anybody has anything they want to bring up from any stakeholder group discussions, or any other things that happened that they want to bring up, please bring forward now.

Okay, great, hopefully that means everybody did have some time to themselves and to their family. So All right, so let's go ahead and jump into the second readings and jump into the TAC document and continue our review of the recommendations that we have been reviewing the past few weeks. So let's go ahead and jump into the TAC document.

So, again, I don't think there's much to cover on the first few recommendations. Just a reminder that on recommendation three, we were looking for some maybe different wording here. I think the intent here is probably nothing that we want to change, just maybe wording to make it more clear on this the security mechanisms of the TAC. So again, we talked about this quite a few weeks ago now but this is still an open item that we're looking for as when we reviewed it the first time, there were some concerns about the current language and that we can make it better. So again, take a look at this and provide any comments or suggestions on this field. Theo, please go ahead.

THEO GEURTS: Yeah, thanks, Roger, and hello, everybody. I went through this recommendation with our technical people. And one of our technical people said, why don't you guys go for a standard? And my question to him was like, why would we do that? And his fear is as follows. He is a little bit afraid that every registry will come up with their own requirements. So VeriSign will have a different minimum length than Donuts.

And that is a little bit problematic nowadays, because we got over 1200 TLDs. And to make sure that you can set a TAC in the correct way, before triggering all kinds of error messages with the registry, I suspect that most of us have some kind of validator, I call it a validator. It's not a technical standard term, but in the Registries Stakeholder Group or as a registrar, basically, before a TAC is created, we make sure that it is done, it is validated, matching the requirements of the registry. We do that now already with ccTLDs and the current gTLDs. And doing that is quite a lot of work for some of us. I suspect that if you have to change all these requirements within your back end, you might be in a situation, we are not in a situation, but there might be some of us who have to change the requirements 1200 times.

And that is okay. I mean, there's a policy change, and we are trying to improve the entire process. The problem becomes a little bit annoying when all these TLDs switch around to backends every time. And that happens more often than I'm happy with. I mean, there's one TLD, that has been changed technical registry backends four times now. And that means that every time we have to update them to new requirements set by that registry, and that is basically a lot of work. And that is not something we envisioned years ago. At least I never had the idea that TLDs would move around so much. I mean, they used to be very, very static all the time. And that is no longer the case. I mean, these things move around quite a lot. So I have somewhat of a reservation, if we go with minimum length, I would rather see a standard and the highest standard possible, in my opinion, but at least making sure that it is applicable to all TLDs so we don't have to change that all the time. Thanks.

ROGER CARNEY: Great. Thanks, Theo. Yeah, and you bring up a good point that, obviously, that dynamic has changed over the years. The technical backends being more fluid than they used to be. And it's something obviously, I think that this recommendation is pointing to exactly what you were trying to say and I think like what's going on in chat a little bit here is if you look at it today, basically any TLD can have whatever rule it wants. And the goal here in this recommendation is to set at least bounds on that. And maybe not prescribe exactly. And I think that was the tough part of the wording, is how do you get to wording that is consistent enough across all TLDs. But it's still allowing flexibility of operational things.

And I wonder here if maybe we don't need to get too specific. I mean, we do say based on current technical security standards. Excuse me. I don't know if we need to get more specific or if the

IRT should drive that out. Maybe that's a question for the group. I think a lot of questions came up on the second part of this, where ICANN Org may change these requirements from time to time. And I think there was a lot of discussion. Again, it's been a while. Quite a bit of discussion around, well, that can't just happen when ICANN Org thinks that should happen. That has to be something that appears to be an agreed upon change to go from—air quote here—one standard to another standard.

And again, I think we added some wording here to add in at least sufficient time for that change. But I think that there was concern at the time that the people involved should also be—the contracted parties should be involved in that decision of making that change. So, Beth, please go ahead.

BETH BACON: Thanks, Roger. I just wanted to put kind of a little flag in the sand on this one, that I would love the opportunity to go back to the registries. I'm the only one on the call for the registries today, I apologize for that. But I would like to go back to them and see if there is an operational reason for us to maintain some level of flexibility. So I do like what you were saying, perhaps there's room for like some bounds but maintain good enough flexibility that the registries will be able to still do what they need to do. So I would just love to put a flag there and just say, I'll take this one back to the registries also, if you don't mind.

ROGER CARNEY: Great. Thanks, Beth, that that'd be great, if you could, because yeah, I think the hard part of wording this or even for the IRT would be how restrictive that could or could not be, trying to be consistent but still allow the operational. So thanks, Beth. Berry, please go ahead.

BERRY COBB: Thank you, Roger. Beth, when you take that back to the registries, something to put into context here. And looking at the current wording, or whatever the future wording may be, I think this would become a challenge for the IRT to try to implement this without some more specificity to the recommendation, but still allowing for flexibility. I think Theo makes a very valid point about the lack of consistency here can be quite disruptive.

The other part that I wanted to mention is the aspect here that ICANN Org may change these requirements from time to time, and I believe that there was kind of resistance about hard coding that into the recommendation. So I think this is going to be a challenge to find some balance here. But a consensus policy recommendation can only be changed through an additional PDP. And I don't believe that was the intent, of needing to go through a PDP to change some sort of kind of a more technically focused type of requirement.

And I guess I can understand the resistance about ICANN Org being the one that would be the only entity that would make this change outside of a PDP, to make the change. So I'm not really sure I have a solution here yet. But I do agree that this needs additional work. And, most importantly, the more prescriptive we can be to make it easier for the IRT, the better off we'll be at the same time maintaining some flexibility for future changes without the need to have to launch a PDP to make those changes. I hope that made sense. Thanks.

ROGER CARNEY: Thanks, Berry. And I agree, and thanks to Beth for taking at least that first big part back on what the flexibility needs would be, as I think everybody's saying now is, the more defined we can get, the better this will result and give the IRT a better chance of actually getting something useful put in place. And to Berry's point on the second part, that's what I was remembering as well. The discussion around it was obviously, the technical standards and security changes over time, where some of these other recommendations probably won't change dramatically over time. But we know that security mechanisms change quite a bit in fairly short order. So I think that's what the goal of that second sentence was, was trying to be able to come up with a way to update that without having to do a whole PDP just to update that one recommendation. So, as Berry mentioned, I just think we have to come up with language that is fitting, especially for the IRT to be able to implement it once they get to that spot.

So any other comments, suggestions on this one? Again, this one's been kind of a working one, we haven't seen a lot of discussion on it, but we need to get it cleaned up. And hopefully Beth can provide us, the registries can provide us some information on the first part. But we still need to iron out the second part as a group to come to a way to facilitate, or maybe we had that discussion before, maybe we don't want to allow this to change four or five years from now when security practices change. And if that's what we decide, then we can remove this, but it seemed like a fairly good idea at the time. And that's why it went in here.

Okay, any other comments? So again, take a look at this, come up with any comments, put them in the document, and we can review them as they come in the documents. We do need to update it, again, to provide as much as we can to the IRT and to make sure that if we decide on allowing changes here on an ongoing basis, that everyone's comfortable with that. Keiron, please go ahead.

KEIRON TOBIN: Thank you. Happy new year, everyone. Just in regards to—I'm just looking at this. The aspects of [inaudible] from time to time and response, I'm not sure if we need “from time to time,” it may just be easier to read “ICANN Org may change these requirements in response to new or updated standards.” I don't know how anyone feels about that. I just think it might be a little easier to read. Thank you.

ROGER CARNEY: Thank you, Keiron. And I know “time to time” is in quite a few other documents. So I don't know if that's something that’s a standard or not. But yeah, it does seem to read a little smoother without it. But maybe there's a reason for it. Sarah, you left some suggested wording a couple weeks ago. Okay, can we pull up

Sarah's comment there? Okay, yeah, so I was wondering, Sarah, that comment right below Emily's.

So adding in "in collaboration with the stakeholder groups." So ICANN Org may change these requirements in response to new updated standards in collaboration, or I guess maybe in collaboration with, yeah, probably earlier. Thanks, Sarah. Please go ahead.

SARAH WYLD: Thank you. Hi. Happy new year. Hope everyone's well. I had suggested it actually in the first sentence here after the words ICANN Org. And so I'm not sure that that really solves the problem, but hopefully it helps us get in that direction. Thank you.

ROGER CARNEY: Thanks, Sara.

SARAH WYLD: Oh, sorry. Just to add also, if we are putting that "in collaboration with," I do think it should apply to both mentions of ICANN Org. Yeah. Thank you.

ROGER CARNEY: Okay, I see what you're saying. The very first sentence and then the beginning of the second sentence. Okay.

SARAH WYLD: Yeah, exactly. So ICANN and the registrars and registries will establish the requirements and then will eventually make changes when needed.

ROGER CARNEY: Okay, yeah. You're suggesting that wording after ICANN Org in both sentences, okay. That makes sense. Any thoughts from others on that? That seems to provide that link, especially in the second sentence to that continuous improvement cycle on the second sentence idea. So any thoughts from others? I like the wording, I think it helps. Emily, please go ahead.

EMILY BARABAS: Thanks, Roger. From the staff perspective, I think it might be helpful to have a better or clearer understanding of what collaboration means in this context, to help with the implementation side of things and ensure that it's consistent with the intent of the recommendation. So one thing to consider is exactly what collaboration would mean in that context and include that in the recommendation as applicable. Thanks.

ROGER CARNEY: Great. Emily, thank you. And that may help me think about it a little too, and that when Sarah suggested that into the first ICANN Org, my thought was originally, well, that naturally happens, because during the establishment, ICANN Org and the IRT would establish that minimum. So it's not specifically registry and registrar stakeholder groups, but it is a community through the IRT, that first part on the establish, and the ongoing, I think, that collaboration could be—and again, I don't know if that means there's an IRT to update that standard, if that's what we're suggesting. Berry, please go ahead.

BERRY COBB: Thank you, Roger. I'm kind of going to be pointing to Jody. I know he's listed as an alternate, but maybe he can respond here. I believe he has the most knowledge as it relates to RFCs and what's required from the standards that are set over there. I'm curious if the existing RFCs around AuthInfo codes, if there are any security types of components listed with that RFC. Would it not be better that any changes to the standards on AuthInfo codes, future TACs, be developed there? And we would be able to just point to the RFC instead of Org trying to collaborate with contracting parties about changing the standard.

ROGER CARNEY: Thanks, berry. I'll let Jody talk if he has anything to say here.

JODY KOLKER: I'll have to take a look at the RFCs. I don't know of any standards that are on the RFC for the AuthInfo code. But I'll have to review. I wouldn't bet my job on that quite yet. I'm not sure if it's the best place to have IETF set a standard for that. It might be. And I believe that we have a secure AuthInfo actual RFC out there already that was done by Jim Gould and Rick Wilhelm. Let me take a look at those two things and get back to the list. Thanks.

ROGER CARNEY: Thanks, Jody. I actually forgot about that updated secure AuthInfo one. I think that that was just published. The trick I would say on the RFC—and maybe the secure one helps this out—is the AuthInfo is defined in an EPP RFC that hasn't changed since, I don't know, the early 2000s. And the way the RFC works is you don't actually change an RFC. Unless there's an error in it, that’s the only time you can really change an RFC. You have to create a new one and obsolete the old one. Or you have to create the concept as a separate RFC and may end up getting That's right, maybe the secure AuthInfo one that Jody mentioned may be able to handle that. But we'll let Jody dig into that and get back to the group, if that's a workable direction. I think that that specific change, where that occurs, that's a good idea, Berry, talking about where that may occur. But the recommendation still should have to support that idea. So I think we would still have to have some wording here that allows that. Berry, please go ahead.

BERRY COBB: Thanks. Caitlin, I believe you're sharing the screen. if you can click on Jothan's link to the RFC itself. And as Jothan notes, this is a brand-new RFC. And again, a very quick read, but go to section 4.1. So what I find here is that it is mentioning that it's a secure random value. It's treated as a password length whole number. There's a target entropy with required length, talks about the calculation of the required length. I don't know, by quick read that seems like this has a lot of what we're trying to accomplish here. And I think maybe even a little bit of homework for our contracted party colleagues is, would this provide a path to more consistency at the registry level to basically address what Theo had mentioned that brought this part of the conversation up? Thanks.

ROGER CARNEY: Great, thanks, Berry. And maybe this will even help Beth, when she takes it back to the group. But to Berry's point, I think that everyone should take a look at this. And if it makes sense—and Theo, maybe take a look at it and read through this document as well. You probably already have. Just take another read in the context of this recommendation so that we see if maybe we're able to provide the IRT more specific directions and link to this, or obviously, its successors, something like that. So if the contracted parties and anyone else that wants to read it, wants to take a look at this and see if this helps our discussion around recommendation three, please take a read of this, and we'll touch on it again. Take a read and provide comments in the document if this does or doesn't satisfy or if it's partially there, please let us know and put in comments.

Okay, any other comments on recommendation three? Looks like we've got some good [inaudible] here. Thanks, Sarah, for updating that. And thanks for everybody on the technical side of it. Maybe we do have something that we can be more specific too.

Okay, well, let's go ahead and move down then. I think we didn't have any questions on four. Our last session, in December, we worked on 5.1 and 5.2 considerably. I think we spent most of the time on this one point here. So I think that this is close to what we discussed. I couldn't see anything different. Again, we have some open items here. But especially on the number that we're looking at, and the addition of maybe—I don't know if it's a new recommendation or if it's a recommendation just in this group here. But let's go ahead and go through any comments here. It looks like that first comment on recommendation five is from Theo, needs to be subjected to standard EPP poll messages. Thanks, Theo. Please go ahead.

THEO GEURTS: Actually, I was going to discuss something else. But yeah, if it could be standard EPP poll messages, our developers would love that if we do it that way. Then at least we don't have to go around, fiddle around with all the documentation from all these registries to figure out how they define their EPP pull messages. Thanks.

ROGER CARNEY: Great. Thanks. Did you have something else you wanted to say?

THEO GEURTS: Yeah, in general, I think this recommendation, the notification, I don't see how it is of any value. And 5.2, I still find that the registrar of record must investigate the issue. I think that is going to be exploited. And when I say such things, Roger, do I resonate something with you? Do you get some kind of ideas like how this can be exploited? Or do you just draw a blank there? Am I the only one who can come up with a couple examples here on how you can exploit that?

ROGER CARNEY: Thanks, Theo. I think that, obviously, setting this and making a decision here to force somebody to do something, obviously, there's bad actors out there. And again, you put that hat on, and yeah, a lot of us do that, is try to think of how people can break what seems like such a nice idea and use it to their advantage.

THEO GEURTS: Maybe I should start with a little disclaimer here. When I was doing the ethical hacking certification, I always would get a message or a written warning that whatever I would learn that day would be only for educational purposes. So, examples that I'm going to give here are for educational purposes, you're not supposed to do this stuff for real. But 5.2, I think when we go along down the road, somebody is going to suggest that, okay, if the registrar of record must investigate the issue, it would be better that the registry also informs ICANN Compliance, because then you have something that is accountable, you'll have an accountable process.

I'm not sure if that's going to happen. But if we must investigate the issues, I already see the issue of somebody just going to create an account at registrar A, and then just shoots in a boatload of transfer requests at registrar B and then register B can't investigate them all. And if you have a really nefarious person, maybe a competitor of yours, who decides to spend this weekend to create like 50,000 invalid transfer requests. It's not that hard. You could do that completely under the radar, just set up an account with a registrar under an alias, use some fake ID generator or whatever. And there you go. It's not that hard to frustrate the hell out of your competitor there.

So I'm not too happy with the investigation part. And if you look at 5.1 the notification itself, on paper, it sounds like hey, that's a good idea, but it can be so easily defeated. If I'm going to steal a domain name for whatever purpose, to sell it or you want to perform an attack, you want to take something down, so you want to transfer domain name under your control. This is going to be published, so any attacker is going to read, what does the transfer process involve? Okay, there's a TAC that needs to be generated. Okay. That's all common sense, good security. Oh, there needs to be a notification. How am I going to nullify the notification?

Well, one of the easiest things to do is if during your domain theft exercise, you already managed to get the email address from the registrant, set up a mail bomb. It is so easy. I wouldn't recommend doing it for yourself, but I have done it in the past and these things will flood your email box like there's no tomorrow. So the chances that the registrant is going to see that notification in time, that is just going to be very, very hard. That person is going to be digging for weeks in their email box if he's lucky. If he's lucky, his email provider will shut him down and then he can't even access the account. And if you want to go a little step further and make sure that the person is not going to see that notification, make sure you just perform a DDoS on him. Getting his IP address is very, very simple. Just send him an email with something interesting. As soon as he clicks on a link, you got the IP address. Now for $25, there are services out there that will DDoS the hell out of that person for the entire weekend. Just look at stress tester and you will find some very interesting services there.

Also, if you look at some registrars, sometimes you don't have to do anything. you can register an account with the registrar, you just want to get that domain, to steal the domain name from and register a domain name there and just see how much email that the registrar sends to the new customers. As soon as you know that, hey, okay, it's already X days, and everything of that registrar is going into spam, well, you already are in a very excellent position there just to make the assumption, okay, if these guys are going to send a notification, most likely, it'll end up in the registrant's email box spam folder. So you don't have to do anything. So I'm not a very big fan of this recommendation. I think it can be easily circumvented if you just put your mind to it. And these examples are just easy ones. You can go much, much further if you want. Thanks.

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

KEIRON TOBIN: Thank you, Theo. Yeah, I think you raise some good points. I would just like to know, I thought the idea of the notification was when the domain was unlocked for transfer, and the notification wouldn't come through. And then just in regards to the investigation of where it was, I think that's more for registrars—well, for ICANN Compliance to essentially identify kind of if there has been any issues in terms of the registrant getting the domain back, because obviously, usually when a domain is hijacked or stolen, you would usually go through [inaudible] and work with the registrar, which ICANN Compliance isn't usually involved in unless it's reported to them as well. So that's where I believe that information was coming from. But maybe you are right, and so maybe we need to make that a little more clear in the document. Thank you.

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

EMILY BARABAS: Thanks, Roger. Just taking a step back for a moment to think about this recommendation. It's one that we've gone back and forth a bit on and talked about some possible different purposes. I think originally, it was introduced with the idea that it might mitigate the potential for brute force attacks, and then later kind of folks converged on a more of an operational goal driving it. I guess one way that we can take a step back and test a recommendation or a candidate recommendation, we put all these things out here, it doesn't mean that every single one sticks. So one thing we can do is take a step back and think about if we were to take this recommendation out of the package of recommendations, would there be a hole, would there be an impact on the sort of core goals of this PDP, which is the security and efficacy of the transfer policy?

And if the answer is no, maybe some of the tinkering around the edges of the operational matters are not necessary for this package of recommendations. One thing for the group to consider is whether this needs to stay in. So again, just kind of taking a step back and thinking about if there's another way to look at this without going into all of the details of the recommendation text. Thanks.

ROGER CARNEY: Great. Thanks, Emily. And great reminder there that yes, that's the reason we're reviewing these, is to see If—not just that they should change or not, but that we do agree on that they should exist and they're serving the purpose. Theo, please go ahead.

THEO GEURTS: Yeah, I think that's a great suggestion there. So yeah, let's take it in mind. And just to follow up a little bit more on this, during the Christmas holidays, I was thinking back a little bit on this recommendation. And I sort of felt like how similar it was with the IRTPC change of registrant policy. And I thought we can change and wordsmith this over and over and over till oblivion comes but we’re never going to fix this. And we never fixed it within the change of registrant policy. We ran into the same operational challenges there. We would change the wording one week, and then there would be an operational issue with the wholesale registrars. We would change the language again, and then we would have an issue with the retail registrars again.

Short story, we spent months on trying to solve something that was not really solvable through a policy like this, where notifications are sent to the registrant. And that is not security, it will never be. And just to make sure we spent months on it, and looking back on it now, there are some pretty large holes in that entire policy there. I'm not going to mention them because if I would do that, I would reveal real issues, so I'm not going to mention what the holes are. But if you look at a policy, because it is public, you can throw anything at it nowadays. And we are a lot further in time now. Cybercrime has become so sophisticated. For $200, you can get yourself a crime as a service apparatus which just does everything you want to attack a target. And it doesn't cost much, it doesn't require any technical knowledge. So it just comes to be how sophisticated a cybercriminal is. And we can wordsmith this till oblivion, and I'm going to be on [inaudible] pointing out new flaws in it. Thanks.

ROGER CARNEY: Great, thanks, Theo. Yeah, and I think that as we discussed in our last session, and Emily mentioned it, that we went from this possibly being a security feature to recognizing that that was not necessarily what we were trying to do and it was more of a user experience or operational kind of concept. And to Emily's point of, does it serve the purpose of this PDP, what we’re tasked with, does it help answer the charter questions, does it provide something specific that nothing else is resolving? I think that's a good way to look at this. And as we've talked through it, again, we've moved on from this being something that's security related, which would fit nicely into several of the charter questions, to something that's more of a user experience.

Again, not trying to negate user experience, because obviously, one of the big things is consistency. But yeah, it's one of those when you look at it, does this provide anything, a consistent view or security view that we're trying to answer in the PDP charter questions? And then I'll leave that open to the group. I would say that that's a great way to look at it. And thanks, Emily, for bringing that up. And thanks, Theo, for throwing on this week's stumbling block for this recommendation, because that's actually perfect. And what we want to do is test those in the real-life ideas.

So again, I think let’s, everyone, take a look at it. Does it actually help us achieve what the PDP is supposed to do? Is it answering any question that we haven't answered already or providing additional information? So take a look at it and see. I think obviously, we've talked through and it's good. I wouldn't say it to useless talk for sure, because we talked through it and got a good understanding of this was not necessarily a security issue, but more of a user experience issue.

Okay, so I'll leave that open. And I think that that’s a good question. And please comment on this, if you see this as being useful or not. That's really probably the next step on this before we continue, as everybody said, wordsmithing this to death. If we don't see the purpose here, then let's remove it and move on.

All right, so let's go ahead and jump into something this discussion did lead to, which is an additional candidate recommendation highlighted toward the bottom here. If a gaining registrar requests a transfer and inter-registrar transfer lock is in place, the transfer must not proceed. I think this was our—I don't know if we call it a timing discussion that we had last week or last session, and maybe even the one before that, where the lock supersedes anything else. If there's a lock on it, nothing happens. It just needs to be noticed that there's a lock and communicate back to the registrant so that they can handle that with their sponsoring registrar. And as simple as removing a lock or determining what the lock was for, and working through that process. That's where this recommendation came from. I don't know if anybody has any comments or questions on it. We did talk about it quite a bit last time. So Steinar, please go ahead.

STEINAR GRØTTERØD: Yeah, hi. I'm just wondering whether this is some sort of requirement for the gaining registrar to assist the registrant when there is a look set on a domain name to be transferred, or is this purely a statement that inter-registrar transfer requests must not supersede any locks that is on the domain name? Thank you.

ROGER CARNEY: Thanks, Steinar. Yeah, I think the discussion around this was, as you mentioned, a gaining registrar probably won't have a lot to do except for help explain to the registrant the possibilities here, but the registrant really—and I think in our notes from last session actually detail that out pretty good was, when this occurs, there could be different locks for different reasons. And it's really up to the registrant and the registrar of record, the sponsoring registrar, the losing registrar, to resolve those issues. And obviously, the locks can be for different reasons. And I think that that's where we left that, is it could be a service that they bought from the registry, it could be as simple as a client lock that can be easily removed. And that can happen and then transfer can go through, or it could be a lock for UDRP or for other legal reasons. That obviously will need work and attention to not just explain, but to possibly move forward on or not. Steinar, please go ahead.

STEINAR GRØTTERØD: Yeah, I think it's definitely an educational purpose. We have to teach the users, the registrants about the different types of locks.

And I do want to emphasize that registry-set logs do have, in my opinion, more important meaning than client-set logs, because it's very often connected to URS, UDRP cases, etc. which there should not be any transfer initiated on that kind of domain name without any preconditions being set. Thank you.

ROGER CARNEY: Great, thanks, Steinar. Any other comments or questions? Again, this one, if I remember right—and maybe Emily can plus one—I think this directly came out of our last discussion on this topic five, it just came out because of the timing that everybody walked through. Thanks, Emily. But I guess I'm interested in comments on, is it useful? Again, going back to Emily's idea, is it useful and does it serve a purpose here? Theo, please go ahead.

THEO GEURTS: Yeah, as far as I recall, we were discussing what should happen if there is a lock on the domain name. And basically, what we sort of mirrored is what is happening now. If you try to transfer a domain name with such a lock on it, then you get a message back that it is not possible. So I think from that perspective, the language sort of reflects this, the current status quo. But reading the additional candidate recommendation, I sort of wonder if it is not overly broad here. If a gaining registrar requests a transfer and an inter-registrar transfer lock is in place, the transfer must not proceed. Is that not an excellent piece of language which some registrars might use to sort of block all kinda legitimate transfers? Did we sort of make sure that we covered this further or earlier on in the policy? It's just like, oh, I've got to put everything on a transfer lock and I'm going to screw my competitors over here. It sounds very broad. Thanks.

ROGER CARNEY: Great. Thanks, Theo. And that's a good point. I think that we do have a discussion of that. I guess we'll have to look at it. But we do still have to resolve our next discussion, after we go through these candidate recommendations, is still to hit the 60-day lock, and which has been more than the 60 day lock, but locks in general, and that discussion still has to be fleshed out as to where we're going to head on those. So this recommendation will be directly tied to that. And I think that this recommendation again came out of the fact that we were trying to straighten out or hopefully make a little more sense out of locks and transfer process and how they work. So Berry, your hand was up, but maybe I said what you were going to say. So Berry, please go ahead.

BERRY COBB: Yes, you did. And the whole point of how this got listed here, as you noted, was based on our prior conversation, and we were trying to unwrap about whether the domain should be unlocked at the time of requesting the TAC or not. And I believe that there was a deliberation around how a domain might still remain locked, even if it's a client-based lock up until the time the transfer goes. But I think Emily notes it correctly in chat that we parked this one and we circled back to see if we're not going to address it in another way. And I'll put a little plug in here, as I've mentioned it before, staff has put together a swim lane view of the transfer process. And there is a specific section about the point in time when a registry is going to start to take action on a transfer, that if the domain is locked for the variety of reasons that you mentioned, it needs to be resolved either from the registrar of record and the registrant before that transfer can proceed. And kind of channeling Theo here, especially the way the current text is read, is it really necessary to define a policy for what is really pure operational in nature? So I'll stop there. Thanks.

ROGER CARNEY: Great. Thanks, Berry. Yeah. And again, I think, as we teased this out last week, it was a good point to notice. And again, I am not saying that we keep it or get rid of it. But I think our discussions, when we hit the 60-day lock discussions again, will hit on this topic as well. And to Theo's point, it may be a little broad right now, but I think it's a good point that we should remember. And again, do we keep it or not? I don't know. But it's a good topic that we hit on and noticed and it'll be in our deliberations anyway, so it'll be noted. But yeah, I think when we hit the 60-day lock, we'll pull this back up and see if it makes sense moving forward or not.

So, any other comments, questions on this? Okay, let's go ahead and move down to recommendation six then. All right, no comments or anything on this. I think this was fairly well accepted. But let me read it. Emily, please go ahead.

EMILY BARABAS: Thanks, Roger. Just noting that I think the leadership team—and this was before the holidays so it feels like a long time ago. But I think when we were revisiting these recommendations six and seven, and looking back on some of the deliberations, there was a question raised about whether it makes sense to structure this in a more sequential fashion. So Roger, as you're reading through six and seven as it was originally proposed, it might also be helpful to read that sort of redline text right below it, which would be a condensed six and seven sequenced in a little bit more of a logical manner that could potentially replace what exists already for six and seven. So it's not something the group has discussed previously, but it also doesn't really change the meaning. It's just about logic. Thanks.

ROGER CARNEY: Great. Thanks, Emily. Yeah, and I do remember when staff broke that out. And when I read it, it did flow easier for me. And I think that maybe that was the question we were trying to solve there. But let me go ahead and read these real quick. And then we'll jump into the recommendation six new wording down here too. But currently, the working group recommends that the registrar continue to generate the TAC, set the TAC in the registry platform and provide the TAC to the RNH or their designated representative.

The working group further recommends that the TAC is only generated by the registrar record upon request by the RNH, or their designated representative. After confirmation that the TAC has been successfully set at the registry, when the registrar provides the TAC, it should also provide information about when the TAC will expire.

Recommendation seven says the working group recommends that when the registry receives the TAC, that the registry must securely store the TAC using a one-way hash that protects the TAC from disclosure. And I do remember that Sarah and I went back and forth on disclosure and we kind of agreed that—I think Jim actually said a few things too, the disclosure may be the right word there. So that's what the comment is there.

But let me read the new, maybe more flow friendly version of recommendation six and seven combined. The working group recommends that the TAC must be only generated by the registrar of record upon request by the RNH or their designated representative. 6.2, when the registrar of record sets the TAC at the registry, the registry must securely store the TAC using a one-way hash to protect the TAC from disclosure.

6.3, 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. So as Emily mentioned, the original candidate recommendation six and seven, I think the new recommendation six says the exact same thing, just maybe more in an organized fashion and in a more sequential fashion.

I'll ask the group, is it conveyed correctly and are we saying what we want it to say? Theo, please go ahead.

THEO GEURTS: Yeah, I think it says what we wanted to say. I've got one question, though. We set requirements around the TAC itself but you're not setting any requirements on the one-way hash itself.

ROGER CARNEY: That is true. And I don't know that we need to or not, if the one-way hash—I suppose if we wanted to get specific on it—I don't know that we need to or not. It's a good question. I just don't know if we are concerned if a registry uses a different one. It doesn't affect the process. But to your point, would it affect the security level? Maybe that's the question. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. I agree that we need to set some minimum level, because if you use a very, very old hash, you could basically just have it plaintext, it wouldn't make any difference. So there needs to be a minimum requirement. Thank you.

ROGER CARNEY: Thanks, Kristian. Berry, please go ahead.

BERRY COBB: Thank you, Roger. I'd also ask maybe if Beth can tack this on to her action to go back to the registries. And I'm wondering if the RFC 9154 might also have a connection to this one-way hash thing. Thanks.

ROGER CARNEY: Great. Thanks, Berry. Yeah, and I was just going to ask actually, anyone on the call know a good current level that may be suggested that Beth could take? Or we can suggest to the Registries Stakeholder Group. Theo, please go ahead.

THEO GEURTS: Yeah, basically, what Kristian just mentioned, I just looked up the one-way hash and there can be some really, really old hashing algorithms which are totally insecure. So I think when it comes to the one-way hash, if you want to do that correctly, you should be pointing out to advisory stuff like NIST or CISA or NCF from Europe, who wrote extensive documentation on how you should be hashing certain stuff. Thanks.

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

BETH BACON: Hey, sorry. So predictably, I accidentally left the Zoom Room and then as soon as I came back, I heard, “So, is there anything we can tell Beth?” I was like, “Probably what you just said.” So if there is something with regards to the one-way hash, I just missed a little bit in there. Can I trouble people to maybe drop in the document and just put that in there where it's relevant and then I could flag it for the rest of the registry folks? Just because I missed it and I don't want to make you redo this all over again. Thank.

ROGER CARNEY: Thanks, Beth. I'll ask Kristian or Theo to drop just a comment in there to make sure that this is—yeah, not using, as Kristian said, hash, the term itself can be pretty loose. So if Kristian or Theo drop in there something.

BETH BACON: Yeah, sorry to make work for you guys. I just missed Kristian's comment, but I heard Theo's original thing. So thank you very much. I apologize, guys.

ROGER CARNEY: Great. Thanks, Beth. Okay, yeah, that's a good point to bring up forward. So thanks, Theo, for dropping that comment in there. Is there any other comments on these? Again, I do prefer this new recommendation six to the old six and seven. I think it flows a little easier for my head to understand, but maybe it doesn't for others. So please let us know if you prefer the old way to the new way. I definitely like the new way better.

Okay, any other comments on six/seven? Thanks for that chat, Jothan. 6.2 may be addressed in the RFC as Berry mentioned, and Jothan quickly looked up. Okay. Yes, Keiron. Let's get back on that and we'll revisit that when we get back to it when we hear back.

All right, let's jump into recommendation eight. The working group confirms the following provision of Appendix G, supplemental procedures to the transfer of policy contained in the temporary specification for gTLD registration data for that registry operator must verify that the AuthInfo code provided by the gaining registrar is valid in order to accept the inter-registrar transfer request. And obviously, I think Emily probably put in, with terminology updates in accordance with other relevant recommendations, e.g. AuthInfo, incoming TAC.

So we're just basically confirming what is already said in policy. Thanks, Emily. Yes. The new six is just replacing six and seven but says the same thing. Just in order. Thanks. And on eight, any questions or comments? I think that, again, this is just from current policy, and we're agreeing that it should move forward. So Theo, please go ahead.

THEO GEURTS: Yeah, I would personally reword this a little bit just to make sure that our recommendation is in line with current policies, and then just remove the supplemental procedures to the temporary specification. That is going away at some point anyways. So I would keep it just in general as we operate, or must abide by general ICANN policies anyways, without referring to very specific ones. [inaudible] policy.

ROGER CARNEY: Yeah, thanks. I don't know that any of our recommendations so far says that they have to. So I think this is just—yeah, I see what you're trying to get at, the first point here. The recommendation really is just that they had to verify it. And where that came from is just a reference. Is that your concern, Theo?

THEO GEURTS: I thought it was just redundant. All policies that are applicable are important. So yeah, just like I said, it's just suggestion. You're going to have language at some point which points to the temporary specification, which will be gone if the IRT on the EPDP phase one speeds up by any miracle. So you're going to then have a reference to a policy that no longer exists. That is a little bit of my point. We always have policies which we need to be compliant with, which we need to take into account without saying very specific what they are, and the temporary specifications is one that's going to be outdated, and it's very specific. But it's no biggie. Thanks.

ROGER CARNEY: Great. Thanks, Theo. Any other comments or questions on this? Okay, excellent. All right, let's jump into recommendation nine. The working group recommends the TAC may only be used once. The registry operator must clear the TAC as part of the completing the transfer request. I don't know if there were any comments here specifically.

Okay. I think that on both of these topics here, this goes back to our original discussions we started in the summer, I think, on the single use and how to make that happen. So I don't know if anyone has any comments or questions here. Keiron, please go ahead.

KEIRON TOBIN: Thank you. Sorry, I'm just rereading recommendation nine, the working group recommends that the TAC may only be used once. Why do we have “may” in there?

ROGER CARNEY: Good question. It’s a lower case “may” so I think it holds different weight.

KEIRON TOBIN: Is there something that I'm missing in context?

ROGER CARNEY: I don't think it's “may” as in an option. I think it's ... But that's a good point. Maybe it shouldn't use that, just not to be confusing. That “may” is not to be optional. And I think that that's probably why it's lowercase. So it's not the capital “may.” But maybe we should make it the capital “must” as Sarah is suggesting.

KEIRON TOBIN: Good point, Catherine. Yes. You may not use it. But does that change that the working group recommends that the TAC—if we change, it “must” only be used once? Okay. Maybe that does, Catherine. Theo, please go ahead.

THEO GEURTS: So it makes sense if you have a database full of domain names that you don't have the same authorization code for all these domain names. And I think that applies for the TAC also. It makes common sense, you don't want to have the same TAC for multiple domain names. I think that is what we are trying to achieve. Now, when I read the recommendation that the TAC can only be used once, the registry operator must clear the TAC as part of completing the transfer request.

I'm wondering how general we are going to look at the word TAC in the sense like it can only be used once. It could be that GoDaddy generates the same TAC as Realtime Register does for completely different domain names. Our databases are not linked together. They are independent platforms. So there could be a situation that two different domain names and two different registrars have the same TAC. And this policy says that is basically—well, we're editing on the fly here. No, never mind. Brain fart. Thanks.

ROGER CARNEY: Thanks, Theo. Okay. Yeah. And I think that—one of the things is something that Theo was kind of wandering around there—yeah, I like the new wording, Emily. And I think Theo is heading down a path is talked about elsewhere, the uniqueness of the TAC across the registrar. Okay, so a slight word update there. Any other comments? Emily, please go ahead.

EMILY BARABAS: Before we go on to the next charter question. I just wanted to note two additional items that the group had considered potentially addressing, but had not made a decision on. One was whether there was any additional guidance the group wanted to provide on who can receive the TAC and whether the group wanted to provide any additional detail about the secure manner by which the TAC is provided. So those don't need to be answered today, but I did want to just put in a plug that those are elements that could still be addressed under this charter question if folks wanted to put in recommendations for those. Thanks.

ROGER CARNEY: Right. Thanks so much for bringing that up. Theo, please go ahead.

THEO GEURTS: Yeah, I sort of regrouped my thinking here. And it now says the working group recommends that a TAC may only be used once. I think if you're a registry operator, that's going to be problematic, because that means that you're going to need to make sure that those TACs, those hash TACs, because it's going to be a hash of the TAC, you're going to need to keep track of that, because they can only be used once. And that can be also problematic, I guess, if the TAC is already used and we generate a TAC, and send it to the registry, and the registry goes like no, that's already been used, generate another one. I think that's going to cause operational issues. How do you track it?

ROGER CARNEY: Yeah, but let me interrupt you. I don't think it means the uniqueness. It means per that domain, you cannot reuse that TAC again. I think that's what this is saying. That it's a onetime use only. You use it once, and it's no longer a valid TAC for that domain.

THEO GEURTS: Okay.

ROGER CARNEY: Thanks, Keiron. Does that make sense, Theo?

THEO GEURTS: Yeah. But non-native English speakers might get a very different first impression there.

ROGER CARNEY: And that's a good point. And maybe we need to add that on there, that it may only be used once per domain or per domain name transfer. And I think we've used the language elsewhere, actually. So maybe we'll grab that. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. Emily just noted that we didn't look at who we should provide the TAC to. But I'm pretty sure just a while ago, at this call, I read that we could provide it to either the registered name holder or the designated representative, which in many cases would be a reseller or some. So I would think that it is covered just a couple of recommendations back, but please correct me if I'm wrong.

And then on the subject that we were just talking about, I think I could also misunderstand it in the same way as Theo. And then also just thinking, have we considered in any recommendation if we should require the TAC to be randomly generated each time?

Because how it works currently today is that the registrar can set whatever they like and some registrars, they give the registrant the option to choose the TAC themselves, which is maybe not the most secure way. So I'm just thinking, I don't remember if we talked about it before, but personally, I would prefer a recommendation that said that the TAC needs to be randomly generated each time, but maybe we will we have it and someone can help me find it. Thank you.

ROGER CARNEY: Great. Thanks, Kristian. And I think this goes back to our recommendation three, on the syntax of the TAC. And, again, let's all take a look at that new RFC that Jothan put in chat and take a look to see if that doesn't solve those issues. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. Just to follow up, having a required way of having the Auth ID doesn't mean that you can still give the registrant the option to make it themselves, we see that at many registries. So if you have like it has to be this syntax, small letters, large letters, and so on. The registrant can put in words that are easy to get and all kinds of [inaudible]. So I don't think the syntax is enough, I still think we need to require it to be randomly generated each time.

ROGER CARNEY: Great, thanks, Kristian. And I think that's a good point to bring up. And maybe we need to clarify, because I think we're saying that the registrar of record is responsible for the generation, not the registrant or its designated—the registrar of record is the responsible. And I think we've said that, but let's make sure that it's clear that it's only being generated by the registrar. And as you said, that we make sure that there's—I don't know if random is right or not, but uniqueness to it. So Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. And a quick follow up. It could also be a registrar employee that wanted to make it easy for the customer by making the Auth ID pronounceable or something. So we see this happening. So I just have to mention it. Thank you.

ROGER CARNEY: Great. Thanks, Kristian. Yeah, we need to be clear on that to make sure it's not that simple. So okay, great. Thanks. All right, I think we're down to about nine minutes. Let's jump into recommendation 10. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. There was also the other question and I think Emily found it on the screen and highlighted it. 6.3 there. Yeah, so that was the one where Emily said that we didn't talk about this, but I see it right here. So isn't this already good?

ROGER CARNEY: Yeah. And Emily was just looking to see if there's anything more needed than that. So that was her main question. Thanks, Kristian. All right, let's jump into 10. The working group confirms that the transfer policy should continue to require registrar to provide the TAC to the RNH or designated representative within five calendar days of request. Although the working group recommends that the policy state the requirement as 120 hours rather than five days to reduce any risk of confusion. The working group further recommends that the policy make clear that 120 hours is the maximum and not the standard period in which a TAC is to be provided.

Any comments or questions? I think we've talked about this not necessarily specifically 10. But talked about the idea several times. But any comments, questions or concerns? And I know that that last sentence, I don't know if anybody's on that can quote Marc Anderson, but he always has a good verbiage for the make clear that 120 hours is the maximum, not the standard. He's got some nice little wording that says that. But it still makes sense here. Kristian likes the 120 hours better than the five calendar days. So yes, I would say that's true, Kristian.

If there's no comments, let's jump into the last recommendation here, recommendation 11, which we've updated slightly. Again, I think that staff took a stab at trying to make sure that multiple concepts are pulled apart here, but I'll read the original one and then read the alternate one.

The working group recommends the transfer policy include a standard time to live, TTL, for the TAC of 14 days enforced by registries. Working Group recommends that the registrar of record retain the ability to set the TAC to null at any time in response to requests from an RNH.

Alternative alternate language reads the working group recommends that 11.1, a standard time to live for the tack TAC be 14 calendar days enforced by registries, and adding a footnote that registry should set the TAC to null after transfer complete.

There's a question. We kind of just talked on that in an earlier recommendation that we just hit. But let's jump into 11.2, registrar of record may retain the ability to set the TAC to null anytime in response to request from an RNH. And then another question, after a period of less than 14 days by agreement of the registrar record and the RNH. Any comments or questions on 11? Theo, please go ahead.

THEO GEURTS: Yeah, on 11.2, the second bullet where you can set up an agreement with the registrant, why is that in there? I don't see what it solves.

ROGER CARNEY: I think that that discussion was around the possibility of a registrant or—the registrar wanted that window to be smaller so that the exposure of transfer is less. So maybe a high-value domain, they want to complete it in a day or three days instead of leaving it out there for 14 days.

THEO GEURTS: Okay. But you can also turn it around maybe. So you can set up an agreement with the registrant which they never read that agreement that there is always going to be 14 days because you agree to it. And if for any reason the TAC is created and somehow not working, which is sometimes happening for whatever reason, HTML formatting in email clients, sometimes these things go wrong. And then the registrant cannot nullify the TAC and create a new one because there's an agreement in place. Just thinking out loud here. Seems a little bit exploitable.

ROGER CARNEY: Yep, you bet. Okay, any other comments or questions here? Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. If I remember correct, what we were trying to do with this sentence was to allow a registrar and registrant to agree on maybe automatic nulling it after like two days or three days or something. I think that was what we were talking about back then. Personally, I'm good with the just standard 14 days and then at any time if the registered name holder requested. But I think some people in the group asked that it was possible for some registrars to, for example, have a standard seven days instead. I'm personally [not] in favor of it. But I think that was what we were trying to put in there, back when we talked about this last time.

ROGER CARNEY: Thanks, Kristian. Berry, please go ahead.

BERRY COBB: Thank you, Roger. So a couple of things here. One, again, in RFC 9154, there's a little bit of information about TTL. In general, it's basically stating that there is no current definition of a TTL and that essentially, there's flexibility based on as they use proprietary registrar specific criteria that may provide for transfer specific TTLs tuned for particular circumstances.

At any rate, what I find interesting looking at this RFC is their use of sponsoring registrar, but I'm going to set that to the side. And then finally, I'm curious in terms of consistency, 120 hours, about the time for sending the TAC to the RNH, I wonder if instead of days, we maybe convert this to hours as well. I know the number of hours grows quite a bit here when we get beyond one week. But it may just make things a little bit more cohesive if we looked at total hours instead.

ROGER CARNEY: Thanks, Berry. Okay, we are at time here. It sounds like the 14 days—and to Berry's point, whether that should be hours or not—is agreeable to people, everyone. But it may be that the 11.2 needs to be looked at a little more. And again, I encourage everyone to take a look at that RFC that wants to get into that detail and take a read of that. And maybe that solves some of this.

But let's get back to 11.2 at our next meeting, or any questions really, but specifically this since we didn't get enough time to talk through it. Okay, any other comments or questions about anything else? Otherwise we'll jump off and start back up here next week.

Okay, great. Well, thanks, everyone. Happy new year to everyone. Great discussion today. And again, take a look at that Recommendation five. Does it fit? Does it not fit? Please put some comments in the document. Again, recommendation three, we're still looking at the wording there. And again, let's take a look at that RFC that Jothan provided and see if that solves some of the problems in three and maybe even 11 and elsewhere. Thanks, everyone, and we'll talk to you next week.

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

[END OF TRANSCRIPTION]