ICANN Transcription
Transfer Policy Review PDP
Tuesday, 29 June 2021 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/VwTpCQ
The recordings and transcriptions are posted on the GNSO Master Calendar Page: http://gnso.icann.org/en/group-activities/calendar

ANDREA GLANDON: Good morning, good afternoon and good evening. Welcome to the Transfer Policy Review PDP Working Group call taking place on Tuesday, the 29th of June 2021 at 16:00 UTC.

In the interest of time, there will be no roll call. Attendance will be taken by the Zoom Room. If you are only on the telephone, could you please let yourselves be known now? Thank you. For today's call, we have apologies from Sarah Wyld, RrSG. They have formally assigned Rich Brown, RrSG as their alternate for this call and the remaining days of absence.

All members and alternates will be promoted to panelists. Members and any alternates who are replacing members, when using the chat feature, please select panelists and attendees in order for everyone to see your chat. Observers will remain as an attendee and will have access to view chat only. Alternates not replacing a member are not permitted to engage in the chat or use any of the other Zoom Room functionality such as raising hands or agreeing and disagreeing. If you are an alternate not replacing a member, please rename your line by adding three Z's before your

name and add in parentheses alternate after your name which will drop your name to the bottom of the participant list. To rename yourself in Zoom, hover over your name and click rename.

As a reminder, an alternate assignment must be formalized by way of a Google assignment form. The link is available in all meeting invite emails. Statements of interest must be kept up to date. If anyone has any updates to share, please raise your hand or speak up now. If you need assistance updating your statements of interest, please email the GNSO Secretariat. Please remember to state your name before speaking for the transcription. Recordings will be posted on the public Wikis pace shortly after the end of the call. As a reminder, those who take part in the ICANN multi-stakeholder process are to comply with the expected standards of behavior. Thank you. And over to our chair, Roger Carney, please begin.

ROGER CARNEY: Thank you very much. All right. Just a couple of quick follow-ups from our last meeting where we went over goals and the transfer authorization code. The goals have been edited and posted to the Wiki so I encourage everyone to go look at the Wiki and look at the goals and provide any comments if they have any suggestions. As well as definitions and terms document has also been uploaded to the Wiki. On the screen here, you can see. And I encourage everybody to take a look at those and to make any suggestions on the current verbiage there and plus anything that we're possibly missing there. So, both documents good to go ahead and look at. Again, this goals is what we covered two weeks ago now but it was

a good discussion and any further comments are welcome. I think that was all of the catchup on that. Thank you.

And there's the terms. And again, just take a read through them. The terms and definitions is more of just a baseline document so that everybody's talking from the same spot because I assume some of these will probably make it into our document but most of these are just generalized knowledge definitions just so everybody's using the same definition.

Okay. Let's jump into the outreach document. We were targeting for completion of this today in hopes of getting it sent out yet this week sometime. I guess the only big item left is the DNS and DNSSEC discussions that we've been having in several meetings, plus on list. At this time, it appears that the general feeling from the group is that this PDP is probably not the place to solve this problem. I think that generally people agree there is an issue there that should be reviewed but it's out of scope for this group and probably even out of scope and maybe a little too technical for this group to get into. I think from this group standpoint, it won't be part of any work that we're doing.

The one thing I do question is, do we have some kind of comment or maybe even an official recommendation that this should be looked at somewhere? This DNSSEC, DNS issues? And I think that where it should be looked at is probably the biggest question mark. I mean, I'm not sure that it's even in the GNSO remit to look at this. Maybe it's more of an SSAC or IETF. I know there's probably three or four IETF RFCs out there that mention different ways to make these transfers of DNS and DNSSEC better. And I think that maybe there's an opportunity for someone there to pull

those together and maybe create a best practice idea or again, maybe SSAC has ideas on that. Steve, please go ahead. I cannot hear you if you're talking.

STEVE CROCKER: Yeah. I was muted.

ROGER CARNEY: There you go. Now I hear you well.

STEVE CROCKER: Thank you very much. So, I'm in 100% agreement with you actually. Obviously, we're not going to solve the technical details within this group. Let me just go back for just a second to the goals. Enable registered name holders to move their domain names to new provider, thereby increasing consumer choice and competition. And then under additional policy goals, transfers should be registrant friendly.

So, under that rubric, the reason why I and a couple of others have raised this issue about the domain name service is because it's very often intimately tied to the registration. Let me turn that around another way and maybe the following formulation will be comfortable to everybody, that during a transfer, any services that are inextricably tied to the registration, the registrar should cooperate in transferring smoothly. Some version of that is what we're really trying to get at. The technical details of how to do that, what the state of the art is and all of that, 100% agreement that that belongs elsewhere. SSAC and IETF and so forth and it's being

worked on. And I see Volker has been quick to say, "No." I don't know why, Volker, you would say that.

Anyway, that's the way I think would be helpful to frame this, that whenever a registrar's involved in transfer, that any services that are inextricably tied to it, where then the transfer should be done smoothly. And it is out of scope for ICANN policy. Well, why does that matter? It's good for the registrants. It's good for the Internet. And that does not imply that it includes email, websites, Minecraft servers and so forth, unless the registrar insists on killing those services as part of transferring the registration in which case it would apply, but I think that in practice, those things are generally priced and sold separately.

ROGER CARNEY: Okay. Thanks, Steve. Again, I think everybody's kind of in agreement that the work isn't ours necessarily but it is something that it could be resolved elsewhere. And again, to Steve's point, the registrant would benefit from resolution of that. Again, not our issue and we're not going to take it up. My only question to the group—and I'll let everybody talk—is, should we make a recommendation or comment, however we do it in our report, that suggests that this work should be looked at somewhere? And not somewhere, but come up with where we actually think it should be done. So, Kristian, your hand was up and then you brought it down. I don't know if you wanted to make a comment.

KRISTIAN ØRMEN: Yeah, [inaudible] but I have grandkids in the background so I'm trying not to [inaudible]. But like Steven said at earlier meetings that some registrars would tie DNS directly to their domain, that is the same with websites and email and so on and especially for email and some hosting companies tie the whole thing together, domain, website, everything. So, and this policy is only about the actual transfer of the domain between providers. I think it's very important that we keep these things apart because else we are going to start regulating all the hosting businesses within this policy. And I really, really think that's out of scope and I don't think it belong to this document at all.

ROGER CARNEY: Okay. Thanks, Kristian. Theo, please go ahead.

THEO GEURTS: Yeah, thanks, Roger. So, back to the question, if we would put out a recommendation or a comment, I think if we put out a comment, that would be okay. There's not much to it. But if we put out a recommendation, I'm not sure how that goes procedure-wise within the GNSO. I mean, if we come up with a recommendation, doesn't that imply that the GNSO has to do something with it and what would that be and would it be bad or would it be good? I have no idea. Thanks.

ROGER CARNEY: Thanks, Theo. And I think I had the same thought processes that, was—I'm not sure this is a GNSO issue to resolve. But again, I mean, obviously I think a lot of people on this call agree that it is

an issue for registrants, it's just not an issue for this PDP, and possibly not for the GNSO to solve. But, yeah, and I would have to look at that, Theo, is what way does that recommendation if we did a recommendation, what does that mean? And again, I don't think we want to tie the GNSO to this necessarily but again, maybe just a comment saying, "Hey, we discussed this and this is a good registrant feature that we need to pursue somewhere and make the suggestions of where." Okay, Steinar, please go ahead.

STEINAR GRØTTERØD: I'm pretty sure that the registrant or the end-users would like to have some sort of best practice somewhere that they can kind of check out when they're doing a transfer. But I do agree this is the technical stuff and the DNSSEC and all the services, this should not be included in the policy. But maybe this in the end, we'll end up with some sort of guidelines which we can all agree about. Thank you.

ROGER CARNEY: Thanks, Steinar. Okay. Any other comments? At this point, I am going to suggest that we move forward with the outreach with nothing about the DNS, DNSSEC issue in it. Again, trying to keep the scope to what we're responsible for in the outreach letter. And I think we continue to discuss if it's appropriate or not to provide a comment or if it is a recommendation, how that looks as to who would be the owner later on of this kind of work. Emily, please go ahead.

EMILY BARABAS: Thanks, Roger. I see a question about putting a timestamp on the letter. So I can certainly respond to that. It sounds like our direction here is to remove the suggested text so that it's just the charter questions included here as the questions for input. We will put a date on it. The proposal is five weeks, so that's 35 days. We'll fill that in and since there's nothing new we're putting in the letter, I don't think this needs to necessarily go out for one last pass over review from the group. Unless you think it does, Roger, and if that's the case, we can send it out as soon as tomorrow to the groups with a 35-day deadline. Does that sound right? Thanks.

ROGER CARNEY: Thanks, Emily. Yeah, so I think that sounds like the plan moving forward. To Mike's comments in chat, I think what we're hearing is there is no appetite for the expansion of this PDP to take that on. And again, it would be a question of if the GNSO is even responsible for taking that on or not. So, from this PDP standpoint, we won't be delving into that. Okay. Any other comments, questions? Taking on trying to solve DNSSEC, DNS issues during transfer. Okay. Well, I think we can move forward with this outreach letter and we can wrap up this item here. Okay. Next on the agenda. Yes. Staff, please go ahead.

EMILY BARABAS: Hi, Roger. So, you all should have seen with the agenda that you received a spreadsheet of metrics from our contractual compliance department. This is in response to a request for updated metrics on various aspects related to the transfer policy. So, we have a colleague here, Holida Yanik from the compliance department

who's going to explain what compliance is able to provide, what they're not able to provide in response to the requests—which did include some specific elements that people were interested in—and sort of an overview of some of the different elements that are included here. So, I'll hand it over to Holida to speak to that. This is going to be a pretty brief agenda item so that we can continue on with the discussion, but questions can be provided over the mailing list and we'll do our best to get responses to those questions after the call. Thanks.

HOLIDA YANIK: Hi. Thank you, Emily. So, before moving on to the metrics for transfer complaints that ICANN contractual compliance received, I just want to briefly describe the role of contractual compliance function and its scope for those who may not be closely familiar with ICANN Contractual Compliance. So, contractual compliance enforces the policies developed by the community and incorporated into the ICANN organization's agreements with registries and registrars and ensures that the obligations set forth in those agreements are met by Contracted Parties, mainly by processing complaints relating to potential instances of non-compliance.

And here, it is important to keep in mind that our enforcement authority is limited to the requirements set forth in these agreements and policies. And we have no authority, for example, in response to the complaint about failed inter-registrar transfer to request the registrar to facilitate the transfer or in case of unauthorized transfer complaint to request or instruct the registrar to return the domain name to the prior registrant or, for example, to

require from registrar to initiate the proceeding under the transfer dispute resolution policy, because these are not set forth in the transfer policy agreements.

So, when addressing the complaint, the validated complaint with the contracted party, contractual compliance rather asks for details regarding how the requirements stipulated in the transfer policy have been followed in the specific case. With that, I will now provide you an overview of complaints received by contractual compliance from external users and involving various transfer issues. So, in the table, you can see the first set of data provides the total number of all transfer related complaints received by compliance from 1 June 2017 to 31 May, 2018 and after enforcement of GDPR and implementation of temporary specification. So, here in this case, that is from 1 June 2018 to 30 April 2021.

In here, contractual compliance provided pre-temporary specification data so that the group will be able to see whether there has been a change in trends. As you can see, the average number of transfer complaints received per month increased from 436 to 475 after implementation of temporary specification. However, here, I'd like to make a disclaimer. The number of transfer complaints received starting from October and November 2020 and onwards was severely impacted by the large influx of complaints resulting from the situation caused by the failing registrar and it has definitely raised the average number of transfer complaints received after implementation of temporary specification.

So, moving on to the next set, as you can see, all of the following sets of metrics are presented in two separate groups, namely Kayako and NSp. On 29 August 2020, ICANN organization launched its compliance solution within the naming services portal abbreviated here as NSp. It's a platform intended to provide a single interface for communication between ICANN and its contracted parties. We have migrated processing of complaints received from ticketing system called Kayako to a new and improved NSp system which facilitates contracted parties to monitor and respond to the address compliance cases within the same platform.

The second set of metrics is a summary of unauthorized inter-registrar transfer complaints received post temporary specification, while the third set provides the number of unauthorized change of registrant complaints received from 1 June 2018 to 30 April 2021. So, the main issues reported in these types of complaints are usually hijacked domain names or email accounts, hijacked control panels, private dispute issues. So, here are the complaints about third parties who allegedly owned the domain name and are not transferring the domain to the complainant and these parties are with whom ICANN does not have any contractual relationship. And we can also see complaints when the domain name lost due to non-renewal but the complainant is not aware about it and files unauthorized transfer complaint with ICANN against the registrar or reseller.

So, when contractual compliance was utilizing Kayako ticketing system, for unauthorized transfer complaints, the categories unauthorized transfer and unauthorized change of registrant were

selected by the complaint processors taking into account the description of the problem given by the reporter within the complaint itself. So, since the system requires manual tagging by the processor, it is possible that some cases were missed out or were not tagged properly. So, complaint category column, within the set of data with NSp label, provide the categories now selected by reporters when submitting complaints. So, this means that these numbers of complaints are taking into account what the complainant's reported to us while filing the complaint.

And the red note below stating, other complaint types had cases—no other complaint types had cases with this complaint category means that there were no unauthorized transfer complaints, sorry, misfiled under different complaint types than those presented in the table. So, as a clarification, as an example for misfiled complaints would be the complaint involving unauthorized transfer filed as abuse complaint.

The fourth group is a summary of complaints received by contractual compliance and involving failed and/or denied change of registrant requests. So, again, a clarification regarding change of registrant complaints received under the complaint type registration data inaccuracy. These are basically complaints involving COR that were misfiled as a registration data inaccuracy complaint. So, in such cases, reporters usually believe that the registration data for the domain name is inaccurate and they want to change, update the domain registration data or were unable to change or update the registration data with the registrar or reseller.

The group five provides the number of complaints received by compliance involving failed and/or denied inter-registrar transfer

complaints. Contractual compliance does not have specific category for all AuthInfo code not provided but we see that most of inter-registrar transfer complaints refer to the inability to retrieve the AuthInfo code and/or inability to unlock the domain names, unless reporters specify a different category such as those you can see in the complaints category columns provided in this table.

Here, you can also see a number of inter-registrar transfer complaints that were misfiled as abuse, domain name renewal or generic registrar complaints. So, we can also see that out of 13,416 inter-registrar transfer complaints, in 358 cases, the complainants reported that inter-registrar transfer was denied due to 60-day COR lock. However, please note that compliance started to capture this data after the launch of naming services portal.

So, you can see that with the launch of NSp and an updated complaint submission form, now there is a possibility for contractual compliance to gather more granular data concerning the complaints received including the data on the possible nature of misfiled complaints. And as you can see in our case, with regard to transfer related complaints, the data on possible reasons for denial of transfer which was not quite possible to collect through Kayako ticketing system. And however, as you can see, the NSp system has not been in place for not so long. Additionally, the data obtained through this system provides a different level of granularity than it was with Kayako ticketing system used up to 29 August 2020, and thus not providing possibility to compare the data and observe the trends from pre-temporary specification period.

And further, as I mentioned earlier, the data after October and November 2020 period has been severely affected by the unfavorable situation caused by the failing registrar and so may not provide a fair picture regarding the volume of complaints that would have been received in absence of the situation.

And as a final note, to sum up, I'd like to repeat that contractual compliance enforcement authority is limited to the requirements set forth in the policies in ICANN agreements. And the effectiveness of enforcement often depends on the clarity of the obligations contained in the agreements and policies. And if an obligation or policy or agreement language is ambiguous or open to conflicting interpretations, our enforcement powers can appear diluted.

So, since this working group is engaged in transfer policy development process, I'd like to note that the clearer and better understood the obligations are, the most straightforward it becomes to enforce them. So, with that, I thank you for your attention. And considering the time limits, I'll be glad if you can direct your questions via email and we'll be glad to respond to them. Thank you.

ROGER CARNEY: Great. Thanks a lot. That's really good information. And again, I think there's quite a bit of a discussion in chat and again I encourage anybody with specific questions to send it to list and we can try to dig into any of those specific questions. I think one of the keys that we were looking at for these numbers was something to look at how the complaints pre-GDPR. So, the difference between

when we were required to do FOAs versus when that was relaxed and most transfers went through an AuthInfo only and I think if you look at those numbers and specifically looking at the number one item up there, it didn't seem to change a lot between pre-GDPR, pre-May of 18 to post. So, again, I'm not sure you can glean a lot out of that but I'm just throwing out there that it doesn't seem there was a dramatic change and any issues. Again, looking at the idea here was, is the AuthInfo secure enough versus requiring the FOA. So, just throwing that out there for people. All right. It looks like we have a queue building here. Keiron, please go ahead.

KEIRON TOBIN: Hello, Holida. Thank you for that presentation. Just in regards to the suspension or termination of registrars' agreement, what category would that fall just out of curiosity?

HOLIDA YANIK: Kieron, thank you. Thank you for your question. Can you repeat to make sure that I understood it correctly? Do you mean whether the terminations are stemming from transfer related complaints?

KEIRON TOBIN: Yeah. So, I just want to understand the data in terms of, because it seems to be like so when a registrar loses its accreditation, usually I can imagine you receive people who send reports saying that their domain has been stolen. I just want to understand those numbers to where that's coming in from just to ensure that that doesn't obscure our data.

HOLIDA YANIK: In the compliance notice page, the notices page, published in ICANN Org page, you can see the number of termination notices sent to registrars including the detailed explanation of the issues, what kind of issues have not been remediated by the registrar and for what purposes the termination has been issued. But currently, right now, I cannot say the exact number of those situations.

KEIRON TOBIN: Sorry. Holida, I just mean in terms of, so, obviously, if a registrar was to lose its accreditation and that registrant is in limbo which means are they—when they message you saying that they have had a domain that has been potentially stolen, where would that fall in this category of what you're showing us here? I mean, is that categorized in other, are you classing that as an actual complaint, even though nothing can be done? That's what I'm just trying to wrap my head around just so I can understand the numbers a bit better.

HOLIDA YANIK: Okay. I understood you. So, these are the numbers of complaints received but these do not include the resolution code. So, with those types of complaints, we process the data, educate the reporters accordingly and usually close the complaint with a terminated registrar resolve code. But, of course, we provide the information about the current situation about the failing registrar and its possible termination or upcoming termination. And, yeah, so everything would be reflected in the closure codes that we use.

KEIRON TOBIN: Perfect. Thank you.

ROGER CARNEY: All right. Great. Thanks. Owen, please go ahead.

OWEN SMIGELSKI: Thanks, Roger. Thanks, Holida, for coming to present this. I do appreciate seeing the metrics. I was wondering if it's possible for us on the team or at least the public in general to see the breakdown of these numbers. I know the numbers are presented on icann.org and I still do periodically stalk those to see what's going on. But it would be good to have this sheet where it's all together as opposed to having to go through the various months of metrics that are on the compliance reporting page there.

And then also want to kind of follow up on what Keiron was asking there. The reason why I think they see a lot more increased complaints with regards to a registrant failures, it's not necessarily that many complaints after a registrar's terminated that you see it but it's kind of more of the Canary in a coal mine when a registrar is starting to fail or having problems, you start to see a lot more people wanting to transfer out. And that was certainly the case and what happened last year when people couldn't access, their domains weren't working and couldn't get out so ICANN—I feel sorry for my former colleagues there because processing 800 complaints a month for transfers is something like four or five times the normal volume and those are pretty tedious complaints, especially when you don't have access to WHOIS data as well,

too. So, I think that's why it's kind of skewing so prior to that, the numbers look a little bit better.

But I guess one thing I would kind of want to throw out there, why I wanted to see this—maybe ask Holida's feedback—is, I know when the Temp Spec and GDPR came into place, there was an increase in WHOIS inaccuracy tickets, a lot from registrants stating, "Hey, that's not me anymore. How come I can't see my registration data in there?" I'm wondering if that led also to an increase in change of registrant, the COR complaints, people saying like, "Hey, this was changed without my permission" or does it appear to have not really had an impact on that? Thanks.

HOLIDA YANIK: Thanks for the question, Owen. As you already know about our internal procedures. As I said, in the Kayako system, we've been using the Kayako ticketing system when the GDPR came into force and we started enforcing the temporary specification. And unfortunately, we were not able to capture the data regarding misfiled complaints like complaints alleging that there was a COR and wanted to change the registration data because the reporter did not understand that the domain name is still with them but the data is redacted.

So, I will repeat myself again. So, the metrics regarding misfiled complaints, we started to gather beginning from the launch of the NSp. But to gather that data you are asking about, unfortunately we need to be making a manual investigation of all the complaints previously, but that seems impossible. Does that answer your question?

OWEN SMIGELSKI: Yes, it does. Thanks, Holida. I appreciate it. And then also we'd like to see the actual spreadsheet even if it's read only or something like that so we can think about the numbers ourselves.

HOLIDA YANIK: And I see your question again regarding the older data regarding transfer complaints. I believe that ICANN contractual compliance provided a transfer-related metrics for the period from 2012 to 2018 in inter-registrar transfer policy, IRTP status report, if that can help.

OWEN SMIGELSKI: Great. Thanks again. I think that is useful to look at that report as well. Theo, please go ahead.

THEO GEURTS: Yeah. Thanks and great to see these numbers. This is excellent. So, I would remind everybody that this is related to the amount of transfer complaints which is something completely different than actually domain theft or domain name hijack that is not represented in these numbers as far as I can see. Though it is interesting to observe that pre-GDPR and post GDPR, the number of average complaints dropped 100 complaints a month. That's interesting fact to see that post GDPR, the numbers were actually on an average with 100 complaints lower and kept going strong. That's interesting to see. It's also interesting to see that the [ones where the] court order went up. But like I said, this gives us a fair

amount of information about the number of complaints but it doesn't drill on the domain theft issues. Thanks.

ROGER CARNEY: Thanks, Theo. Okay. Well, good. And if people aren't watching chat, I just noticed—and Theo kind of just touched on it—yeah, I think we're fortunate in a way that complaints fortunately for us are extremely low compared to the volume of transfers that do occur. I think that taken in the scope of the overall transfer, yes, the complaints are low but, obviously, we can always improve on items here and there so I think that's the goal. But yes, it's fortunate for us, we have a good transfer process in place, it appears. So, okay. I think we can move on from the numbers then. And again, if anybody else has any questions that pop up or anything, please send me the list and we can get them answered there as well.

All right. So, let's move on to the AuthInfo discussion that we have been having for a few weeks now. And just to jump on maybe something early here is it sounds like we may have our first possible recommendation coming out of the group, and that being a definition or a settling on calling it the transfer authorization code. So please, people, noodle on that and if that's something we'll continue to push and think about. So that probably is one of our first recommendations, is to use that terminology moving forward when we're discussing these things.

Last time we met at ICANN, we had started just on b2, we just introduced it, I believe and kind of left it for people to think about over the last two weeks. Again, I think we can jump in on b2 and this is probably what I would consider one of the lesser agreed

upon things that's been talked about. So, I think that the discussion here will be good.

And again, I'll just read the question itself. The registrar is currently the authoritative holder of the AuthInfo code. Should this be maintained or should the registry or authoritative AuthInfo holder, what reasons should be one, a registrar, registry have it, what's better? Thoughts from everyone. Okay. So, I'll kind of stir the pot here and say I think that the registry should be the authoritative holder. Any registries say that they don't want it to be that? Keiron, please go ahead.

KEIRON TOBIN: Yeah. I think I agree, Roger. I think the registry should definitely be the definitive but the registrar should also have that as well. But I think at the top part, that should be the registry as the holder of it.

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

JIM GALVIN: Thanks, Roger. I guess the question that I would ask is, what do we mean by authoritative holder as part of how to answer this question? So, the way I think about it from a security point of view, one looks at these things and you want to scope and tightly contain your security properties. I'm going to frame it in that way for the moment here. So, what that means to me in terms of the AuthInfo code is, it should only exist at the registrar or more importantly, it should only exist when it's needed, is a way to think

about it. And to the extent that it should only exist when it's needed, then obviously the registrant has a relationship with the registrar. The registrar would cause one to come into existence and give it to the registrant then to use. And there's probably some rules around all of that that have yet to be talked about.

So, in that sense, there's no real storage of an AuthInfo code—there's no real storage of the transfer authorization code—the TAC—unless it's being used. So, storage and the authoritative holder are very tightly scoped and they're tightly scoped to the actual action and act of transfer. And so, that's my real question in all of this is, is how broad is the scope of the problem we're trying to solve with this question. Thanks.

ROGER CARNEY: Thanks, Jim. And I think it's a really good point that you bring up. And I think some of the probably any disagreement would be clarified by setting that scope correctly. And I think that b2 is the authoritative holder may be better worded as maybe the manager of the AuthInfo code, who should be the manager of the AuthInfo code. I think that's what this was trying to get to. Kristian. Please go ahead.

KRISTIAN ØRMEN: Thank you. So, I'm just thinking out loud and maybe sometimes my English is not good enough for the word picking, but in my mind, the registrant owns the auth code. I, as a registrar, set the auth code in the current system in the registry and give that to the registrant and the registrant is basically the owner. And I'm

guessing or maybe hoping that the registry probably hash it in some ways so they don't know what the auth ID is either. And personally, I would say, I don't even need to save the auth ID because I can give it directly to the registrant and I don't need it myself. I need it as a registrar from the registrant to transfer in a domain and I handle the auth code by setting it at the registry and giving it to the registrant but the registrant is the holder of the auth code in my mind. Thank you.

ROGER CARNEY: Thanks, Kristian. I think Jim was kind of going down that same path as what you were thinking there, is the registry obviously has to hold it for a period of time. At a minimum, the registry has to have it for some time once the registrar sets it. And as to your point, Kristian, maybe the registrar doesn't even keep it. They pass it along and then they're done with it and there's no record of it at the registrar anymore. And that is an idea that could go down, we could use as that path. Again, to me, I think the discussion is, who manages that process? And as Kristian mentioned, really, does the registrant own the auth code? And if so, who manages that process? And Kristian described today, obviously, it's managed mostly by the registrar who creates it and provides it and then the registry actually just enforces it once they get it. So, again, continued discussion on this path as to, okay, once the registry gets it, then what happens and so forth and so on. So, I think that that's what this question is trying to get to. Barbara, please go ahead.

BARBARA KNIGHT: Thank you. So, I think this is actually a good discussion. I think by default, I think that the registry operator ends up being authoritative from the standpoint that if an AuthInfo code comes in with a transfer command that does not match what's in the registry's records, that's going to fail. That being said, I think that it's—the information that the registry has is really only as good as what is passed to them by the registrars. So, I think by virtue of the fact that the registrars have the relationship with the registrants, where all of that falls out relative to who is actually setting the AuthInfo code, I think it ends up being almost the registrars that have to kind of manage that if you will, to pass that into the registry database in order for it to be able to work as designed. So, I think as I said, by default the registries almost become authoritative because if it doesn't match what the registrars are passing, it's going to fail but I don't necessarily think that we are the manager of that data. Thank you.

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

THEO GEURTS: Yeah, thanks. And I was actually thinking along the same way as Barbara was doing, I mean, yes, in that sense, when it comes to the check if the auth code is still valid or correct, that should be on the part of the registry. You want to have that check there. When it comes to the security of the auth code, either you pass it along like Kristian mentioned which is perhaps a good idea, I didn't hear it yet in that manner, but yeah, that could be a very good way to have it secured. But in general, when it comes to security, either

be it the auth code or the personal data of the registrant, we already have a high standards which we need to comply with either it be GDPR or a cybersecurity act regardless in which country you're from, if it's applicable, you need to be compliant with that. So, either be it a personal info of a registrant or the auth code, it needs to be very well protected by the registrar if the registrar stores that authorization code in its database. Thanks.

ROGER CARNEY: Great. Thanks, Theo. Sorry, I didn't mention it earlier and luckily Emily caught me on it and posted it to the chat. The working document is posted as well so if you guys want to follow through on the working document, Emily provided a link just a couple messages ago so grab that. And I would say that there's a post in chat as well about TTL and I don't know if we need to discuss that here or not. It obviously is going to bear on a management aspect of the auth code so just something to think about. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. Now that you bring up TTL and, well, what do we put in the [authority] holder role because, for example, I would think that it would be the best if the registry would handle a TTL on the auth code. So, if we put the [authority] holder of the auth code in who's responsible for doing things, invalidate after days and so on, then I would like to put more roles on the registry. But I don't know how important the actual name [authority] holder is, yeah. But personally, I think the registry should handle a TTL on the auth

code. I don't see why you would put that on the registrant or the registrar.

ROGER CARNEY: Okay. Thanks, Kristian. Keiron, please. Go ahead.

KEIRON TOBIN: Thank you. I think this is probably a question for Brian or anyone who's in that industry, just to kind of, for me to understand a little more. In terms of like when a law enforcement requests comes through or whether a domain has been terminated at its current registrar, how do you work in terms of transferring that domain to the different party? Is there an auth code that's involved in that or is it just the registry backend that kind of completes that? I'm just trying to understand that process a little more. Yeah, I mean, I don't want to put you on the spot, Brian. Or if anyone else knows.

ROGER CARNEY: Okay. Maybe something to post to list Keiron, see if we can get some discussion on it.

KEIRON TOBIN: Thank you.

ROGER CARNEY: Yep. You bet. All right, Tom, please go ahead.

THOMAS KELLER: Thank you, Roger. Yeah, I think personally, this really comes from the discussion we haven't really had whether auth code or transfer register code, however you want to call it now is having a TTL and how the whole process looks like. So, I assumed as a whole—answering this question could be a bit premature at the time being where we haven't really had a look at the holistic process and whether we want to change the current setting or whether not. I think that's a discussion we should be having sooner or later to say, "Okay, where does it start? How is the transfer started? What credentials do you need? What security measures are in place before we actually come down to deciding on who's responsible for what?" Thank you.

ROGER CARNEY: Great. Thanks, Tom. Yeah, and I think one of the good things that this has brought up is maybe, the authoritative holder maybe is not the correct terminology we should be using. Obviously, we've identified at least three interested parties here, the registrant actually being the owner possibly, being the owner of that data which seems to make sense. But the registrar having a management capability somewhere. And I think the registry having at least the decision-making process of, if the supplied transfer authorization code is valid or not to what it knows. So, I think that maybe, again, the authoritative holder, maybe beginning to split out into more definitive roles here. Keiron and Tom, your hands are still up. Is that something you want to bring? Okay. Thank you. Jim, please go ahead.

JIM GALVIN: Thanks, Roger. I want to agree with one thing that Thomas said, actually agree with all that he said but I want to highlight something that he said about it might be too soon to fully answer these four questions here and offer some just some concrete data points for us to be thinking about in this space. On the question of storage, if we move in the direction of truly implementing one-time passwords and using the TAC in that form, okay, then there is no storage really. There's a little bit of storage in the sense that the registry has to have a copy to compare to what comes from the gaining registrar, okay. But there doesn't have to be any storage. It's possible to build out the system in such a way that it's a one-time password. You generate it, you hand it to the registrant, stick it in the registry but there's otherwise no storage.

Now, you get to the question of how long does it even get temporarily stored, if you will, in the registry. And the question that I would give to the group to think about is, as a registrar, what kind of flexibility do you want in this space, right? So, one question to ask is, do you want—if you set up the idea that the registry has to enforce a particular rule here, is it going to be a uniform rule or is it going to be a rule where the registrar has to set it? So, with the AuthInfo code, you have to decide how long you want it valid for and you've got to tell the registry that too so that they can then act on that.

Well, I would question how that's much different than the registrar knowing for itself what it wants the lifetime to be and it just sets it to zero when it doesn't want it to be valid anymore. Okay. So, you can either have complete control for whatever's appropriate for your own business practices or you can limit yourself to some fixed

value with the registry or you still have to tell the registry what you want and they have to have maximum flexibility to support whatever you might say.

And I'm not sure that you want to go down that path, which brings me to the last question of, right now today, registries have a very tightly scoped responsibility in this transfer process. They receive an AuthInfo code and they simply check to make sure they got the same code from the gaining registrar when that happens. If you really want to go down the path of expanding the scope of responsibility of a registry, then as a registry, the question that I would ask is, what is the benefit of that? Okay. And that's where you get into this question three down here, what really are the advantages of doing that? What do you hope to gain by the registry having more responsibility in this transfer process? What is the purpose of moving responsibility that is entirely within the registrars to the registry? And I would ask that question and ask for some careful consideration of where we're trying to go with that.

So, bringing this back around to where I started, I think Thomas had it right. It might be a little soon to definitively answer these questions. There were some interesting details to be considered which we'll be better able to answer once we have a better, fuller picture of what the process is going to look like overall. Thanks.

ROGER CARNEY: Thanks, Jim. Yeah, and I'd like to add to that. I think that obviously this is great for discussion and it'll lead to better discussion as we continue along here. But I think all these questions and answers will be better framed once we get through all the issues of the auth

code itself and then we can come back and look on those. It's just a good way to start marking your way down these concepts. So I think that Jim's question is valid is, if you want the registry to maintain all of this information, what's the advantage over the registrar having that management ability versus the registry having that management ability. So, I think Jim's thrown that out on the floor for all you registrars. Tom, please go ahead.

THOMAS KELLER: Yeah. Well, even though I want to repeat your last thing. It's a bit early but I think that the main benefit and I know the registries don't like to hear that but it would be a uniform management of it and it would be enforcement. If you let it run by 2000 registrars, it's very unlikely that they really adhere to the same process and they will always find some kind of an excuse why they'd done it differently and why they deviate from it because of the terms and conditions wherever they stay. But if you have it at the registry level, as a policy, then this is the same for all registries across all gTLDs. And I think that's a very big benefit for the registrars and especially for the registrants at the end of the day.

ROGER CARNEY: Okay. Good. Thanks, Tom. Obviously, the registry doing it, we only have a few hundred registries less than that backend that would be enforcing something like this, so the idea of standardizing or simply simplifying it to a least common denominator makes sense. Registries' thoughts on that? Anyone, really thoughts? Jim, please go ahead.

JIM GALVIN: Thanks, Roger. I do understand that comment about the benefit. If anything maybe today in today's world, the scale of the management problem changes if you put it on registries rather than registrars, but it seems to me that in either case, you have to create rules and procedures that have to be followed. It doesn't really change the problem. Either the registries have to enforce the rules and procedures or the registrars have to enforce them and either way ICANN compliance has to deal with it. So, it's not immediately obvious to me that that is a criterion that we can use to decide whether it properly belongs at registries or registrars. I'm looking more for a defined business process or defined security benefit for moving responsibilities from a registrar to a registry. In other words, changing the way that we do it today in some significant way. Thanks.

ROGER CARNEY: Okay. Thanks, Jim. Tom, please go ahead.

THOMAS KELLER: That seems to be a very interesting discussion. So, I would like to argue this is having the security benefit of having a neutral party managing the process. And in both cases of winning or losing registrar, they stand to win and lose nothing. They're not a neutral and they will do an act on the information they have from the customer or maybe act in bad faith. This is not the case for the registry because the registry as long as the name is maintained in the database, they don't really care. So, I think this adds a lot from

a security perspective and it makes the whole process more easier and more transparent at the end of the day, which is good again for the end-user because if there's a source of reliability which will not be there and will not be the case if only registrars are running the process. And we already see that with most of the ccTLDs having already introduced such a process that it's much easier and that certain disputes can even be solved at a registry level where you can say, "Okay, how can I get that data if my registrar just went bankrupt or whatever." So, I think this is adding a lot in terms of security.

ROGER CARNEY: Okay. Thanks, Tom. So, I think I'll throw it out there and we don't have to continue on it but I'll throw it out there. But to Jim's point and to Tom's point here, I guess, is trying to come together there in the middle of where is the, I guess, not necessarily the enforcement because the enforcement, as Jim mentioned, will be policy-driven enforcement. But where is the flexibility best managed at? Is it at the business side on the registrar side or is it on the registry side of managing it for standardization and things along that line? And again, as Jim mentioned, standards can still be enforced through policy and that becomes an ICANN issue. But I guess that's the big difference here to me is, is it a business model? Maybe some registrars want tighter control over their authorization codes or some that don't really care. If it's requested, they give it and then it's gone. Jim, please go ahead.

JIM GALVIN: Yeah, thanks, Roger. I guess the question that I have—and we can take this conversation as far as you want for today, Roger—is, I'm really trying to understand the improved security that Thomas is highlighting. I'm all for improved security, but I think the thing that occurs to me is either way, however, this thing comes out on the issue that we're talking about, the registrar is kind of in the middle. The registry, whether they create the code or don't create the code, it still has to go through the registrar to the registrant.

So, I'm not seeing any improved security in that sense. If you're worried about whether a registrar could implement it properly and a registry could implement it properly, well, that seems like it's taking us into a conversation of who's more likely to be a good player, a registry or a registrar? And I'm not sure I want to get into that comparison. I don't feel good about that at all. I think we're all equally likely to be good players or bad players. So, it feels like that's even going down the path of suggesting that registries are somehow going to be riding herd on registrars in some way. And yeah, speaking as a registry, I know I don't want that job. So, that's just doesn't feel good to me. Now, I may be missing something else along the way there and so I'd appreciate some more discussion about the real advantages and whether we do that now or at some other time. That's the question that I still have in my mind. Thanks.

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

THOMAS KELLER: Thank you, Roger. So, from my point of view, I think the main difference is that you have a standardized way of an [audit trail.] This can be done and reviewed very easily with the registry. It will be much more complicated with the registrar because the registrar might have the benefit of actually changing it. The registry, if they haven't written the system off and the code has been changed by both registrar, for what reason, whatever the flexibility in the system is, it can be easily proved and that's a big difference. You have one reliable source of reference.

And you don't need to get into judging who is a good registrar or a bad registrar. All you have to do is showcasing what happened in the system and this basically comes in for free, right? Because it's in the system and it's locked and then what you do with the current transaction as it stands. So, I think this would be a big security improvement for registrant, have the security that there's one final source of information and not two, of the two that may or may not keep correct records. You can always say, okay, but this comes down to policy and the registrars have to do it as well but it's just more likely if it's done by a neutral party that has no special benefit in the whole discussion.

But yeah, we haven't even decided whether we want to go for a TTL, any extended measures, so I think it's good for now at least from my point of view of this discussion, maybe we move on to something else because I think otherwise, we get stuck here for the rest of the day.

ROGER CARNEY: Thanks, Tom. And I agree. I think this discussion is great. I don't think we're going to solve this issue on this call here. But I'm hoping everybody gets a general understanding of the issues on one side or the other and be able to walk that line over the next week and think about it. So I love this discussion. Thanks. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. I think the whole discussion have a couple of different parts to it like, for example, the TTL is one thing and who should be the manager of that if we decide to do a TTL. That could both be the registrar, the registry, and if the registrar have to do it, they basically when it runs out have to set a new auth key and that could fail. So, in my mind, that would be more secure if the registry takes care of the TTL if we decide to do one. For the actual like who makes the auth code, for me it's not important if it's the registrant, the registrar, the registry, we just need some minimum requirements to be sure that the actual code is secure enough so it's not like 123 or something like that.

And personally, I would prefer basically no one to have it except the registrant. If we give the auth code to the registry, they could hash it in their system so they don't even have it but they have a hash that they can check the code they get from the gaining registrar that the code is correct and by that, they don't even need to hold the auth code in their systems. So, it's all about the security and who's the holder of different things. I don't think we can say registry is the holder of everything or registrar is holder of everything. We need to look at each specific process and say who's responsible. Thank you.

ROGER CARNEY: Great. Thanks, Kristian. And it's a good security point that you make is, the auth code can be generated. The registry can hash it so they no longer have it. They've never had it if that's the case. The registry, registrar, obviously, temporarily has it and then passes it to the registrant. And really the registrant is the only one that stores it and again "stores" in air quotes there, and the registrar could actually get rid of it, not have to store it on their side. So, you are enhancing that security mechanism where really the registrant is the only one that has it and that's their proof that they have that ability to do what they need to with it. So, Theo, please go ahead.

THEO GEURTS: Yeah. Thanks. So, when it comes to the TTL of it, that might be something we can discuss later on. Sounds like a good idea. Hashing of AuthInfo codes could be a good idea. I don't know if the current situation is so unsafe that it should warrant such measures, but we could definitely look into that.

The main point I wanted to highlight here is, I keep hearing the word a registrant having access to the authorization code. That is fine with me. But as a wholesale registrar, I rely on an entire business model that the reseller does all the work for the registrant and is authorized by the registrant and will need access to the auth code. And if he has to go back for every single transfer, thousands a day, that is going to be a nightmare for those guys. I mean that is something that cannot happen, so there must be always sort of—that we need to strike a balance here when it comes to workability

around all the business models that are out there. And reseller model is one of those models that a reseller does a lot of work for the registrant and they need to have access to it. And I think the entire security of such authorization codes is in my case—that's on me. I mean, I need to make this as secure as possible either way. But so let's keep that in mind while we move along. Thanks.

ROGER CARNEY: Thanks, Theo, and thanks for bringing up the different business models just to make everybody, again, think about those different circumstances where it may apply in your reseller or corporate domains or something like that. You've got to be thinking about all those scenarios where that will work and where it won't work. So thanks, Theo. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. I just wanted to agree with Theo that we definitely need to rethink to include the reseller in the model. But also with that, we need to be open to different business model but we can at least still say that the registry and the registrar does not need to store the auth ID. Like the registry can store it or will have to store it at least hashed, but the registrar doesn't have to store it. The reseller doesn't have to store it. They can send it to the registrant. But I think it would be good to be open in the policy to say that the registrar can store it.

ROGER CARNEY: Great. Thanks, Kristian. And I think that obviously we can come to some kind of temporary, I mean, when you talk about data storage,

people talk about it being written hard, or temporary which is still written somewhere but obviously it's not there for any use, I guess, long-term use. So, I think there's a line there that can be drawn as to what is temporary, what does that mean to be temporary? Thanks.

Okay. Well, good. Again, great discussion and I think that's what we want to do on all these charter questions for the transfer authorization code, is to coalesce around each time we go through each one of these, we're thinking about the previous ones and that'll give us a more cohesive view of it. So I think that's great. Okay. I think that we can call that on b2 for now. Again, we're not done with it. We'll come back to it, we'll review it as we go through all of them but we'll hit on topics, all the future ones here we'll hit on topics coming back to it.

Okay. I think, let's go ahead and move on to b3 and we'll just—I think again, like last time, we'll just introduce it and kind of leave it there and let everybody think about it for the next week or so. So, I'll just go ahead and read it off. This is in the provisioning of the transfer authorization code. So the transfer policy currently requires registrars to provide the AuthInfo code to the registrant within five calendar days of the request. The question is, is this an appropriate SLA for the registrars' provision of the AuthInfo code, or does it need to be updated? Again, we don't need to get into a substantive discussion here. I just want to introduce it. The note here is the CPH TechOps group thought that the five days seemed to be reasonable to keep. Again, we don't need to get in too deep here. I just want to introduce it so that everybody has some time to think about it. Jim, please go ahead.

JIM GALVIN: So, thanks, Roger. I'll just offer something for folks to think about, registrars specifically to think about. I think that there's an opportunity here. At one time early in our discussions, the idea, the concept was at least opened up about more instantaneous transfers and doing more near real time and allowing all of that to occur. And I make the following observation. If we truly move the TAC towards more of a one-time password kind of model, as a concept, one possibility here is that the TAC itself is just calculated on demand and there are rules about the right way to calculate it, but you sort of generate and create one on demand and then you offer it and it goes off and it comes back.

So, what that suggests is if you want the business processes to work in that way, then a five-day period during which you have to write the AuthInfo code is way overkill. Okay. I mean, at scale, there's no reason you couldn't do this in near real time. Somebody asks for it, you just provide them one, you stored it at the registry, all that can be automated, nobody has to know anything, it just sort of happens. So, just something to think about as you think about your own processes and how things work and what you really want out of your own business models, I offer that as something to consider for the group. Thanks.

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

KRISTIAN ØRMEN: I definitely think that it's important with instantaneous transfers, but we need to think in all business models. We have many, many different registrars working in different regions. Some registrars might still work with papers and would send the auth code by UPS or some strange thing or manually checking if the request is legit before giving it out. And there's so many different possibilities of business models and security mechanisms that the registrar would include. So, and we have to just consider that and be sure that the policy would not stop those business model from still working. Thank you.

ROGER CARNEY: Great. Thanks, Kristian. All right. Steinar, please go ahead.

STEINAR GRØTTERØD: I'm trying to think about this from the end-users, registrant point of view, and I actually think that the five days is also a timestamp from when the registrant is requesting the registrar or the reseller to actually get some feedback. I do understand the technicalities, and we don't need five days to create the auth code, etc., but it's some sort of a timestamps for actually I can request to have some feedback to the auth code within five days when I'm requesting this. Thank you.

ROGER CARNEY: Great. Thanks, Steinar. I think that kind of goes along with what Kristian was saying is, the possibilities are that there may be something in between there. I think, obviously, one of the goals would be to have a fairly quick transfer option but as both of you

and Kristian mentioned that there's different models that have to be handled for that. Tom, please go ahead.

THOMAS KELLER: Yeah. It really comes down to the question whether we stick with the current process or whether they're going to change. And I think if we move to a model where we may even move away from the [FOA2] which is adding an additional five days for checking and putting that in front, then the five days make complete sense. It could even be 10 days to verify a process but once it's verified, then you might have a one-time pass, whatever you want to call that and that could be close to real time transfer at that point of time. So, I think we really need to look into the process and what we want and currently, I think that reviewing a lot of the stuff under the view of this, is current process working but I think the idea—and there was endeavor the white paper was doing with the TechOps is to reinvent a bit the transfer to do it differently and not just take pieces, look at the pieces and see whether it's still fitting or not.

ROGER CARNEY: Yep. Great. Thanks, Tom. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. I think if we should make it less than five days, we should maybe word it in a way that if a manual process is needed and then X amount of days, but it should then be business days instead of calendar days, if we make it less than five. Thank you.

ROGER CARNEY: Thanks, Kristian. And I think one of the things that Tom was trying to allude to is, once the authorization code has been created and given to the registrant, then the technical as quick as possible make sense but maybe there's a process that leads up to the release of that authorization code that may be zero to, as Tom mentioned, maybe 10 days, whenever that is. Thanks. Theo, please go ahead.

THEO GEURTS: Yeah. I think it's not a matter of how fast we can generate a code and deliver it to the registrant. I think most of our processes for most registrars, this is an instant process for most of them. It's either you request the auth code and you get it by email or by another delivery mechanism. Email is not the best way to do that. But in the Netherlands, we have those instant transfers for .nl. Most of the registrants have access to their auth code. So, usually this thing goes really, really fast. In the entire five calendar days, I don't really see the use of it on when you need to refuse the [inaudible]. Who does that? I mean, and it's a serious question. I mean, just how many transfers are going on, on a yearly basis? Almost five million. There are still registrars out there that do manual review of that stuff? But that's something we can go back to next time. Thanks.

ROGER CARNEY: Thanks, Theo. I'll give Kristian the last word and then we'll try to wrap it up. Go ahead, Kristian.

KRISTIAN ØRMEN: I can quickly answer that and say that in last data, we have a list of block domains that we would review before giving out the auth ID. It could be either be on historical abuse or it could be on very high value consumers. But normally with consumer just goes into the interface, get the auth ID. But if they are on the blocklist, we manually review it first.

ROGER CARNEY: Great. Thanks, Kristian. Okay. Again, great discussion again. We'll start back up on this next week and talk about this. Just everybody start getting their thoughts around it and seeing where we can go from there but we'll bring it up next week. So, I will turn this back over to staff to close us out.

EMILY BARABAS: Hi Andrea. Do you mind closing us out? Thanks.

ANDREA GLANDON: No. I was just going to ask if there's anything else you needed to do. Okay. Thank you. This concludes today's conference call. Please remember to disconnect all lines and have a wonderful rest of your day.

ROGER CARNEY: Thanks…

[END OF TRANSCRIPT]