ICANN Transcription
Transfer Policy Review PDP
Tuesday, 08 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 the agenda wiki page: https://community.icann.org/x/6gjQCQ

The recordings and transcriptions are posted on the GNSO Master Calendar Page: https://gnso.icann.org/en/group-activities/calendar

JULIE BISLAND: Good morning, good afternoon, and good evening. Welcome to the Transfer Policy Review PDP Working Group call taking place on Tuesday, the 8th 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're only on the telephone, could you please let yourself be known now? And hearing no one, for today's call we have apologies from Theo Geurts, RrSG, John Woodworth, ISPCP. They have formally assigned Jody Kolker, RrSG as their alternatives for this call and for 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 functionalities 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 Google assignment form. The link is available in our 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 Wikispace shortly after the end of the call and as a reminder, those who take part in the ICANN multi-stakeholder process are to comply with the expected standards of behavior. Thank you. And over to our chair, Roger Carney, please begin.

ROGER CARNEY: Thanks, Julie. All right. As everybody can see, day of celebration, we get to jump into some work today, so good for us. But before we do that, I'm going to slow us down so we don't work too hard but it looks like we have one new active member and I wanted to give Keiron a chance to come to the mic and introduce himself and let everybody know who he is. Keiron, can you please let us know?

KEIRON TOBIN: Hello. Thank you for that, Roger. My name is Keiron, and I've probably been active in the ICANN community for around five years now. So, I did have a bit of a break for about three or four years in between that just

due to workload and moving around in different departments. I'm the Manager of Global Policy for GoDaddy and the Head of Abuse and Compliance for Uniregistry which was recently purchased through GoDaddy. So, we're just sorting the merger out there. But in regards to the PDP transfer and everything else, yeah, you've got my full attention so thank you everyone for—I'm not sure exactly in terms of the fast movement that was taking place so a huge thanks to Julie and everyone else who was involved in that process and I look forward to best help in the best possible way I can so thank you.

ROGER CARNEY: Thanks, Keiron, and welcome. All right. Just a few more things. I think we've talked about the SO/AC outreach letter that we've been working on. We'll get that sent out to the entire group after this call so everybody can start taking a look at it. And we have a couple of dates as well assigned to that. We want any comments or additional questions that people would like to add done and back by the June 24th so just a little more than two weeks away. Again, any comments, the sooner, the better, I mean, don't have to wait until June 24th so if you want to post those to list or even in the document itself. And then the second date is the June 29th which is our last meeting of June but we're hoping to get that letter approved and finalized on that meeting so we can get it sent out by the end of June to all the other groups.

Speaking of which, I guess, I kind of hit on it, as you noticed, our homework, our today's agenda, our document for today is posted to Google and we wanted to make sure that this was good for everybody to, I guess, collaborate through the Google docs system. Again, we'll be

doing more and more docs through that if everybody's good with that. I know some companies don't allow it and some people have to work around it but it is one of the better tools that we have available to everybody. So, let us know if that's a problem for anyone that we can't get worked around. So, otherwise, we'll go forward with using Google docs to share documents.

Okay. I think that was all of the lead up work before we actually jump into doing some work. Any questions from anyone? Okay, great. All right. So, let's jump into our, yes, our AuthInfo discussion. So, thanks to staff for putting this together and I'll turn it over so they can introduce it and walk us through.

CAITLIN TUBERGEN: Thank you, Roger. So, to facilitate the group's discussion on the first topic of AuthInfo codes, the support staff team worked together to produce a document that's supposed to aid the group in its discussion of this issue. At the top of the document, what we've done is to introduce the relevant policy texts or the existing policy texts around AuthInfo codes. So, in the first section, you'll see all of the relevant provisions of the policy currently enforced with respect to AuthInfo codes. So, I'll quickly walk through that for those that might not be as familiar with the transfer policy as our registrar colleagues. So, beginning at the top, you'll notice the first section of the transfer policy which is dedicated to inter-registrar transfers. Section 5.2 provides that registrars must provide the registered name holder with the AuthInfo code within five calendar days of the request from the registered name holder, if the registrar doesn't provide facilities for the registered name

holder to manage the AuthInfo code themselves via their control panel. Section 5.3, notes that registrars may not employ any mechanism for the registered name holder to obtain the applicable AuthInfo code that is more restrictive than the mechanisms used for changing any aspect of the registered name holders contact or name server information.

Section 5.4 provides that the registrar must not refuse to release an AuthInfo code solely because there is a dispute between the registered name holder and the registrar over payment. Section 5.5 provides that AuthInfo codes must be unique on a per domain basis. And section 5.6 provides that the AuthInfo codes must be used solely to identify a registered name holder, whereas the form of authorization still need to be used for authorization or confirmation of a transfer request as described in earlier sections of the transfer policy. So, those are the five sections of the transfer policy that applied to AuthInfo codes. The need that we've also included the updated language from the Temp Spec that is now part of the interim registration data policy around AuthInfo codes. So, the first section of that notes that the registrar and registry operator shall follow best practices in generating, updating the AuthInfo code to facilitate a secure transfer process. And secondly, registry operator must verify that the AuthInfo code provided by the gaining registrar is valid in order to accept an inter-registrar transfer request. So, again we hope that it would be helpful to isolate the relevant language about AuthInfo codes on this document so that you don't have to cross-reference between the relevant policy language in our discussion. So, if we can scroll down a little bit. The next section provides a working definition that staff support added that was pulled on directly from the ICANN website. I think I'm going to hand it over to

Roger now to discuss the working definition and how the group wants to proceed on this.

ROGER CARNEY: Thanks, Caitlin. Yeah, and I think that this may be something that evolves or maybe we can hit fairly close early on but I think it's good to get a definition as a lot of people use different terms here to describe this, you know, password, AuthInfo, auth code, whatever else comes to mind. And I think it would be useful to have a good definition that is applicable for all of our work here. So, I think this is a good start and I think that we can add to this. Obviously, some of the charter questions are going to possibly modify this directly so I think that, again, we'll probably iterate through this definition as we start to come to agreement on some of the charter questions. I don't want to spend too much time here but if everybody can pull this in and think about it and also, as we're working through the charter questions to start thinking, okay, that'll probably change that concept somewhat so we can actually go back and edit that as we go through. Thanks, Berry, for your notes in chat. Okay. I think we can go down and actually start into the charter questions. And I think the biggest question for the charter questions are if people think there may be a better order to possibly work these questions in, otherwise, we'll just probably just work sequentially through them. But if anyone feels like maybe question four should be first or whatever, that would be good to know. So, I don't think we need to go through and read these because we've done that once or twice already and I think everybody's fairly familiar with this. So, Berry, please go ahead.

BERRY COBB: Thank you, Roger. Just real quick, can you scroll back up to the top for the first comment I made about unique codes? And thank you, Jim, for responding back to me. So, I was just a little bit curious and perhaps subsequent discussions can maybe help illuminate how this exactly works for those that are non-technical or non-registrars and registries. But as James noted, the registrar generates this random note, a number code, and then it gets stored in the registry. Is it possible that two registrars could develop the same random code? Has it ever happened? Is it even worth mentioning or understanding kind of AuthInfo code collision, so to speak, is that even possible? I'm just curious about that. Thanks.

ROGER CARNEY: Jim, please go ahead.

JIM GALVIN: So, I'll offer the comment that sure, from a pure, straight up technology point of view, two different registrars could certainly generate the same code for something and use it that way. But one of the things to keep in mind is, you need to be able to correlate that to something. So, the fact that they might generate the same code is really not interesting in and of itself. If an external party wanted to take advantage of that, they need to know that these two people are both trying to transfer a name at the same time, oh, by the way, they just happened to generate the same code. I mean, you've got to figure out that that could happen. The likelihood of that happening really is near zero and being a real risk is

very low. Besides, you can do things if you really are concerned about it, you can do things to avoid that. For example, you could hash the domain name and that has a much higher probability of just giving you a unique value and then all of that goes away. But if that's a real concern, that's something to talk about from a technology point of view. Thanks.

ROGER CARNEY: Thanks, Jim. Any other comments, questions? And again, it looks like several people have already started adding some comments to this document, which is great. All right. So, let's go ahead and move down into—so the charter questions down here, I think that they're all kind of broken out and kind of in an order on purpose and that they're broken into sections and really the sections are tied to each charter question but we'll go through those just to make this pretty clear. I know the first one is about retention and overall security. The second one being about authoritative holder of the AuthInfo codes, third section being provisioning of the code itself and the fourth section being about the expiration of the code. And again, we want to highlight this just so people understand. Now, currently this is laid out in this order but really, we're looking to see if anybody thinks maybe the order should change slightly or completely. So, I'll open it up to people that have ideas, thoughts, about changing the order or if everyone is good, we could just start with charter question one. Okay. My only thought on that was that the first two or three could maybe be swapped around. And I don't know if anybody had preferences about talking about who should be the manager of the auth codes first, before we get into auth codes. Thank you, Sarah. Jim, please go ahead.

JIM GALVIN: So, I don't think that we should—I like this order and since you just quickly offered up that maybe we should talk about the manager of the auth codes first in front of all the stuff, I want to suggest that I think this first item up here, I think it's important to do this one first. Even before we talk about manager, you need to know what your goal, what you're ultimately trying to achieve with the AuthInfo code or whatever we ultimately talk about, which is also one of those questions there. I think that's critical because it is from that point that you will derive all the rest of the requirements that you all want to decide if you can agree to follow and from that we'll then come out, who's going to manage these things. So, I like the order that's here and I want to say no to your suggestion to put the manager in front. Thanks.

ROGER CARNEY: Perfect. Thanks, Jim. And I think you're getting the same thing from Sarah, so okay. Well, good. Then I think we can just jump into the discussion around charter question one, b1 that is, and it's all based on the security and do we have evidence that it's secure? Are there thoughts of making it more secure? And again, some of the bullets down here just from past people—but we don't want it to talk about past people, we [inaudible] talk about past people with this group. So, interacting with those thoughts, getting to some conclusion here. So, I'll open it up to anyone that wants to make any comments on, if it's secure enough, if it should be more secure and also thinking about, do we have any evidence that proves that this is secure? Sarah, please go ahead.

SARAH WYLD: Hi. In terms of evidence—and I feel like maybe we talked about this in the previous call. There must be some evidence that we can look at, specifically, I would say related to ICANN compliance tickets that indicate perhaps there are many tickets or no tickets about auth codes being insecure, about people losing their comments, about people not being able to get access. So, to what extent have we already looked at compliance ticket rates is—because I'm not sure and I don't recall specifically in like the policy status report or the review that came out before we started this. I can't recall if they actually looked at that. But if not, that's what we should look at. Thank you.

ROGER CARNEY: Thanks, Sarah. Yeah. And I think that that's something to look at and I think maybe even since the dependency on auth code has changed pretty dramatically three years ago when we implemented the temp policy, that may be a look back and a look forward is useful as well not just that specifics around that. I don't know if maybe staff has something maybe during the issues report or during their gathering of information if they had any contact with compliance in any thoughts on that but, Jim, please go ahead.

JIM GALVIN: Thanks, Roger. I want to suggest that I don't think asking if AuthInfo is secure enough is the right question. I don't think that's framing the right question. If you look down at the comments that I note down below, I think that we should think of AuthInfo as a mechanism to achieve the

goals. And then, there's the question of whether our use of that mechanism is appropriate to the circumstances at hand. There's a certain amount of baked in process here and AuthInfo obviously fits into that baked in process in a certain way. And so, are there things we can do within that process to make the use of AuthInfo better? But the real question on the table here is, what are we trying to achieve with AuthInfo? And I think that in the transfer process, I think we need to be very clear about the goal of the transfer process, what we're trying to derive from it from a security point of view and then we can talk about whether or not the mechanism is being used in the best way possible. So, cutting right to the chase, my comment down there below is I make an assertion about the goal that we're trying to achieve here. Okay. And Sarah highlighted it and put a plus one there. Thanks, Sarah. That really, I think is the most important point. And then we can step back and say, "Okay, are we using the AuthInfo element in an EPP transaction, okay, in the best way possible to achieve that goal?" And I make a couple of references further down in my discussion there. So, I really would like to suggest that we frame the question and start the discussion in a slightly different way. That's just my advice. Thanks.

ROGER CARNEY: Thanks, Jim. And a good point of reaching back to the goals and thinking about AuthInfo as a mechanism just like FOA being a mechanism of a goal of—and I don't know if this goal is broad enough for what we're looking at or maybe it's exactly what we're looking for. So, I'll let that be a question as well. Should the goal encompass, I mean, this goal is documented that Jim suggested here is specific to, okay, can we identify the actual registrant? Are there other goals that we're looking for? And

again, I think Jim maybe hit on a point, maybe not specific to AuthInfo but this transfer itself, is there a bigger goal that leads us to these mechanisms? And it's one of the things that we're going to touch on next week at the ICANN session. We're going to spend half of our time talking about what this PDP is here for and what it's doing, the goals of the PDP itself. So, I think that this is a good lead in for that discussion. But yeah, I think that maybe we think about is Jim's suggested goal here the right precision, should it be broader or narrower? So, I'll leave that open as well. Steinar, please go ahead.

STEINAR GRØTTERØD: Hi. I'm just curious because I like the wording of Jim here, what is the difference between the auth code and the one-time password as you're referring to in your comment in the doc? Thank you.

ROGER CARNEY: Yeah. Thanks, Steinar. I think that that's one of the reasons for coming up with a definition and as I think Berry may have thrown in chat earlier was, kind of coalescing the different thoughts on what everyone calls this. Is it a password? Is it an AuthInfo, auth code? You hear all the time in different ways. And I think unless someone else wants to jump in, but I think it all means the same thing and it's the code that you use at the domain object level and moving it from one registrar to another, whatever you call that code, that is what we're speaking about. Jim, please go ahead.

JIM GALVIN: Yes. Thank you, Roger. At a conceptual level, they're all the same thing. That's really the point here. It's worth noting that in EPP it's called AuthInfo, okay. But externally from a textual point of view, it has all of the names that the staff has called out for us in some of the prior text up above. So, AuthInfo as the EPP element is just a particular choice of this thing that we're trying to create, this authorization code, AuthInfo code password, whatever you want. My use of one-time password, that is just a way of saying, this is the goal that you're trying to achieve. AuthInfo is simply an example of a one-time password. One time password brings a lot of security principles with it. You say one-time password and from a security point of view, you now know what that means and what you have to do with it and it naturally tells you what the next set of rules are and processes that you have to obey in order to achieve that. So, one time password has all of the goals that you would be wanting to achieve from the use of the AuthInfo data element which we could contextually name an authorization code. And I hope I have not confused all of that by saying that but in general, the easy statement is they're all the same thing. Thanks.

ROGER CARNEY: Thanks, Jim. And I think that you've answered Berry's question from the RFC, it is AuthInfo. So, Sarah put in chat that she likes the idea of transfer authorization code which is pretty descriptive, I think. And maybe we'll document that and see how others feel about that, think about it. Does that portray what we're trying to portray, I guess. Does it say what we're trying to come to here? I think it's a little more descriptive and we don't get into the technical issues on AuthInfo too much but it can be used for other things besides just a transfer of the

domain name. So, I think that Sarah, throwing in the transfer makes sense especially for what we're discussing. Daniel, please go ahead.

DANIEL K. NANGHAKA: I don't know whether it would be good for having at least one standard name that can be used to avoid confusion. If we had to say we're going to use the EPP code or transfer authorization code, I think it would be good to have at least one generic name that we can use. Probably you can recommend that for all registrants to take it up. I think it would help a lot. Thank you.

ROGER CARNEY: Great. Thanks, Daniel. Yeah, I agree. I think that coming to that standard common across all registrars would be useful so that someone's not using auth code or someone's not using password, it's the same wherever they go so the registrants have that standard terminology. Okay. Thanks, Owen, for keeping all the TACs and NACs and TEACs together there. Okay. I think that that's good. Let's think on what Sarah suggested, the transfer authorization code, and we can make specific reference to technical use of AuthInfo where we need to but when we're describing it, I think using a more appropriate name for our purpose is better. So, I'll ask Jim then if this goal that you stated here works for everyone, are we ready to discuss what evidence there is and how secure it is?

JIM GALVIN: I think that the security of it then falls out from let's see—let me phrase this differently. Are you trying to evaluate historically what has happened or you're trying to think about what you want to do in the future?

ROGER CARNEY: No. Thanks, Jim. And I think that's important because I think that that's two things, right? You want to know if there is an issue. I don't know that you're all that concerned about proving that it's great, right? Does it show security issues in the past? So, again, to me, thinking about four years ago when FOAs were required for everything to two years ago when FOAs were not required in most transfers were going through just on the AuthInfo or the transfer authorization code, I should say, is there a difference that shows that it's not as secure as we want it to be? And then also thinking ahead, can we make it secure enough not for just replacement of the FOA but how this group thinks it should be secure? Does that make sense, Jim?

JIM GALVIN: It does. So, let me answer the question in the following way. From a straight up security point of view and not giving any consideration to business processes and what's going to work best internally with overall registration processes and such, I can tell you that our use of AuthInfo, if we were to continue going forward with the current usage of it, for the purpose of supporting transfers, is not secure enough. I think that there are changes that are necessary and really should be made. At a minimum, you have this issue of it's not uniformly managed and

processed at independent registrars. And I think that that's something that needs to come together. We need to create a certain amount of homogeneity about what it means to have a transfer authorization code and in terms of what everybody does to create them, how long they store them, whether or not they store them, how they're protected. If you really wanted to adopt proper security principles that would come with a one-time password, then no, it's not secure.

So, with that in mind, then there's some discussion to be had about how a transfer works and the sequence of steps, the whole business process that goes with it and then we look at how we adapt the security principles that come with a one-time password into those business processes and make sure that we get everything covered and that would be the path to success. Thanks.

ROGER CARNEY: Thanks, Jim. That's great. And I think that's a good point and I think if we go back to, I think meeting one or two of this, I think maybe it was meeting two, where staff pulled together a couple of slides showing that mechanism, the normal mechanism of transfer and working from that business concept and through to your point of, a lot of what you were referencing was a lot of future security items to add that make it better or make it harder. I guess that's this group's decision is, is it useful? Is it too burdensome? So, every time we add something, we're adding burden to the whole process so we had to think about that as well. Keiron, please go ahead.

KEIRON TOBIN: Yes. Just in regards to the FOA going back to 2018 time, I believe a lot of that was just in regards to data privacy laws that were changing obviously with CCPA and other kind of privacy laws coming into place. I think if we were to implement a new step as well, it would probably be useful to have someone in regards to a privacy expert just to ensure that what we were doing covered the bases, because I feel like without someone with that knowledge on board, we could end up creating something where we ended up kind of going back to the initial stage to reevaluate that back from the beginning.

ROGER CARNEY: Thanks, Keiron. And that's a really good point. I can't remember, someone put in this document, actually, maybe it was Berry or Jim, I can't remember, talking about, if we create a transfer authorization code, are we creating an identification that is basically creating PII or personal information, personal identifying information so that we're back to competing against any data privacy laws? I don't remember who put that in there. Something similar to that into this document already. So thanks, Keiron, for that. Daniel, please go ahead.

DANIEL K. NANGHAKA: Thank you very much. So, with the rapidly changing technologies right now, I think security is becoming a key thing. Many systems are adopting the two-factor authentication, and also to add on the mode at which the AuthInfo code is transferred to the user sometimes may pose a security threat. I suggest that, if possible, we could recommend that two-factor authentication be enabled such that in the process of

transferring a domain, the owner, the domain owner can be able to verify the authentication that this is a genuine transfer of the domain that is happening and it can please proceed. Otherwise, in case the two-factor authentication hasn't been enabled, there is at least substantial risk that could happen since the domain is becoming more of a business [this time.] Thank you.

ROGER CARNEY: Thanks, Daniel. And that's a good point of how the code is presented or given to the registrant. And it kind of probably crosses several of these charter questions in themselves so, you can see it being used here or provisioning and all those so I think it may tie across several and maybe we will have to hit it multiple times to get to the final answer but, yes, good point. Thanks. Sarah, please go ahead.

SARAH WYLD: Hi. I was also thinking about Berry's comment in the document as to whether the auth code is personal data. And I think it could be but it is not necessarily the case and actually I think mostly it's not. So, the auth code would let you confirm that whoever provided it to the gaining registrar has authority to do the domain transfer but it doesn't tell you who they are or who owns the domain name. So, it's very difficult, although I guess not impossible to use that code on its own or in combination with other data to identify a natural person, right? Although as Jody said, it can in some, maybe edge cases be used to validate contact information. So, I would say we need to protect the auth code as we would protect any other potentially sensitive piece of

information like a password but it's not necessarily personal data. And even if it is, I do think that we have a very clear legal basis, legitimate interest to use that auth code to approve a transfer. Thank you.

ROGER CARNEY: Great. Thanks, Sarah. Yeah. And that's a good point. I think probably the thing just to pay attention to is not—make sure we don't tie this to personal data. As you pointed out, I mean, it is a transactional element so it's for a reason, not a person, but we just have to make sure we're not creating the transfer authorization code based on someone's name or domain or whatever so it ties back. I think it needs to be separated to allow for that. Okay. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. Just a couple notes like I would say the comment on that, we first need to agree on a goal. I think the goals should be secure transfers. I would say the AuthInfo code is a good method for registrar transfers. I think there is a lot of small tweaks we can do that would make it more secure than today that we should definitely look into and one of them being like time to live which basically makes it a one-time password that Jim talked about. Like for many other things in today's world, we have owner change stuff with less security than auth codes. So, like in Denmark, for example, you just need two codes to owner change a car, just to compare. So, I would say the auth code is definitely comparable to that. In order to, I think it was Daniel's comment about 2FA, I just want to say that both registrants and registrars are different. We need to be able to cater to all the different types out there. For

maybe some registrar or registrant, the most secure method would be to deliver the auth code with UPS and require signature for someone who would be inside a control panel with 2FA and maybe some other way I haven't thought about yet. So, we should be sure not to tie it down too much but of course be sure that it is delivered in a secure method. Thank you.

ROGER CARNEY: Thanks, Kristian. That's great. So, I think we're coming to some ideas that we can get documented. A few of these bullets, especially at the end of this list here under b1 is asking, what are those things? And, I mean, Steve and Kristian and Jim have hit on a few of them already. The TTL, one-time use, I don't think today—and maybe one of the registry partners can tell me, I don't think it is required that it's a one-time today so I don't know that that's a fact today but it's a good idea of improved security measure going forward. So, and again, like I said, the TTL being along with that. Kristian, your hand's still up. Is that an old hand? Thank you. Tom, please go ahead.

THOMAS KELLER: Yeah, thank you. Roger. So, I just want to add one point and that is that we shouldn't forget the user. So, currently the whole transfer process is, please, excuse my French, a pain in the butt and a lot of people don't really get it. And so, just making it very secure, it doesn't mean that people can use it at the end of the day and if they can use it, it's getting insecure, to can that they ask other people for how to use it and then the [token might] pass hands that it shouldn't. So, usability is one of the

additional issues I want to bring up if you consider the security of the [token.]

ROGER CARNEY: Great point. Yes. Thanks, Tom for bringing that up. And I think that that's what we're seeing in chat here as well as that usability factor. I mentioned just a while ago that I think of the transfer authorization code as a transactional identifier. not as a person or anything like that. I think it identifies a transaction. And so, I think that the discussion in chat here about, okay, would bulk be allowed and could you use one or not? I think that's something we need to work on and decide but again, I think if you think about it as a transactional item and not as a specific, it kind of expands what that means. Jim, please go ahead.

JIM GALVIN: Thanks, Roger. The question about usability and bulk are exactly excellent questions and important. That's really what I was trying to get at when I talked about, we need to talk about the business processes that need to be in place. What is the process that we want to have present? What are the uniform steps that we're all going to follow to make this work? And then we have to talk about where's the uniformity in each of those steps that we're all going to honor and respect? AuthInfo, the auth code, one-time password, it is just a mechanism to achieve a particular type of goal. As part of the business process, you care a lot about usability. Are you creating a sequence of steps that are going to make sense to people or fall out naturally or are going to have to be explained? And then bulk is always a special case and the question

then becomes, is bulk a separate business process that's going to be codified and dealt with separately? That's a question that's actually discussed at b5. You haven't gotten that far here but it comes up later and it's there. Or do you want to incorporate it in? And those are all choices to be made and they're all related. Thanks.

ROGER CARNEY: Great. Thanks, Jim. Yeah. And good discussion going on in chat. And I think that, yeah, I think that as we—hopefully we're documenting these business reasons for these things. And, Jim, you mentioned, I think kind of twice now, another possible auth requirement of being consistent across the systems. So, it's consistent with every registrar, registry. They're not making up the fact that, "Hey, you can have a four-digit code if you want or the next time you go to a different place, it's 32 digits it has to be." I think that's another good requirement for security looking at it that way, and security but standardization as well. Keiron, please go ahead.

KEIRON TOBIN: Yeah. I just wanted to point out, coming from a registrar that essentially had loads of domainers and stuff like that, I think the one-time auth code for group bulking would be honestly, like, I think the domain industry would welcome that with open arms. I do get Sarah's point in regards to the security concerns but I think that's something that could essentially be ironed out potentially by just looking, making sure individual accounts. Again, the onus would have to go down to the registrar directly but I think from that, just helping people in terms of

like, rather than obviously—I mean, if you're transferring a couple of thousand domains which we've seen many times in the past, can you imagine the full list for different kind of domain names with auth codes? And not to mention as well from a technical aspect as well in regards to the smaller registrars, it may actually help them overall because it would mean that they wouldn't need to essentially get—I mean, you would essentially be able to download it for each one if that's what you wanted to do individually but from a concept of changing it to just a single one may actually help the smaller registrars as well.

ROGER CARNEY: Thanks, Keiron. Yeah. And I think Sarah brought up the point of security and I think that that's a good point to bring up, one for many, kind of idea there. And as Keiron pointed out, maybe we just have to iron out the other security features like TTL. I mean, does that add to or decrease that security exposure of one to many domains? And you guys kind of think about that as well. So, Steinar, please go ahead.

STEINAR GRØTTERØD: We're jumping back and forth on the questions here but—and it's very, very interesting, honestly. Well, from an end-user perspective, I think it's—and that's my hat. There are kind of two elements. How does the registrant get access to get the auth code? So, this first normally procedure is that you have some sort of control panel done by a registrar. And from there on, you get the auth code security password or whatever we call it. So, it's not only about the security element for the auth code itself but it's also the element of getting into the

information to get the auth code. And that also brings into a level we touched during the process, the kind of recommendation—not the recommendation, kind of [inaudible] saying that there should be an easy way for a registrant to get that information, get access to where they can find the auth code. Badly phrasing but hopefully understood. Thank you.

ROGER CARNEY: Great point Steinar. And I think that goes back to what Daniel was saying as well. And I think even when you start talking about that and you're talking about usability, but I think it's also drift over into security because the harder the usability is, the more likely users will do things that are not very secure. So, if they have 10,000 of these, they're going to copy them somewhere, they're going to save them somewhere and again, possible exposure. Again, just thinking out loud, so I'm not making any statements. I'm just trying to go through the process. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. It was just to reply to Steinar that in the current transfer policy, it says somewhere that a registrar should not be allowed to make it more difficult to get the auth ID than to make changes on the domain like nameservers and other changes.

ROGER CARNEY: Yeah. Great, Kristian. And again, I mean the current policy already has similar wording in it stating, you can't make it more convoluted. It

doesn't say that, but more, any harder than it is to change the registrant name or whatever. Obviously, the transfer of an asset somewhere else has some liability to it, so it's one of those where it's changing DNS. I mean, is it the same? I don't know. Giving the domain to a different person, is that more or less an issue than it is to change the DNS record? Steinar, please go ahead.

STEINAR GRØTTERØD: Thank you. I'll give an example, Kristian, and I'm aware of the wording here. But similar to the requirement for registrar to have on the website information about their abuse contact, I was thinking in the same way. There should be requirements to have information about how to get the auth code one way or another. Of course, that kind of depends on the registrant knows the registrar and maybe that's a tricky one when they have the registration done through a reseller, etc. But in my opinion, it's at least a start. Thank you.

ROGER CARNEY: Great. Thanks, Steinar. All right. Great discussion. Great chat going on. All right. I suppose getting back to the actual questions, I think Jim got us onto the right track of, okay, what are we solving here? And that helps us decide if it's secure enough or knowing how better to secure it. So, I think that we've got several good businesses or goals to this, reasons why this should exist and I think that Sarah brought up the possibility of reaching out to Compliance on getting some data from complaints either on the transfer process itself—and again, this may be auth code related or maybe even just user experience related. And

maybe we can get some information from Compliance on that. But also, I think we look at pre-FOA or when FOAs were required to when they weren't to see if there's a breakage there that we may see surveys out to Contracted Parties. I suppose that's an option, Sarah. I don't know, time-wise how that works out but, again, I think if we can get some information from Compliance, that will help. Tom, please go ahead.

THOMAS KELLER: Yeah. The one thing I want to point out is going back to Steinar's thing is that I don't believe that we should be too prescriptive on how auth codes can be passed on. Every registrar is very different. That could Pose difficulties. And as we know, that would make it very hard for compliance to go after anyone basically. So, rather staying away from that but if it comes to the security level and see whether it's secure or not, I think we could look at the ccTLDs and see what they do because they've done it for a specific reason, I guess. So, we don't need to reinvent the wheel but maybe just copy what's already out there.

ROGER CARNEY: Good. Thanks, Tom. Okay. So, just getting back to the charter question itself. Tom, your hand is up. Did you have another or is that an old one? Thank you. Okay. I think the evidence, we can try to reach out to compliance and see. For the first part of the question, is it secure? I think people think it's a secure mechanism that needs improvements, is what I'm hearing. And I think that we have a few of those improvement ideas laid out. Again, TTL, one-time use. Jim had the idea of standardizing the auth code across Contracted Parties. Other high-level

thoughts like that of what we need to do to make it more secure—or improve the security? I don't want to say more because that makes it sound like it's not secure. I'll just say improve the security.

Okay. Let's take a look at the list. Did we touch on these bullets? I think we hit most of them. We did touch on high levels. Do we want to get into some more detail like specifically, bullet three is periodically updated and I think Jim and Steve both mentioned the one-time use? Do we need to get into more detail on what that one-time use is? And maybe this crosses the line of who manages it and how it's managed so I don't know if we want to get into that now. Thoughts? Jim, please go ahead.

JIM GALVIN: Yeah. I'm not sure, Roger. Do we need to talk more about what one-time use is and whether it's applicable or not? Maybe I'll just comment on a couple of things and you can tell me if we need to have this discussion or not or if this is not the right place. When I think about one-time use, and the idea that there was a discussion to be had here, the first thing is whether or not we believe that the goal of a trust authorization code is simply to make sure that we're correlating the registrant at both ends, from the incoming registrar to the gaining registrar, and that is its singular goal.

With that in mind, I think a one-time password is probably enough but there's some discussion in the chat room about two-factor authentication. I think two-factor authentication is overkill for this particular application but I'm certainly open to being dissuaded of that

opinion. If anyone has a particular motivation for believing that there's a threat that only two-factor can deal with, I absolutely want to have that discussion.

With that in mind, what I'm looking for and the kinds of things that I think should be present in auth code is, we should have some guidance about how you create one. We should have some guidance about how long it has to be, what it needs to look like when it's created. These are sort of technical guidelines. You need to have some technical guidance about its lifetime and what it means to manage that, what it means to make it go away or not go away. And, of course, some guidance about when they come into existence and when they don't which is tied to that lifetime.

When you start getting into where and how it's used—so the TTL and stuff—then you get to talking about the management of it. So, then becomes the question of, okay, obviously registries have a role in the use of the auth code. And how much of a role do they have when you start talking about the creation and management and the TTL of it. That's when you get into that discussion.

But I feel like there's a few things that we need to get through. And I feel like I'm not prepared to answer even those questions myself without a little more understanding that people believe we know what our business processes are. I'm sure that you all do. You're registrars, the majority of people here. But I'm concerned that we do need to have some specific questions. We don't have to do them right now, if you think there's time and a place for that elsewhere. So I hope that helps. Thanks.

ROGER CARNEY: Thanks, Jim. And maybe I'll take the easier one and take the longer one, second here. The two-factor authentication, I guess, my question to the group would be then, do people see that the policy should … Jim's recommending that it's not a requirement but are you recommending that they don't do it or are you just making it more—not a policy statement. It's just whatever the registries or registrars choose to do.

JIM GALVIN: So, I'll answer that right up front and just say, "That's an important question." And I think that registrars as a group, you're the ones that really have to answer that question because that gets to usability. Coming at this from a security point of view, I would say that you want one system that everybody is going to have because otherwise you don't have interoperability and then you surely have confusion. if one registrar only does two-factor and one only does one-time password, well, that's not going to work. You can't transfer between them and so that comes to bear on that question.

Whether you actually choose two-factor or one-time password, well, now there's a different set of issues, which is what I was getting at, and what you need to evaluate to choose them. So, I do think you have to decide on one. That's one of those minimum-bar homogeneity things that you have to cover if you want the system to work. Thanks.

ROGER CARNEY: Great. Thanks, Jim. And I think that that's a good point and I think everyone should think about, is it a requirement? And again, I think you had to look at it from both sides. Is it a requirement it has to be there, is it a requirement that it can't be there, or is it an optional thing? And again, I see different registrar business models that may or may not implement something like that just because of their relationship to their registrants.

But to your other issue, Jim, of the technical items that we need to talk through, I'll throw it out there. How much of that gets put into policy versus how much of that is left to implementation? And I'm not asking for an answer, Jim, just something to think about. How much of that actually needs to be policy-driven, versus implementation-driven, versus actual technical standard driven. So, just something to think about. Keiron, please go ahead.

KEIRON TOBIN: Thank you. Yeah, I agree. I think the 2FA is more of a hindrance. If it was a universal approach, I don't think it would go down well and I don't think that's the overall thing of what we're trying to achieve here, as well. I think in terms of like looking as to the best practices and stuff like that, maybe if registrars wanted to implement them themselves then, yeah, that could be optional if they wanted to add additional security into that. But making registrars … Again, as Owen said before, maybe the smaller registrars, they don't have that capability and I just don't think that would be a fair approach.

So, just to note back as well, if we do reach out to ICANN compliance, in regards to the stolen domain aspects, can we see those potentially request just go a bit more specific in regards to stolen domains request that weren't accessed from within the account? I think ICANN should be able to pull that data in terms of when it's done its investigations. But I just think if we just went on with a generic thing, I think they may send us more data than we essentially needed. Thank you.

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

KRISTIAN ØRMEN: Thank you. So, in order to give out the auth code to the registrant, there are several different secure methods. 2FA on the control panels is just one of them and we shouldn't lock us down to one specific type. In regard to 2FA as a whole, actually everybody does that today because the losing FOA is not a form of authentication. The auth code is authentication and the losing FOA is another. So, we actually do 2FA today so but that depends if we later in this version decide to keep the losing FOA or not. But it is two-factor authentication, since we have two different methods of doing the transfer in the current process. Thank you.

ROGER CARNEY: Thanks, Kristian. Yeah, it's one of the things I think about is, even some registrars force two-factor just to get into the control panel. So, your

example, Kristian, would be a three-factor for some of those that already do two-factor. So, Tom, please go ahead.

THOMAS KELLER: Thank you. Yeah, I want to add to what Kristian just said that we already have two-factors and everyone talking about two-factors authentication it has to be clear that multiple methods that can be used at multiple touch points. And currently we already have it in some way. The main problem is the current way we're having it, there can be five days in between the transfer. And this is where the usability aspect comes into it as well. So, we have lots of people calling us saying, "Well, I gave you the code and I did something there and unplugged so why it's still taking that long?"

So, at one time when we wrote the white paper as a group, we said that the transfers should be instant. And if the transfer should be instant, all the information should be there at the point of handing out the transfer code. And at a point of time, we could think about whether you want to change that [inaudible] to an obligation the registrar has at the point where he hands out the auth code and not later on at the end of the process. So, I think we need to look at the whole process a bit more holistically than just going item by item because they have dependencies under each of them or to each of them. Thank you.

ROGER CARNEY: Thanks, Tom. And thanks for jumping way ahead on us for bringing up the instant transfer idea. But now, I think it's important to recognize that this is pretty intertwined so I'm not sure that you're going to be

able to pull some pieces out without at least, at a high-level covering, the concerns brought in from elsewhere. So, I think that it's important to do what you said and what Jim had mentioned earlier, is look at the whole process from the top-down as you go through these to see where that works out.

Okay. Any other comments, questions? So, no one's arguing with Jim's goals here so I think we'll use those and we can, again, edit those, comment on those, iterate through them and see if we need to add anything to that so that we can bounce back the decisions made for each of the specific security points.

Additionally, I don't think I heard anybody going against Sarah's suggestion of the transfer authorization code. So, I think that, again, we'll use that and move forward and, again, we can iterate if people think there's a need change to that or we come up with something better later on. So, again, we'll need to reach out to compliance to see what they have information-wise and to Keiron's point, let's be specific so we're not over overreaching on all the transfers information that they have. Okay. Other thoughts, concerns? Steinar, please go ahead.

STEINAR GRØTTERØD: There's one bullet point in the b1 question, in what circumstances should the registrar not provide the auth code? I assume this is going to be discussed more in detail in the dispute section when that comes or is it essential to have it some sort of a test of it now? Thanks.

ROGER CARNEY: No. And I think we can touch on it if we want to, Steinar. Thanks for the question. I really think that this comes into the provisioning as well, a couple of sections below this as to … I think Tom even kind of hit on it in his discussion of the instant is, when and where that transfer authorization code is provided or evaluated and provided. So, I think that, again, it's one of the bullets here. We can high-level discuss it here but I think it should come up in the provisioning topics, mostly. Thoughts?

So, okay. I think that when you look at all these bullets, I think we've covered each of them. I don't know that we've gotten to the specifics. We've got about 20 minutes. Thoughts on, I guess, how far down, does this group need to get? And I think this is the important thing that Jim was kind of hitting on, the technology side of things. How far down does this group need to get to define an auth code? Should we be defining that it is 20 to 32 characters long, random, with whatever hashing needs to be done, that registrars should not store this data? Do we need to get down to that technical level? Thoughts? Jim, please go ahead.

JIM GALVIN: I would say yes, And I think if I remember everything that you just said, I would say yes to all the things that you said need to come out eventually in all of this. What I said more generally in the chat room is that to the extent there's a security impact, then it's a policy consideration and there needs to be some comments about it. There's probably different ways to phrase it so it's more of a policy than a specific implementation detail. For example, on the length

considerations, well, the standard has that built into it. We should examine all those parts and see if that's all covered, that kind of thing.

But things like, is it created as needed? Is it created at create time? Does it have a lifetime? Those are policy considerations because they most definitely have a security impact. And if we're trying to achieve a certain level of security, then we have to put in the minimum set of requirements to achieve that. That would be my advice and I think that we just need to figure out what those minimum set of rules should be. So, at some point here, we're going to have to have that discussion.

And part of this is, is from my point of view, and speaking now as a registry, my experience in watching what registrars do, it's the fact that there's variety. And some of that variety is bad choices. Let's be honest. There have been registrars who set the same AuthInfo code for all domain names and they set them as soon as it's created and that's what lives for the entire lifetime forever.

So there are certain kinds of practices like that—certain kinds of security practices that we have to get to. I believe that are important to get to in all of this and they should be part of the updated policy. If we're going to be dependent on the AuthInfo code, whereas previously we were more dependent on the follow-up in all of this system … But if the security of it, and the effectiveness of it, and its efficacy is going to do dependent on AuthInfo, then we have to say some things about AuthInfo and its management. That's what I would suggest. Thanks.

ROGER CARNEY: Great. Thanks, Jim. And I would add to that that … And I think you kind of touched on it. But yeah. I think it's not just the security but also how much of it should be standardized. And again, I think you have to balance this. How much of it's standard across all registrars versus allowing some variability, which on top of it, some variability may add to security. To your point of some registrars that set the password when it's created and it's all the same across every domain, is very concerning. And those are the things that we want to try to stop. So, Tom, please go ahead.

THOMAS KELLER: To answer that question, I would like to break it down into three groups. So, the one thing is a process so how should the process look like, how to transfer domain name from A to B and who should be involved. And that is definitely, I think, the remit of that group and that's a policy discussion. That is something we weren't able to have in any other forum. That's why we having this PDP currently.

The second group is, who is going to have the operational burden? So, we cannot have a mixed system, as Jim already pointed out that some registries, registrar has to do it and other registries, registry is doing it. This will just cause confusion and it will be a very clunky, not very customer-friendly process no one understands, probably even registrars. So the second part, I think, needs to be determined in this group as well—whether the registrar is responsible for doing certain checks or whether it is set with the registries.

And then there's a third group. This is the, I would like to call the technicality group. So, how long is a password? How long can it be valid and so on? I think this is very, very technical and I think that is something—and how is it supposed to be implemented and what are the restrictions and maybe the problems around this implementation. I think that can be passed down to the Tech-Ops group saying, "Okay. This would be our advice how to do it and this is due to normal technical standards, whatsoever, that's out there and that can be used." I don't think—I don't know, actually—whether this group is set up to have all these professionals actually being good in IT security. I'm certainly not. But the two other groups I mentioned before, these are the things, I guess, we definitely need to work out in this group.

ROGER CARNEY: Great. Thanks, Tom. And I think you kind of said exactly what Steve put into chat as well. So, I think that that's one the things to look at. And, I guess, my question is, is—Steve, and you, and I think Jim also agrees, Tom—that we talk about the technical solution should be provided elsewhere. How do we link that technical solution into the policy? Tom, please go ahead.

THOMAS KELLER: Yeah. I wouldn't talk about linking. I think this could be some kind of a request, as we have seen that with other PDPs, to the Tech-Ops group, in a certain timeframe, to come up with an answer to it. And this would be incorporated into the PDP. So, it cannot be left alone, floating there as an opinion but it would have to be incorporated by a consensus

policy in our PDP. Otherwise, I don't see that happening or being effective.

ROGER CARNEY: Yes. Thanks. And I think that was the point I was driving at is Tech-Ops did for almost two years—18 months—went through this in detail and it has a lot of good information but it's information at this point. So we need to get that put in somehow—or again, not specifically Tech-Ops but whatever a separate group or this group agrees to. So, thanks, Tom. Steve, please go ahead.

STEVE CROCKER: Thank you. I'm basically in agreement. Just one small thing to about the linkage, if you will. The registries and the registrars obviously have a very strong concern about the cost of implementation and the usability, how all this fits into their business processes. So, on the one hand, you want a system that's secure and designed by people who have the basics for doing that. And whether that's Tech-Ops or somebody else, that's fine. But you also want to know that the result of what they provide is going to fit smoothly enough into the business processes.

So, the natural tension is, are the security folks going to go too far down the path of making something that's so secure that it satisfies that requirement but is tough to use and is overkill? And on the other hand, you don't want to have a group like this, basically—no disrespect intended—trying to design something that requires a certain amount of specialized knowledge about the state of the art and cryptography and those kinds of issues. So, you need some sort of interaction there.

And what this group needs to do is say, "Here's what our concerns are," and then pass it to a technical group that is going to design something, and then have some back and forth as to whether or not that is in fact a satisfactory solution from all of the different perspectives—the security perspective, business processes perspective, usability, etc. Thank you.

ROGER CARNEY: Great. Thanks, Steve. Really appreciate it. Okay. Any other comments? Okay. So moving from here then, I know that Tom has put a name out there but I don't know if others have other ideas that would be good as a technical reference for this group to work with on this.

Tom suggested the Tech-Ops group, which for those that don't know, the Tech-Ops group is a combination of registries and registrars that meet consistently—I think it's every other week, maybe once a month now. I can't remember—but to discuss the ecosystem that they're responsible for. They try to stay within their own bounds, that system-wide aspect, and they definitely try to stay out of policy. Again, that's their goals for those that don't know. Thanks, Tom. I think it was once a month now.

Thoughts? Are there possible outside groups that we know of that could drive us to a good transfer authorization code technical solution? Steve, your hand's up. I don't know if that's still an old one. Thank you. Keiron, please go ahead.

KEIRON TOBIN: Yeah. I've noticed in the market a couple of ccTLDs have started some, let's say, interesting ideas. So, I think just as potentially looking at some of those as well would be quite interesting, just to see in terms of if we can have a look at whether that would be accumulative to the rest of the other businesses on the gTLD side.

But in addition to that as well, I think the best type of knowledge here … I know a lot of these people on the call probably do generate transfers but it's one of them where you do sometimes forget. I know me and Roger carried out something recently. And you forget every step all the way. So, if you've not recently done a transfer, honestly, it's super helpful. And if you've not done one since prior to 2018, it's changed entirely. It's just a useful step, kind of thing to do and it might help you understand a bit more of the kind of concept sof what the customers go through as well. Thank you.

ROGER CARNEY: Great. Thanks, Keiron. Okay. Just doing a time check. We've got about five minutes to go. I think we can stop here for the day. Again, just a reminder. Be on the outlook for the SO/AC letter, it should be out in your email coming soon. So, just take a look at it. See if we're asking the right questions. Right now, it's basically just all the charter questions and looking for responses. But look for additional questions to add and any comments on the ones that are going out. So, again, we need all the comments back by June 24th.

And again, speaking about next week, we have our meeting next Wednesday, I believe. And we will be covering, again, something that

we've kind of started here but the goals of this group, the goals of the transfer policy. We're planning on splitting that time evenly to cover the goals, which now is kind of making me think the goals, maybe leading into the process itself—the transfer process/business process that goes into it—which will lead us into the AuthInfo discussion the second half of next week's meeting. So, I will open this up for last comments, questions from the group. Emily, please go ahead.

EMILY BARABAS: Excuse me. Thanks, Roger. Just one housekeeping item that we haven't heard any concerns about the time that we're currently using for this call on a reoccurring basis. So in light of that, we're going to go ahead and start sending out invites for July and August. So, just a reminder that there's no meeting the week after ICANN71. And then, beginning on the 29th of June, we'll continue to meet weekly at this time slot. Thanks.

ROGER CARNEY: Perfect. Thanks Emily. Again, so, just if you didn't catch that, we'll meet next week, obviously for ICANN71—off a week and then back at the end of the month. And at that time, we're hoping to finalize the letter and get it sent out for SO/AC input and SG input. Okay. Anyone else? Emily, your hand's up still? Is that an old, new?

EMILY BARABAS: Old hand. Sorry.

ROGER CARNEY: Okay. Thanks. Okay. All right. Well, great discussion. I think this will lead in well into our discussion next week at ICANN71. So I want to thank everybody and I'll give everyone a whole three minutes back.

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

[END OF TRANSCRIPT]