ICANN71 | Virtual Policy Forum – GNSO Transfer Policy Review PDP WG
Wednesday, June 16, 2021 – 14:30 to 16:00 CEST

JULIE BISLAND: Hello and welcome to the GNSO Transfer Policy Review PDP Working Group meeting.

Please note that this session is being recorded and follows the ICANN expected standards of behavior. During this session, questions or comments submitted in chat will only be read aloud if put in the proper form, as noted in the chat. Questions and comments will be read aloud during the time set by the time set by the Chair or moderator of this session. If you would like to ask your question or make your comment verbally, please raise your hand. When called upon, kindly unmute your microphone and take the floor. Please state your name for the record and speak clearly and a reasonable pace, and please mute your microphone when you're done speaking. To view on the live transcription, click on the Closed Caption button in the Zoom toolbar.

With that, I will hand the floor over to Roger Carney. Thank you.

ROGER CARNEY: Thanks, Julie. Welcome, everyone. It's been just a little more than a week since our last meeting. It probably seems a little longer for those that have been attending ICANN71 meetings the last few days. But let's go ahead and get started.

Just a few things to kick off. Just a reminder that the homework for the SO/AC letter is out there. We need comments back by June 24th. Again,

we plan on discussing it at the June 29th meeting and finalizing it so we can hopefully get it sent out by the end of the month.

Also, I just wanted to give everybody a heads up that staff has started working on a definitions document for us. It's not so much for anything new, really. It's more to document and pull in the definitions that we'll be using just so everybody has the same baseline going forward from there.

I think that was about all for any administrative items. I think we'll go ahead and kick off and jump into our agenda here. We can move on to About the PDP. I will turn this over to staff. Thanks, Emily.

EMILY BARABAS: Thanks, Roger. Hi, everyone. This is Emily Barabas from staff. So, for those of us who are joining from outside the working group, welcome. We're just going to take a couple of minutes to talk about what this group is about so that you can follow discussion a little bit better.

So the transfer policy is an ICANN consensus policy governing procedures and requirements for registrants to transfer their domain names from one registrar to another. This was originally called the Inter-Registrar Transfer Policy or IRTP for short because this is ICANN and we love our acronyms. The IRTP first went into effect in 2004. There was one policy review that took place before this PDP, and that took place shortly after implementation.

Just a little bit about the PDP. Mission and scope. The PDP is intended to conduct a holistic review of the transfer policy to determine if

changes to the policy are needed to improve the ease, security, and efficacy of inter-registrar and inter-registrant transfers. The PDP is organized into two phases with a single charter, and there are a total of eight topics in the PDP over those phases. Phase 1 is in two parts, A and B. The PDP just got started last month with Phase 1A. So that's where we are right now. There are two topics within Phase 1A: form of authorization and auth-info codes. We'll talk a little bit more about that, but we're going to be focusing today, for half of the session, on the topic of auth-info codes.

In terms of where we are right now, the working group did some initial setup tasks and then conducted a high-level review of the charter questions and topic areas that will be covered and is now beginning substantive deliberations on the first topic, which is auth-info codes.

In terms of participation, members are limited in this working group to representatives that are designated by SO/AC/SG/C's, but anyone is welcome to sign up to observe at any time.

So that is a very brief overview.

The next thing we're going to do is dive into the working group's discussion. The first topic is going to be about policy goals. I'll do a brief intro and then hand it over to Roger to facilitate the discussion.

So there were a series of goals that were used to guide the work of the IRTP working groups, which was a series of policy development process working groups previously doing work on this topic of transfer policy. So we thought maybe to start the discussion about principles guiding

the upcoming work by first looking at the principles that guided previous work and see if some of those are still applicable, if they need to be modified. But that sort of gives a little bit of a starting point. And those goals are outlined in the transfer policy status report, which was published prior to this PDP that gives some data and statistics to help guide the work that we're doing. These goals listed here on this slide were first introduced in a 2005 staff paper that's linked from these slides.

So I'm just going to read through them, and then we're going to move over to another format for the brainstorm discussion. The first one was to enable registered name holders to move their domain names to a new provider, thereby increasing consumer choice and competition. The second goal was to ensure the IRTP includes sufficient protections to prevent fraudulent domain name transfers and domain name hijacking. The third goal was to clarify the language of the IRTP so that ICANN-accredited registrars consistently interpret and apply the policy. And the fourth goal was to clarify language and visibility of the transfer dispute resolution policy so that providers and panelists consistently interpret and apply the policy.

The questions we'll be discussing, again, are, are these goals still applicable and are additional goals still needed? And the objective here is, by setting goals to guide the work, that that will help the question of, what is the problem we're trying to solve in the recommendations that the PDP puts forward?

So what I'm going to do now is move us over to something called a Jamboard. What I'm going to ask everyone in the group to do is to follow this link. What you'll see here looks sort of like a … one moment. Let me reshare it. Okay. Hopefully, everyone can see what looks like a board full of Post-It notes.

At the top of your screen, you'll see a series of green Post-It notes. These are the policy goals that were used for the previous IRTP. Below that, just to start the conversation and prepopulate some of this board, we also have a series of principles that were used to guide the work of the Contracted Party House Technical Operations Group in some of the work that they did and produced a 2018 paper with some recommendations regarding changes to transfer policy and associated processes.

So I'm not going to read through all of those now, but I think we probably have people on this call who can speak to those and who would potentially like to advocate for adopting some of those principles. So they're here for discussion and further consideration.

Then, if folks have other thoughts about goals that they think should guide the work of this working group, you'll see some blue and pink sticky notes at the bottom of this page. All you need to do once you're logged in here is to just double-click on one and you can add text to it. Or, if there's not a blank sticky note available, there's a little icon here on the leftmost menu. It's the fourth icon. It looks like a sticky note. You can just click on that and it will create a new sticky note and you can

add text there. Feel free to ask any questions in the chat about how to use it, but hopefully that gives a little bit of an introduction.

Are there any questions before I hand it over to Roger to start the discussion about goals?

Okay. Seeing none so far, I hope that that's clear. Roger, I will pass it back to you to start up the discussion. Thanks.

ROGER CARNEY: Great. Thanks, Emily. All right. This hopefully is a good tool to get us thinking and get it documented as we go through this. When we started planning for this session, we had talked about developing some of these principles/goals for the whole PDP itself, and it was interesting that Jim took us down this path last week, actually, coming up with some of the more, I would say, not as high-level as this but trying to develop those concepts of, what are we trying to achieve? And I think that that led really well into this. Again, we talked a little bit last week about some of those things, but we kind of want to take a smaller step back and not specifically talk about the transfer authorization code but more holistically across the PDP, I would say, as to what our goals [are], again, looking at historical principles and goals. Do they still apply, do we need to update them at all? Do we need to add (probably more importantly)?—anything that we don't see here. So I think we can start with just examining, as Emily noted, the items from the original IRTP here in green and the ones that Emily read off, basically. Are these goals still applicable? And do we need to add anything to them?

So I think that I'll [allow] everybody just to take a minute or two to read through here and see if they think that they're still applicable. If not, come online and say what your thoughts are on those. And if you think they are still applicable, it would be good to hear as well so we can get that positive reinforcement back that this still makes sense to continue on. So I'll give everybody a minute or so just to read through those top green ones, and then we'll get started on those, and then we'll move down to the tech op principles after we have a discussion on the top ones. So please take some time and read those. Julie will make sure that we get back here in about a minute.

SARAH WYLD: Hey, Roger, I have a question.

ROGER CARNEY: Yeah, go ahead, please.

SARAH WYLD: Thank you. Hi. This is Sarah from the registrar team. Can you hear me okay?

ROGER CARNEY: I can. You sound good.

SARAH WYLD: Excellent. Okay. So this second goal mentions both fraudulent domain name transfers and domain name hijacking. I'm just curious if those are

different things because, if they're the same thing, then the redundancy might be confusing. And if they're different, maybe we should explain that somewhere. Thank you.

ROGER CARNEY: Thanks, Sarah. I'll open that up for anybody that can talk to anything that's non-hijacking as a fraudulent transfer. Anybody with thoughts on those?

Jim, please go ahead.

JIM GALVIN: I'm sorry, Roger. I think I might have lost something in that question. Could you restate that? The question.

ROGER CARNEY: You bet. So Sarah is asking if there's some redundancy in that second green card with preventing fraudulent domain name transfers and preventing domain name hijacking. Is that redundant or is there some fraudulent transfers that are not domain name hijacking? Does that clear that up, Jim?

JIM GALVIN: Yes. Thank you.

ROGER CARNEY: Okay. Steve, please go ahead.

STEVE CROCKER: Thank you. So two things. So the first and the second green things—the one enabling name holders to move their domains, and the other to ensure that they prevent fraudulence—are the opposite sides of the coin in terms of making good things happening and preventing bad things from happening. So those are both good.

There's a third, more subtle element, which is to do both of those efficiently so that you don't have unnecessary pain in terms of cost or delay and, at the same time, without increasing the number of errors. That is, you don't want to prevent proper transfers from happening, and you don't want to facilitate bad transfers. And you also want to do both those at reasonable cost and time delay and so forth for everybody. So that's my first point.

The second one is responding to the point in the chat about the pink sticky there: "DNSSEC transfer has a role in mitigating domain name hijacking." That's not anything I would say. I've raised a point with respect to transfers that, in the process of transferring from one registrar to another, if that registrar is also providing the DNS service and, most particularly, if they're provided assigned DNS service [(]that is[,] DNSSEC-signed[)]—then, almost always, you have to transfer the domain service as you transfer the registration. And that's a tricky process to do if you don't want to have any disruption in the service. And it requires cooperation from the losing registrar/DNS provider. So that's related to all of the words in that sticky but is an entirely separate point.

ROGER CARNEY: Great. Thanks, Steve. Yeah, to your point on the first item that you talked about of trying to make it efficient, I think that maybe we can come up with something along that line. You identified both the good and bad there, but, yeah, somewhere, making that, as you said, efficient but cost-effective and user-friendly as well.

STEVE CROCKER: And I see that Sarah has responded to the point I'm making. She says the first sticky does say "enabling the transfer," but it doesn't say anything about how long. So, for example, the discussion that we're having about if 60 days is the right amount of time to put a restriction on further transactions and so forth is related to the kind of third dimension that I'm talking about here.

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

THEO GEURTS: Thanks. When I'm looking at this and "Should the IRTP include sufficient protections?" I think that is a good way to go about to make sure that we have something along the lines that there should be sufficient protections on a registrar level and on a registry level.

What I would caution about or be vigilant about is that we don't go down a path to create additional protections on a policy level. Those are not required and would be very overly restrictive to all kinds of

business models and, usually, they don't solve anything also along the way.

So if there's language there where we could put in, "Okay, a registrar should/a registry should have protective measures in place," great, but don't go beyond that. Thanks.

ROGER CARNEY: Great. Thanks, Theo.

Okay. I see … I'll just throw this out there, as Sarah brought it up. Maybe I'll throw out a possible fraudulent that's not hijacking. The only thing that came to mind was maybe an aftermarket sale that occurred that shouldn't have occurred. Again, I'm stretching here because I'm trying to find a fit here. But it's the only thing I could come up with.

But in support[, Sarah Steiner] also mentioned maybe just removing domain hijacking, as that is a fraudulent domain transfer. Yeah, okay. And I think it seems like there's agreement there, that maybe that's not needed. Okay. A lot of agreement there. Okay, good. So maybe we can shorten that up and maybe remove any possible confusion there.

Heh. Yes, Maxim. Yes, that'd be good.

Okay. And getting back to Steve's comment on the DNSSEC—there are several comments in chat on this new pink DNSSEC sticky note—several comments are yes, and several comments are, "Yes. Someone needs to solve the DNSSEC transfer issues, but it's not currently in our charter to

discuss." So maybe this isn't perfect here. That's what I'm seeing. So we'll have to think about that.

Steve, your hand is still up. I assume that's an old one.

Thank you. Theo, please go ahead.

THEO GEURTS: I have a question about that DNSSEC issue. Perhaps I'm not understanding the problem. We are also a registrar. We don't do hosting. We do offer, for all gTLDs and ccTLDs where DNSSEC is available, that to our resellers. Here in the Netherlands, we use DNSSEC. DNSSEC adoption is extremely high. It's over 50%, so that's pretty high. And I don't see any issues. I see all of our resells that DNSSEC enabled, and we get transfers in and out on a daily basis, and a lot of them. And I never heard anything from our staff like, "Are there any issues?" Maybe I have been asking them the wrong questions, but I don't see the issue here. At least I don't. So that would be helpful if we get some more information about it because I don't see an issue so far at the moment. Thanks.

ROGER CARNEY: Great. Thanks, Theo. And I think Steve can talk to it a little bit if we wants to, but I'll say something. If a domain has DNSSEC on it and they transfer it to a new registrar, you risk the breaking that chain of DNSSEC when it moves. People have been talking about, can you solve that in a more efficient way?

Jim, please go ahead.

JIM GALVIN: Thanks, Roger. The issue for … Well, it's not really an issue. The point for Theo … I happen to know that, in the Netherlands, the reason why he as a registrar would never see this issue is because the registry itself is intimately involved, and the particular protocol solution that they've chosen for this solves this problem of DNSSEC transfer. So the registrar is not part of it. So that's a country-code solution, and they happen to be well-cared for in that respect.

The issue with DNSSEC transfers for gTLDs, though, is the fact that the registry is not intimately involved in this process. There are a variety of reasons for that. This probably is not the right place to talk about it.

But the bottom line here is there needs to be a way for the new key DNSSEC keys being used to sign the domain in the new location to be made available in the old location. That's one. Number two, there must be continuity of service until there has been proper distribution in the Internet of those keys and of new nameservers. If you don't have both of those things, then you get loss of service. There's a variety of reasons why that is currently true in the gTLD market. I mean, it just fundamentally is true across the board. Some registrars have solved this. Some DNS providers have solved this and made arrangements and that kind of thing. But there is no uniform solution. So there becomes a window of vulnerability in terms of hijacking and such because you have to go between signed and unsigned in order to effectively make all of this issue. And that's kind of the issue.

So maybe we should have some discussion about scope here. I think that's a very appropriate discussion to have. Whether or not being able to make those key transfers in the gTLD case is within the scope of mitigation of hijacking. That's why I kind of added this stick-it there. So I appreciate all the discussion on both sides. I just would like to put it out there as a discussion that we should have. It might be best for Steve to manage all of that as our subject-matter expert here in that space. Thanks.

ROGER CARNEY: Great. Thanks, Jim. Yeah, I think the scope will play in. So I think that'll be important on this topic. Obviously, it's an important topic to solve, but are we the ones to do it?

Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. I said it earlier, but I want to say it again: the DNSSEC issue is with nameserver changes. It's not with registrar transfers. Registrar transfers mean [straight-to] process that changes the administrative body of the domain name, and it has no technical issues at all. Nameserver changes is another operation done by the registrar on behalf of the registrant. The registrar has to change their nameservers and update DS records whenever the registrant asks the registrar to. While this sometimes happens at the same time as a registrar transfer, it does not have to happen at the same time. And it is not part of the actual registrar transfer procedure. Thank you.

ROGER CARNEY: Great. Thanks, Kristian. You got a lot of support in the chat as well.

Steve, please go ahead.

STEVE CROCKER: Thank you. Sorry for the delay. I'm getting off mute. So, first of all, Jim covered the technical aspects of this very well, and it's much appreciated. I'm sensitive to the discussion here about whether or not this properly this belongs with this group and whether or not it's properly related to change of registration.

Let me try to make just two very simple points. If you're changing the name of the registrant but not changing the registrar, then the issue that we're talking about probably doesn't come up because the name service. stays the same.

The issue, however, does come up if you're moving from one registrar to another and, in that process, the existing registrar insists on giving up or not continuing with the name service. That is, if the registrar is providing name service and kind of has it bundled as no extra charge, then when you change registrars, you are necessarily being forced to also change the name service. And that's where the trouble arises because the registrant, if he wishes to have continuity in his name service, and particularly if he wishes to have continuity with his signed name service, has to get the cooperation of the existing name service operator, which is the existing registrar.

Now, Sarah asked, "Could the domain owner in that scenario not do a DNSSEC update first?" In some sense, it's still the same problem because cooperation with the existing name service operator, which is the existing registrar for the scenario we're talking about, is still required.

So it's boiled down to, is there a policy question? I would say the following. For those registrars that offer DNS service, which is basically all registrar, and for those registrars in particular that are offering DNSSEC-signed service in their name service, which ought to be everybody, the policy question is, should they also support a glitch-free transfer, a smooth transfer, of name service whenever that's required or requested by the registrant? That's the policy question. The details of how to do that are being pursued very actively and successfully. This group is not the one that's composed of the rights of the people, except for a couple of us who are intimately involved in it, to do all that. But it's easily packaged into a very simple policy statement, which is that the registrars should support smooth transfer of DNS service from one DNS operation to another.

ROGER CARNEY: Great. Thanks, Steve. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. I agree that a registrar should help a registrant with changing the DNS server and updating the DS record at all times. So it

has nothing to do with transfer. We have to do this today, tomorrow, whenever, as long as the domain is registered with us.

We also have to do it if the domain name is transferred from one registrar to another, but it is not the same [inaudible]. It's completely different. If the registrant has a contract with the registrar outside of the actual domain [and] they do DNS, then that contact expires if they move the domain. Of course, the registrant can change the nameservers before they change the registrar. It is still too very different operations, and they are not connected. Thank you.

ROGER CARNEY: Thanks, Kristian. That's a great discussion. Again, I think we get to if DNSSEC is in our scope or not. Again, as everybody has leaned toward, it may be not appropriate for this, and it's definitely not in our charter today. But as Jim mentioned, is it part of fraudulent? Is it part of security? I think you can say that. I think it's a stretch for this group to get to that spot, though.

So I would say that, from this group's perspective, the DNSSEC items are important and we can't forget about them, but we're not going to solve them here.

But one thing I want to come back to is [Werner] actually put in a suggestion in chat about our green sticky #2 there, possibly changing it to, again, eliminate any confusion but keeping the idea of the hijacking still in there. It's a ways back in chat, so I'll read it to everybody. He suggested to possibly change it to, "Prevent fraudulent domain name

transfers in particular to prevent the misuse of transfer mechanism for domain name hijacking." And it seems to clarify—to me, anyway. I don't know about others. Sarah brought this up. I don't know if that helps, Sarah.

SARAH WYLD: Hi. Sure. I don't feel super strongly about this one, so I will defer to whatever the group decides. I still think that hijacking is a subset of fraudulent domain transfers, so I don't feel like it needs to be mentioned twice. But that's fine. If the group thinks it's helpful, then helpful is great.

ROGER CARNEY: Okay, great. And I'll also put in there slamming as being another possible fraudulent use—or misuse, I should say—of the transfer process. So just throwing those out there.

One idea is, getting back to what Steve thought, do we need an additional goal that ties these together related to efficiency and maybe user-friendless, user interfacing—anything like that that would help here.

Thoughts from anybody about adding that, making it a goal to be efficient, along with the good and the bad obvious ones here?

Okay. Well, we'll just noodle on that and we'll think about it.

Jumping on to the other two … Thanks, Maxim. Yeah. "Suggesting a registrant-friendly transfer." The third sticky being obviously a slight

change … We're not the IRTP anymore. We're just the transfer policy. But outside of that, one little change [to] sticky 3[,] 4. Does any see any issues? Comments, again, on the green? And, obviously, sticky 4 is a little ahead of where we're at but still applicable for the group, I think.

Theo, please go ahead.

THEO GEURTS: Backing up a little bit, "Clarify language of the IRTP so that the ICANN-accredited registrar [inaudible]," etc., etc. That is a goal, and I think that goals should be always there. Why are we bringing this up? I mean, it is pretty clear that such language should be … Everybody should be able to understand it. I get that, but why are we bringing it up here? It's a long wish[:] always use it every IRT that we produce language [at] that everybody can understand and isn't too legal, we usually feel. But what makes this session stick out from all the rest of the policies and IRTs we are doing? That should be a goal that we always should be doing. So why is it in there? Thanks.

ROGER CARNEY: Thanks, Theo. Yeah, it's true. You would think that's [apropos] for many PDPs. Maybe some of the IRTP people who are still around can clarify, but I think the reason why this was [inaudible] [was] because, before IRTP, there was no such thing as consistency in the transfer process. It has improved dramatically, but from an end-user registrant standpoint, it seems still some inconsistent between registrars. So I would say that's my only thoughts on that.

THEO GEURTS: If I may follow up.

ROGER CARNEY: Yeah. Please.

THEO GEURTS: So that's a good clarification and a very good goal. I fully support it. How do we achieve that? How do we monitor such language? How do we get there? How can we sort of put a metric on it, if you will? Or how do we know when we achieve that goal? That's basically the question. How do we go about that? Thanks.

ROGER CARNEY: Thanks, Theo. I'm hoping that, as we get these goals and principles in place, as we're discussing the various different charter questions, we can actually tie those charter questions back to that specific goal so that, once we get there, we can say, "Okay, are we removing anything that's possibly inconsistent? Are we adding a feature that provides a more friendly or more consistent view?"—again, just speaking on the consistent policy part. That's my goal: using these principles to help make those decisions later on when we're answering those questions. Hopefully, that helps.

Okay. All right, let's jump down to the tech op principles. Again, I'll give everybody a minute or so to read through all these yellow items and see if they're still good goals, good principles, to use moving forward. Do

we need to combine some of these or are they repetitive of what we already discussed? Again, take a look at the five goals. Let's see if we can clean these up or if we can just accept them as is. Again, I'll give everybody about a minute. Thanks.

Okay. All right, Theo, please go ahead.

THEO GEURTS: When I'm looking at "The gTLD transfer policy should be changed as little as possible," I'm not sure if that is the goal we actually want to achieve. I think the goal should be that it should be within … Actually, the other Post-Its are much more aligned with what should be the goal and how we can use it, but I think we should not limit ourselves already while we are going to discuss what needs to be changed and what should be done and how we should get things complying with whatever is required and making transfers easier, I think. If you just limit yourself, like, "Okay, we're going to do as little as possible," I don't think that's the right goal to set. I think that one can be removed.

ROGER CARNEY: Great. Thanks, Theo. Again, I think, from the tech ops perspective—maybe Tom or someone else could jump in—originally the goal was to try to provide as much, I guess, security and thought without changing the policy a lot. But, yeah, I agree with you that that's kind of why we're here: to not necessarily change it to change but to look at it as a whole and change whatever is needed. So I would say that that doesn't seem like a goal for us. Thanks, Theo.

Sarah, please go ahead.

SARAH WYLD: Thank you. Sorry, I changed microphones. Do you still me okay?

ROGER CARNEY: I hear you good.

SARAH WYLD: Okay. Thank you. My other headphones died. Okay, fourth goal: "No personal data shall be" … Sorry, fourth principle: "No personal data" … I actually wonder if maybe that principle is not necessary. And you know me. I'm not always the first person to suggest data processing. But the first principle there, I think, is crucial: "The process must comply with data privacy regulations." I'm not sure that we need to prohibit registrars from creating a process that could allow for transferring registration data. I imagine one could have a scenario where two registrars enter into some kind of appropriate agreement to protect data properly and to transfer it according to whatever legal obligations they have. And I'm not sure that we need to make that not allowed. Thank you.

ROGER CARNEY: Thanks, Sarah. And I was thinking the same thing—I guess not necessarily the idea of maybe a cooperative agreement somewhere or whatever. But I was thinking that 1 and 4 kind go together and maybe should be tailored as such. But, yes.

Tom, please go ahead.

TOM KELLER: Thank you. The points that were just addressed were basically in the tech ops paper, and the idea of the tech ops paper was to touch as little as possible to get the process through as soon as possible. So I can totally live with actually getting rid of them, basically. It was just a description on making things easier and faster. But now that we're looking into the whole process, they do not necessarily make sense.

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

THEO GEURTS: Regarding the "no personal data should be transferred," that's a very good point that Sarah made there. It's definitely not something that we should be discussing. If there's a group of registrars who want to share data internally because they're all the same companies/group under the [same] umbrella, they can set up their own agreements to facilitate that. Or if they want to set up with a different registrar/entity, they basically can transfer data. That's not prohibited under the GDPR. You just need to be compliant with all these data protection laws. But you can set it up. So it's definitely somewhat out of scope for us, I think. Thanks.

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

JODY KOLKER: Thanks. Can you guys hear me?

ROGER CARNEY: Yeah, we can hear you good.

JODY KOLKER: I guess I wanted to ask a question on the second yellow goal there—or principle, I guess: "The transfer policy must be instant but with enough time to validate the legitimacy of a transfer." I'm curious as to what the transfer process is considered to be in that principle. Does that start when the registrant asks for the auth code, or does this only refer to the actual process of sending the EPP command to the registry to transfer the domain? If all of that needs to happen in an instant, I think we're going to have some issues trying to validate that from the start of the registrant asking for the auth code. Or does the instant process only refer to the EPP command to actually transfer the domain, thereby taking out the five-day auto-lag period [in the ackinac] period? That's just a question for the group. I'm just curious what we're considering to be transfer process on that principle. Thanks.

ROGER CARNEY: Great. Thanks, Jody. And I would say, going to your examples there, I think, when looking at this, it would be … We should probably clarify so it makes a little more sense if the group thinks that's correct: this is the transfer process from the beginning to the end. And I think this goal

here is to make it, again, kind of going back to the earlier part, the most efficient possible. That's not everybody waiting so long to do whatever they need to do, but it is possible that it goes as quickly as it can. So I think it goes back to what Steven mentioned: making things efficient as well as eliminating the bad and getting the good in there.

So unless others think differently, I would say we should clarify here and say that instant isn't it that it happens when the user clicks it but it's in the process itself.

ROGER CARNEY: Okay. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. I was just thinking we could rephrase the "no personal data" to "Policy should not require registrars to transfer personal data between registrars." If we rephrase it to that, I think we have the original intention of that posted there. And we accommodate the comment from Sarah, which was very good. Thank you.

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

TOM KELLER: Thank you. So I want to go back to the instant. So the idea we followed back in the time is that, once you have all the credentials and you go to

the new registrar and you type in all his credentials, the transfer should be processed right away instead of waiting for another five days' time.

I actually do have an issue with "efficient as possible" because I don't know what that's supposed to mean. That's very broad term and could be anything at the end of the day. I think, if we're talking about "instant," it's pretty clear what is supposed to happen. So the customer doesn't have to wait for the transfer as he does currently.

I think we could tweak the language a little bit and not talk about the transfer process, which is really entailing the whole process from getting the auth code and all that to processing it. But if you just say that the transfer should be processed instantly, then that would make no sense. Thank you.

ROGER CARNEY: Thanks, Tom. Kristian, your hand is still up. Is that an old one?

Okay. Thank you. Okay. So maybe update the instant to be more specific. These are high-level goals, so the instant transfer—would that be a high-level goal versus the high-level goal of efficient? And the instant transfer is just one piece of making that efficient. Just something to think about.

Okay. And I think, if I remember right—let's scroll back—[inaudible] mentioned something about the third yellow sticky being maybe a little too broad and that a transfer token shall be sufficient to authorize a transfer. And I think this kind of goes back to maybe—Tom can jump on if he wants—again, more of a specific goal than an overarching goal. I

think that the idea here was, once a token has been given to the registrant, that's all they need to do. But that's not everything that the transfer policy is.

So thoughts on that? On sticky 3 there? If it's too broad …

Tom, please go ahead.

TOM KELLER: Thank you. I believe it's okay the way it is written because, once you have it, it should be sufficient. But other processes are there to get the token, and how the verification happen at the point of time the token is given out is something completely different. But once you have it, that should be enough assurance for the gaining registrar to something with it. This is a scenario we're living under now for the last two years and has proven not to cause any issues, so I would really like to leave it there.

ROGER CARNEY: Okay. Thanks, Tom. Other thoughts? I see Greg supports that as well.

Again, I don't know—thinking about, again, the objective here as the high-level goals for transfer—if this is more specific to a specific spot or if it fits in a high level. Again, just thoughts for people to think about and see if that works or not.

Okay, great. All right. Well, I think we have actually used a little more time than we wanted to, but that's good because goals are usually not something that excited people a whole lot. So I think getting these

clarified will help us when we're into the details of charter questions and saying, "Okay, is the answer correct?" We can point back to one of the goals and say, "Okay, it's in support of that goal that we all agreed to."

So, again, I think it's a great discussion. Not over. We'll continue to work on this and clean these up. Again, great use of the Jamboard here to document all of our thoughts. We'll get this into a consumable document and start working from there.

Okay. I think we should move on to our next topic, which I think is—there we go; thank you very much—our continued discussion of what Sarah has deemed—I'm trying to stay to it but I catch myself not doing it always—the transfer authorization code and our discussion of our several charter questions on that.

So [in] our last meeting, just so everybody that wasn't part of that is aware, and just to remind everybody else, we had a few things, again, to try to add clarity. We tried to eliminate the confusion of what is an auth-info code versus an auth-code versus a password. And Sarah had suggested maybe trying to use "transfer authorization code" to be specific. So I've been trying to do that until someone suggests something better or something different. I'll try to continue using that.

Something else we talked about was leaving the more technical items here to Tech Ops possibly and how that looks. I think that asking them officially […] Do we need to draft a letter to Tech Ops saying, "Hey, this is what we're looking for"? And, to Jim's point from the last meeting and what we've discussed already, what kinds of bounds and instructions

can we give them for creating a new transfer authorization code to be secure and things like that?

So I think that, as we look at these specific charter questions, I think we need to pull out of there: is there something that we can provide Tech Ops as a direction, saying, "Okay this is that"?

And the third item I wanted to bring up from our last meeting. We had talked about data metrics and getting some Compliance numbers on transfers to see if there has been an issue with [inaudible] three years ago when we changed basically from requiring the form of authorization to basically allowing transfers with an auth-code. Has there been an increase in complaints, fraudulent transfers, that they've seen? Again, again, Compliance. ICANN Compliance is working on that. They haven't gotten those details together yet, but they are working on that.

The other thought was, does it make sense—I don't remember; maybe Sarah brought it up at the last meeting—to possibly poll CPH members—maybe a survey to CPH—along those same lines? Have they run into more issues? Or what are the issues in trying to prove [if] using the transfer authorization code enough, which would allow us to eliminate the FOI and then possibly make it more efficient—again, those kind of thoughts.

Theo, please go ahead.

THEO GEURTS: A quick question there, Roger. You just mentioned that Compliance is looking at the amount of transfer complaints. That's good. Good metrics. I suspect they will be lower since the GDPR kicked in, but that is just speculation on my part.

I was wondering if Compliance is also looking into how many times IRTP D has been activated, so to speak. How many times has that been used? That is specific policy around unauthorized transfers where mediation is done through UDRP providers, just like WIPO, etc., etc. And I was wondering if staff was looking into those metrics also because they could be very valuable for us also. Thanks.

ROGER CARNEY: Great, Theo. I don't know, but we'll definitely get passed along to them. So thank you.

Okay. And, again, I wanted everybody to focus [on this]. I think the agreement here is to ask Tech Ops to create technical specification for the transfer authorization code. So I think that what we need to do, as Jim mentioned last time, is come up with the policy or business definers for that so that it helps them be able to create that correctly for us. So, again, as we go through these, please think about, do we need to send a case to Tech Ops here or there. Again, I think we probably should make it a formal ask so that we can get and set a timeline on it so we can get it back.

Theo, please go ahead.

THEO GEURTS: Yeah, I think we should definitely do that. I'm not sure if we want to send them all the questions that we have listed here because, when I'm looking at the question about registrars requiring to incorporate two-factor authentication or multi-factor authentication, I'm not sure if we should be asking them that. I'm [not] sure of the opinion that [that] is not part of our work. Many laws already require registrars to provide excellent [opsec] to their registrants/users/customers. That is already done by law, so I don't think we need to go there. Thanks.

ROGER CARNEY: Thanks, Theo. And I agree. I don't think we need to send them our charter. I mean they have access to it. I want to be more specific about our request to them and not just repeating what our charter is but actually getting this group to say, "Okay, we need to bound it here and provide them this information so that we get back what we actually can use." So thanks, Theo.

Jim, please go ahead.

JIM GALVIN: Thanks, Roger. To your last point there, I want to suggest that we frame the question to Tech Ops in a context. And, more precisely, at the bottom of this section which is currently on the screen, I had put that text there, and I think what has motivated a lot of this discussion is the highlighted sentence there because it was captured in this discussion about what is our goal here. I think that, in order for Tech Ops to properly answer all of the questions up there about the transfer

authorization code, [they have] to understand what we intend to do with that and what it represents. So, rather than submitting all of our charter, I think that we have to just put all the questions in a proper context. I think that that partial sentence there, that phrase, is the context, but to me, that's the test. That's the question that we need to answer and agree on. And then we can submit the questions to Tech Ops to work on so they have a context in which to do it. At least that would be my suggestion. Thanks.

ROGER CARNEY: Great. Thanks, Jim.

Okay, so I think that I'm hearing agreement. Let's draft a letter for Tech Ops, asking them. And I think that we can start it here, like Jim said. We can start this draft with Jim's goal here as the context of it. But also, as Jim alluded to … And then get into what our specific questions, along that line. Or not even questions. It doesn't have to be a question. We can make a statement saying, "This is required. We have to have this." And it's not, "We have to have 32 bytes," but it's, "We have to have a secure transfer authorization code." So I think that that's good.

Thoughts on specific … Again, bounds or … I want Tech Ops to have something very specific so that they can [get] back to us quickly. But we want it to be their solution to fit our policy. So I think we have to come up with those policy bounds for them. So I say let's start this letter with this goal, and I open it up to the floor now as to, what are those specific policy bounds that we need to look for that we can supply Tech Ops to give them direction? Hopefully, that makes sense. Thoughts on

anything to add to that letter? I guess, again, staff can get the letter created for us and we can iterate on that letter, but I think the sooner the better so that we can get that off and they can get to working on it as they have time. So I think the sooner, the better.

Berry, please go ahead.

BERRY COBB: Thank you, Roger. I just want to try to get a bit of clarity especially about what you're asking staff to do. So I'm going to mention a couple of things, starting back with Theo's intervention, because we were talking about gathering data. We acknowledge that Compliance is working on gathering some updated data. That data was in the context to try to inform the deliberations as to how secure auth-info codes are.

I think what we're going to find is that the data that Compliance has is just a small pie piece of all of the larger transfers out there, and it may or may not—I haven't seen the results of this—be intuitive to inform the question of how secure the auth-info code is.

So I think that that's what's kind of prompting reaching out to the Tech Ops group for looking for additional information that registrars and maybe registries would have where Compliance does it.

So, to Theo's point, in relation to IRTP Part D—and I believe it was in relation to the TDRP—there is data from the policy status report about the number of disputes that were raised. I don't have the exact number on my fingertips, but I believe it was pretty low in the grand scheme of things. And staff will pull that out and we can maybe go out to the

provider sides to update it, but I'm not expecting a significant jump there.

So, taking me back to the reason for my interjection here, I think, if in fact the original purpose here was to try to find out how secure auth-info codes are, perhaps it's more than just a letter to Tech Ops, and maybe we ought to consider a small-but-meaningful type of survey mechanism that could perhaps help quantify what this input might be, as well as qualitative. I think both kind of go hand-in-hand.

But my final comment I'll say is that this can occur in parallel to perhaps the early input, but I do think it is going to take time, and it could push out our deliberations at least from our preliminary project plan around this topic. So we may have to switch things around.

So I hope that was helpful. Maybe the group can provide a little bit more clarify about what we want staff to do. Thanks.

ROGER CARNEY: Great. Thanks, Berry. I appreciate that. Theo, please go ahead.

THEO GEURTS: Thanks, Roger. And thanks, Berry. You're absolutely correct. The statistics regarding the use of IRTP D or any statistics on complaints about transfers doesn't say anything at all about how secure or how well an auth-code functions, of course. That is dependent on lots of different, other factors. Generally speaking, I think the auth-code is usually pretty much a good option to transfer domain names. And,

depending on the registrar, how well their security measures are sort of defines how well an auth-code is good security or well-protected. So that is not dependent on the amount of complaints. Of course, the amount of complaints and the use of IRTP D will give us a good indication if we need to develop more policy around unauthorized transfers by accident or set up anything around that. If the numbers are extremely low or the policy is working as intended, then we don't have to circle back and create solutions for solutions that are already there. That was more to the point.

And, of course, during IRTP C, we had zero information, except from Verisign, regarding unauthorized transfers. Those numbers were pretty low also. But we didn't have any metrics there, which made the policymaking during the IRT extremely hard because we basically had no idea what the reality was. Thanks.

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

JIM GALVIN: Thanks, Roger. I've heard a few people use the phrase "security of the transfer authorization code," or, "security of auth info." I'd like to offer an important distinction here for consideration by the group. I believe, at the policy, what we are talking about here is the security requirements for the transfer. We'd like to know that the transfer is being authorized by the registrant and that that can be correlated with

the identify being presented to a gaining registrar. So they are the appropriate party to receive it.

Now, that's a security requirement about a secure transfer. And there is this question of whether or not a single transfer authorization code is sufficient to achieve that particular goal. I tried to carefully phrase that in a semi-ambiguous way, just to give some room for discussion and when we get to writing the letter.

There is a whole separate set of security requirements about that code itself if that's the mechanism of choice. And that's a distinct set of things. So talking about how big it has to be, it's properties as in uniqueness, it's lifetime—those kinds of things—they are all requirements of that code, which is essentially a one-time password mechanism. That's what allows that mechanism to achieve the goal.

So I want to be careful to separate those two distinct sets of security requirements and make sure that we don't tie them together and make sure that we're careful about what we're trying to achieve and then this choice of mechanism to achieve it and then what we need to do with this mechanism in order to achieve that goal. Thanks.

ROGER CARNEY: Thanks, Jim. I guess I'll add onto that. Again, I think that everybody is hitting on the same idea of [that] knowing the metrics is great. Again, I think that, from Compliance … And I think a survey out to Contracted Parties would be good as well. That's great information to have and it shows how functional, how secure, the current system is.

But to Jim's point, a secure auth-info is possibly different than how secure it is today. So I think there are security mechanisms … Jim kind of hit on one. I don't know if it has really been decided; a one-time password. I think that that one-time password is one of those secure mechanism that Tech Ops may offer as a solution, that it is only good for one-time use. I don't know if that's a policy decision. I think that that's where the line has to get found: is that going to be a policy decision or is that information coming from Tech Ops as a recommendation to make it more secure?

And I think, when you look at Tech Ops, they may provide 15 secure mechanisms. Does that mean that this PDP has to accept 15 changes to the transfer authorization code? I don't think so, but that's something the group will have to talk about.

Okay. Thanks, Jim. Okay, so maybe take a step back then and get back to the questions of … I think that what Jim is saying … Let's start with this idea of the transfer … I'm sorry. Someone wanted to say something?

No? Okay. Oh, Jim. Go ahead.

JIM GALVIN: So the last comment—thanks, Roger—that I just put in the chat room there … I think what's important from my point of view in this conversation coming at this from a security practitioner … What I think we need to decide is that this transfer authorization code is going to be—whatever it's implemented as—our mechanism to both secure and

authorize transfers. That's kind of a policy decision that we have to make, I think. I mean, we're sort of there now. I would argue that that's kind of the system that we have today. It would be interesting just to make sure that we're still in agreement that that's what we're looking for.

And then I make the observation that the way auth-info is used today functions a lot like a one-time password in terms of a mechanism. But it's not actually fully constructed in that way. And that's where we get into this secondary … Well, that's where we get into these other security requirements of the TAC, of the Transfer Authorization Code. Then you get into all kinds of interesting rules about how you want that to be managed. But you have to decide that you're going to fully depend on that mechanism.

I would argue that the current transfer policy in place today, setting aside the temporary specification, was fully dependent on the FOAs. That's where your authorization and security and came from: the presence of that physical paper trail of what went on. And I think the path that we're headed down here is to not have the FOAs anymore, to be much more dependent on the TAC (Transfer Authorization Code, as we're calling it now). We need to make that decision somewhere along the way here. Once we do that, then we'll be in a place where we can say we don't functionally need the FOAs anymore. But if that's going to be true, now we have to look at the security requirements of that transfer authorization code, and it has to be properly implemented and used in order for all of this to work in a secure way, which is the actual goal.

I hope that helps. We're sort of repeating ourselves here a little bit, but I think, in a way, we're getting our conversation down to the proper messaging. So I hope that helps. Thanks.

ROGER CARNEY: Thanks, Jim. And I think that, with the thought of moving the transfer authorization code to the top of the list and working it first, was the concept. If we go back to the goals that we just worked on, one of them being that this code is all this needed, the thought going in here is, yes, this is the end goal. It's to remove the FOAs—both first and second, if need be—or make them optional. But the idea is that this is the way that we're going to transfers. Again, going to the goals—that being one of them—tying back to that … So I think that, when we're looking at these questions here, we have to assume that until we find that it does not work.

Does that make sense?

JIM GALVIN: Yes, for me. Thank you.

ROGER CARNEY: Thanks, Jim. And I'll just make one comment because I know Berry and I talked about this before. Berry put in chat … Again, as we go through these, be thinking about, is there an ask that we can make coming out of this PDP for contracted parties to gather certain data elements or data metrics for us so that, when we review this again in a few years,

that data is available and is helpful? So, again, as we go through these, keep thinking about, "Okay, it would be great if we would have had this. Should we be asking for that going forward?"

Okay. So time check, Emily. How much time do we have? Are we down to our last twelve minutes? Is that what I'm seeing?

Okay. Thank you. All right. So, again, I think Jim is pushing us in the right direction here. So let's assume that the auth code is the direction we're going in. If we find something that fails us, then obviously we'd backtrack on that. But let's assume this is the way we're going and that the auth code is the one thing that we're going to use moving forward—or the TAC, I think Jim called it—[am I short?]—instead of Transfer Authorization Code.

And jumping off of Jim's goal here that he put in the document of making sure that the registrant asking for the transfer is the registrant that is authorized to make that transfer …

So I think, with those things in mind and not looking at specifically these few bullets here, can we answer our charter question, B1? Is it still a secure method for inter-registrar transfers?

Jim, please go ahead.

JIM GALVIN: I'll just say that it could be, but it's not today. Thanks.

ROGER CARNEY: Okay. So the question is still … So you would say it's not currently—so it's not still—but it could easily be pushed in that direction.

And then obviously the follow-up on B1 is: what evidence? I think that this evidence is going to have to be supplied. Again, it's going to be through ICANN Compliance, through a survey, hopefully, that we can generate a survey [with] to contracted parties. And any anecdotal information we have here as well. I think that answers the second part of B1.

Jim, please go ahead.

JIM GALVIN: Thanks, Roger. I want to be careful not to over-depend on this notion of evidence. As we've already discussed and other folks have brought out, the available evidence is kind of a leading indicator, but it's not necessarily going to be definitive for any number of different reasons. I still support gathering that evidence. We should certainly learn what we can from the experience that we have had. All of that is important and useful.

The other piece of this, though, that I'm coming from is a pure, straight-up, academic security principles point of view. So, no, it's not sufficient. That's kind of the answer because there are certain security principles that are not being respected. And those are the things that we would look—I'm presuming here—to Tech Ops to help develop for us. Then we could figure out what the policy constraints are out of the technical

steps that Tech Ops might propose. That's how we meld all of this together and it becomes our work product. Thanks.

ROGER CARNEY: Great. Thanks, Jim. And I would say, again, I agree. I think those policy principles that we would supply Tech Ops we need to think about. I want to go through all of the charter questions so that we can get to a better list of those items.

To your point, Jim, on the more, I guess, technical/academic reasons of "secure," I would ask anybody in the group. It's been three years that we've used basically only the auth code. Do people on this list feel that it has been secured in the last three years?

Theo, please go ahead.

THEO GEURT: Strictly personally speaking out of my own capacity, we've been using the auth-code for .nl since 2010 now, and that has always been sufficient. There are very low cases where the registry actually had to reverse a transfer. And, yeah, like you said, in the last three years I didn't see many issues. But it's just what's happening on my side. It could be very different with other registrars. But I have a feeling that, once we also remove the [attack] factor there, criminals could easily obtain user credentials through the WHOIS and hack themselves into control panels of registrars. It has also a positive effect on the entire things. Thanks.

ROGER CARNEY: Thanks, Theo. That's a good point: several changes have happened and that may have helped it along the way as well.

Sarah, I guess that's the question, right? (in your chat): do we have that answer? Obviously, again, going back to the data that we want to get, I'm not sure that that will specifically answer the question. I think it's more of the experts here that are going to say that it has been better or not. Obviously, that's something that each of the constituencies will have to look at together and get on that. But I think that that's what we're looking for.

Keiron, please go ahead.

KEIRON TOBIN: I'm just coming at this from a different stance. I also think that there's been a lot more security features that have been added to different registrars as well in terms of account levels. So, just even logging into the account, there's been new kinds of developments in terms of two-step authentication. So it's going to make it even more difficult to delve into that data just because, as technology changes, obviously, registrars have become more protective of their stuff. So I think it's going to be a very difficult question to answer.

ROGER CARNEY: Thanks, Keiron. And, again, that's a good point that you're both making: there's been a lot of changes in the last three years. And, again,

that's probably why we'll gather the data but it won't tell the whole story. I think that, again, this group as experts here will have to make that decision as to, is it secure and do we need to make it more secure and how?

Okay. Anyone else?

So what I'm hearing here is, academically, the transfer authorization code (TAC)—we keep using that term now—as an academic thing can be improved, but it has proved secure in the past three years.

And to everybody's point on data, I think: what data will help someone four to five years from now answer this question? That's probably what we need to request from this group.

Okay, great. Well, we have four minutes. Can we introduce B2? Can we scroll down to B2? Okay. I'll just go ahead and read it real quick. "The registrar is currently the authoritative holder of the auth-info code. Should this be maintained or should the registry be the authoritative auth-info code holder? And why?" So I think it's a good question. I think I'll open this up to the floor. I know Tech Ops had several discussions on this, but I'll open it to the floor for discussions, introductions, or thoughts on it. We have three minutes.

Okay. Well, again, the plan here is to go through all of these and then hopefully, by the time we go through all of the TAC charter questions, we will have a better idea of what we need to ask. So as we talk about each one of these, again, think about how does this apply to policy and what we need from Tech Ops?

I saw Theo's hand, but maybe he's not interested in talking now.

Okay. And just real quick, I'll note, too, on B2, that the Tech Ops concluded that, to reach a uniform, transparent, and predictable process, registries should be in control of the storage and processing of the auth code regarding the technical part. So, again, going along with who should be maintaining this, I think that we'll have a substantive discussion next time—two weeks from now? Or two weeks from yesterday, I should say. But we'll start here. Again, the goal [is to get] through all these charter questions and [have them] discussed well and then see what we need to ask of Tech Ops.

All right. One minute left. I'm going to open up to comments. Any other business? Anything anybody wants to bring up? Questions?

Okay. Well, thank you. Thank you, Sarah. Thank you, everyone, for participating. Again, hopefully everyone's ICANN71 goes well. Those in North America are getting their due reward for normal meeting times, and hopefully they're getting some sleep, too, as well.

Thanks, everyone. We'll talk to you in a couple weeks.

JULIE BISLAND: Thank you, Roger. Thanks, everyone, for joining. This meeting is adjourned. We will end the recording now and disconnect all remaining lines. Have a good rest of your day.

[END OF TRANSCRIPTION]