ICANN72 | Virtual Annual General Meeting – GNSO Transfer Policy Review PDP Working Group
Tuesday, October 26, 2021 – 10:30 to 12:00 PDT

CAITLIN TUBERGEN: Hello and welcome to the GNSO Transfer Policy Review PDP Working Group Session. My name is Caitlin Tubergen, and I am the remote participation manager for this session. 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. I will read questions or comments aloud during the time set by the chair 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 at a reasonable pace. Please remember to mute your microphone when you are finished speaking.

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

ROGER CARNEY: Thanks, Caitlin. Welcome, everyone who made it to ICANN72, the last ICANN meeting of the year. A good spot for our Transfer Working Group, actually, since we worked mostly through the summer. Our first meeting was ICANN71, but we had just got kicked off. So this is good timing for us. We've gotten a lot of discussion behind us now and our

path moving forward clear. So it's looking good. So let's go ahead and jump in and take a look at our agenda for today.

All right, pretty straightforward. I'm going to just give an update on where we are. Staff will give us an update on our status and everything, and then we'll jump into continuing our discussion on additional security measures which, for those that participated last week know, a lot of our discussion last week was on certain locks put on by registrars or registries. And we'll continue those discussions and try to get some answers to our charter questions or at least down those paths. And then we'll finish with Any Other Business or questions. So let's go ahead and jump in.

Emily, are you going to take the status update?

EMILY BARABAS: Hi, Roger. Thanks. Hi, everyone. This is Emily Barabas from ICANN Org. I am one of the staff members supporting this working group and will provide a little bit of context for those who are less familiar with the group about what it does and where work is currently so that you can follow along in the discussion afterwards.

So first, as a review, what is the Transfer Policy? It's an ICANN consensus policy governing the procedure and requirements for registrants to transfer their domain names from one registrar to another registrar, also known as an Inter-Registrar Transfer. It was formerly known as the Inter-Registrar Transfer Policy or IRTP. It went into effect originally in 2004, and this current review is the second review of Transfer Policy.

The first one took place shortly after it went into place. Next slide, please.

So a brief overview of the PDP itself. The purpose of this PDP is to conduct a holistic review of the Transfer Policy to see if changes are needed to improve the ease, security, and efficacy of Inter-Registrar Transfers and also Inter-Registrant Transfers, which are transfers from one registrant to another.

There is one charter for this working group, two phases. And eight topics covered in the working group. We're currently in Phase 1A which began in May of this year. And Phase 1A focuses on two pieces, the Forms of Authorization (Losing Form of Authorization and Gaining Form of Authorization) and Auth-Info-Codes. And we'll go over a little bit of background around those topics in just a few minutes.

Where are we now? The working group has done some initial deliberations on the charter questions covering all of the items in Phase 1A and has begun to think about what some possible recommendations could be. And we'll go over where the group is on that the end of this presentation.

The people who are actively participating in this working group are members and sometimes alternates. These are representatives of the supporting organizations, advisory committees, stakeholder groups, and constituencies. Anyone can sign up to observe. That's completely open. But the core team of members are representatives of ICANN's community groups.

So if you're interested in this group and you're a part of one of these SO/ACs, SGs, or Cs, you're welcome to reach out to the members who represent you and learn more about the group's work. You can also provide input that way. Next slide, please.

So like many—well, actually all of the PDPs now in the GNSO—we do monthly reporting to the GNSO Council to let them know how we're progressing, what the status of the work is, and whether we're on target for the goals and the work plan. So this is a very brief dashboard that provides a snapshot of where this working group is. We're at approximately 25% completion in Phase 1 of the work.

And the key takeaways here are that we have some target dates in the coming periods. The goal is to publish an initial report for Phase 1A in June of next year, an initial report for Phase 1B in March of 2023, and then a combined final report taking both of the inputs from the two initial reports into a single document. And that final report is slated to be published in August of 2023. Next slide, please.

So this is just a tiny bit of background for those unfamiliar with some of the topics that are being discussed in Phase 1A. The first one is Auth-Info-Codes. Sometimes these are also called Auth-Codes, Authorization Codes, Transfer Keys, Transfer Codes. There are a bunch of different terms that are used, but the core concept is the same. The working group has been working on a definition that can be included in the recommendations, and so we've included that here. And it's also looking to recommend a unified term for this which is "Transfer Authorization Code" or "TAC."

So this slide uses the term that's included in the charter, but “TAC” is going to be the term that the working group is looking to use going forward to reduce confusion about different terminology.

So, what is the TAC or Auth-Info-Code? It's a token—and when we say “token” we're really talking about a digital token; so a passcode, essentially—created by the Registrar of Record. That's the registrar at which the domain is registered. And it's provided upon request to the registrant or a designated representative.

So how is it used? It's required to transfer a domain name from one registrar to another registrar. And when it's presented, it is the authorization needed for the transfer to proceed. The Registrar of Record, which is also called sometimes the Losing Registrar, typically provides that code via the control panel, but it can also do so by other means such as e-mail and, upon request, needs to do so within five calendar days. Next slide, please.

So a few terms. “Gaining Registrar” is one that you'll be hearing. That's the registrar to which the registrant is transferring the domain name in an Inter-Registrar Transfer.

Losing Registrar. We were just talking about that. Also known as the Registrar of Record. That's the registrar from which the registrant is transferring the domain name.

So in the Transfer Policy, there are two what are called Forms of Authorization that are required. So this is what's in writing currently in

the Transfer Policy, and in a moment we'll talk about what's actually happening in practice which is a bit different.

But in the policy itself, there's a requirement for what is called the Gaining Form of Authorization. This is a form that the Gaining Registrar is required to send to the Registered Name Holder to confirm that the Registered Name Holder, or RNH, does intend to transfer the domain name. This is typically in the form of an e-mail and the RNH can confirm that intent by clicking on a link in the e-mail. And before the European General Data Protection Regulation, that transfer could not occur without the confirmation.

The second Form of Authorization is the Losing Form of Authorization. This is a requirement for the Losing Registrar to send the RNH a notice confirming that intent to transfer. Absent an objection to the transfer within five calendar days, the Losing Registrar can then process the request. Next slide, please.

So prior to the European General Data Protection Regulation, the Gaining Registrar would confirm the transfer contact using the public Registration Data Directory Service. And then they use that publicly available e-mail address to send the Gaining FOA to the RNH, the Registered Name Holder.

But things changed with GDPR, as many of you know. And much of the personally identifiable information in the RDDS was redacted, and therefore it was unavailable to the Gaining Registrar.

So the Temporary Specification for gTLD Registration Data, or the Temp Spec, was adopted by the ICANN Board in May of 2018. It partially amended the requirements in the Transfer Policy to address those situations where the Gaining Registrar is unable to send the Gaining FOA because it can't obtain current registration data via the RDDS. So then in those cases, a transfer could proceed without the gaining FOA.

So an Expedited Policy Development Process (or EPDP) on the gTLD registration data chartered to review the Temporary Specification and provide policy recommendations based on the Temp Spec. And it included the workaround from the Temp Spec in its recommendations which were then adopted by the ICANN Board.

Subsequently, the registrars identified that there were challenges in ICANN Org's position that the Gaining Registrar needs to send the Gaining FOA where the e-mail address is available because in some cases, there's no guarantee that that e-mail will actually reach the registrant. So the ICANN Board reviewed these concerns and ultimately passed a resolution different Contractual Compliance enforcement of the Gaining FOA requirement, anticipating additional work in this area.

I'll just mention one other thing, which is that the Contracted Party House's TechOps Subcommittee, which is a group formed in 2017 by the Registrars and Registries Stakeholder Groups—and it works to look at technical and operational issues that are encountered by the Contracted Party House and develop potential solutions—they developed a proposal on a proposed transfer process that the working group has been drawing on in its deliberations. Next slide, please.

So in order to make sure that the group is being as transparent as possible and providing regular updates to the community, we're going to talk a little bit about some of the potential recommendations that the group is considering. But I want to provide some caveats here.

The group is still relatively early in its work. There have been some really great and robust discussions and some really interesting outcomes of those discussions as well. As I mentioned, they've gone through all of the charter questions in Phase 1A at this stage at a sort of high level, and then it's been an iterative process.

So after the group has gone through each topic, staff has gone back and tried to consolidate the deliberations into some draft text that then the group is coming back to look at now, reflect on, refine. In some cases, potentially, they will completely throw out some of these, what we're calling, candidate recommendations. So they're not even draft recommendations at this stage. They're just candidates.

But it does give you a sense of where the group is going, what they've been talking about. And so we're going to share that here with those caveats.

So as an example, one of the things that the working group has talked about quite a lot is the Losing Form of Authorization, or Losing FOA. The group went into a detailed discussion of what function does the Losing FOA serve, or what functions? So for example, it has a function of notifying the RNH that the transfer has been requested and it's in process. It also provides what we're calling a paper trail function. So it

provides a record that can be drawn on in investigating complaints or disputes about unauthorized transfers.

But the working group also identified that there are some challenges with the Losing FOA, including that it can delay transfer for up to five days. And in some cases, and potentially in many cases, a registrant wants things to move as efficiently as possible when they're initiating a transfer.

So in this case, the working group is looking at some candidate recommendations to potentially eliminate the requirement for the Losing FOA, but essentially replace it with a series of notifications that can serve the similar functions but potentially have some gains in terms of efficiency. So as an example, the group is considering both some notifications that would be mandatory for registrars and others that might be optional.

So for example, the working group is looking at a mandatory notification when the transfer Authorization Code is provided and another potential mandatory notification when a transfer has been complete. Those would both let the RNH know when there's a status update related to a transfer and also provide information about what to do if this is unauthorized and they would like to stop or reverse the process.

Another area that the working group has considered in a lot of depth is the TAC or Auth-Info-Code and how security can be increased for the TAC to help ensure that unauthorized transfers are minimized. So I'll just run through a couple of examples here.

The working group has considered potentially creating minimum requirements for TAC syntax or complexity and having the registry potentially confirm or verify that the TAC meets those requirements.

That the Losing Registrar generates the TAC upon request instead of producing it and having it sort of sit there until it's needed.

That the TAC may only be used once. So once it's been used to initiate a transfer, a new tack would need to be generated to be used as the token for an additional transfer. But the TAC is valid only for a limited period of time, but it essentially expires. This is referred to as “time to live.”

And, finally, that the registry must securely store the TAC using a one-way hash to protect the TAC from disclosure at the registry level.

So with these additional security elements that the working group is considering around the TAC and some of these new notifications to ensure that the RNH is clear on what's happening, the working group has also looked at the requirement for the Gaining FOA.

And this is the one, as we mentioned earlier, where, on policy, the Gaining FOA’s required. In practice, there's compliance deferral. So in practice, the Gaining FOA is not something that's used operationally for the most part. And so one of the things the working group has been looking at is, has there been an evidence of increase in unauthorized transfers with the transfers occurring without the Gaining FOA.

I know that some working group members have sort of, at this stage, contributed that they believe that the transfer process is working rather

well without the Gaining FOA and therefore, with these additional measures, it's not necessary to include the Gaining FOA or a replacement in the policy requirements. Of course the Gaining FOA could not be required as it currently is, but there is the possibility of requiring something that would essentially replace it with a different mechanism for the Gaining Registrar obtaining the e-mail address of the registrant from the Losing Registrar.

So I'm not going to go into a great deal of detail, but the working group is, for the Gaining FOA, working on sort of picking apart the elements of what the Gaining FOA has done, how it might be addressed through other measures, and developing a more detailed rationale for why it might be possible to eliminate that.

If you do have questions about any of these pieces, the best thing to do is to go to the members that represent your group. If you don't know who those people are or you're not part of a group that has a member in the working group, you can reach out to staff and we can help you find the right resources to make sure that you can follow along if this interests you.

I think that's the core of the background. So maybe I will, unless there are any questions, I can pass it back to Roger to discuss what comes next in the agenda.

ROGER CARNEY: Perfect. Thanks, Emily.

EMILY BARABAS: Sure thing.

ROGER CARNEY: Yeah, if anyone has any questions on that, please feel free to raise your hand or throw them in chat. We can definitely provide some input. And as Emily mentioned, we've done a lot of work and discussion and come to some high-level agreement on some things. But it's definitely early, so if anybody sees something of concern or something that they think could be improved, obviously we're looking for that input. So it would be great to have.

Berry, please go ahead.

BERRY COBB: Thank you, Roger. Just one small correction to the presentation in regard to Phase 1A scope. After the group has reviewed through all of the components related to a single domain transfer, we do still have some charter questions related to both transfers that we'll tackle afterwards. Thanks.

ROGER CARNEY: Thanks, Berry. Yes, that's a good reminder that we have one more set to get through. Okay.

We're going to jump into what the working group's been working on. We started this last week. But if anybody has any questions about what we've covered already so far—the background and where we are—please don't hesitate to drop it in chat or raise your hand. This may get

a little dry for some people as well we'll get into some detail here. So just kind of forewarning everyone that you probably saw the exciting part. This will probably get a little monotonous for some. But that's why we're here because we do all this dirty work on the back so it looks good on the front kind of stuff.

Let's go ahead and jump in. I don't know if anybody's … It does look like Sarah has taken a look at this already. But this was put together after our meeting last week, this chart here. And it just outlines, not all of the locks, obviously, but the ones that may pop up into the discussion. So we wanted to see and get them down so people can see what we're talking about and what they mean and where they come from.

So I think that staff put this together after our call last week just because we got, on the call last week, a lot of discussion back and forth on the different locks and where they came from and where they're required or where they're optional. And I think that this chart will help out a lot. And if we're missing one that we need, we can add it in here. But also add any comments or anything to help explain things here as well.

So I think that one of the big things, and the one that's highlighted here is really relevant to the charter question that we looked at last week. And the charter question allowed us to get into a good discussion last week, but I would say the majority of our discussion last week was probably not specific to the charter question itself. A lot of our discussion dealt with things around the charter question instead of

specifically a charter question which was good because I think all those discussions needed to happen.

For clarity so everybody understands exactly what locks we're talking about, that discussion obviously had to happen. And again, that's why this chart was produced.

I'll open up to the working group to see if anybody has any questions or comments on this chart here itself. We'll get more specific into this first one and the charter question at hand, but I wanted to open it up to see if anybody had any questions or comments on the chart itself. No? Excellent.

Okay, so let's get into this first item here, into the specific charter question that we're trying to answer. The charter question is charter question a6 that we're dealing with, and it specifically says, "Survey respondents noted that mandatory domain locking is an additional security enhancement to prevent domain name hijacking and improper domain name transfers. The Transfer Policy does not currently require mandatory domain name locking." It allows a registrar to NACK an Inter-Registrar Transfer if the Inter-Registrar Transfer was requested within 60 days of the domain create or within 60 days of it being transferred.

I think the key here, it allows the registrar to NACK it. It doesn't say that they have to NACK it for those reasons. So the charter question really is, is mandatory domain name locking an additional requirement that the working group believes should be added? So should we change from

optional? Should there be mandatory pieces or should some pieces be optional?

I think that's where it falls down as this 60-day transfer, does it have to be mandatory that you can't transport? You have to NACK it, deny the transfer. Or are there reasons to allow the transfer in that window? So I think that's what the charter question's trying to get at.

I think this this first line here is really what we're talking about. The registration, I think a lot of registrars apply locks by default when … And I think someone mentioned it last time. Not even if it's truly a lock, but at least it's a soft lock that the registrar's watching even if it's not truly locked at the registry.

Jim, please go ahead.

JIM GALVIN: Thanks, Roger. Jim Galvin from the Registries Stakeholder Group. A comment about this domain locking. Just an issue for us to complete the discussion on.

I'm pretty sure I've mentioned this before and I just don't see it captured here at the moment yet. There's the statement there in the charter question that "domain locking is an additional security enhancement to prevent domain name hijacking." But I think, to be clear, that's not true of all domain locking. A lot depends on two things.

One, the assumption that a registrar locking it is going to prevent domain hijacking is dependent on good account protections because if

someone can hijack a registrant's account, then the locks being present or not being present are fairly straightforward to remove. So there's no additional security enhancement there. So there's a dependency there and security features.

And second, if we're talking about even Registry Lock, because we've had some separate discussions about Registry Lock being an additional hijacking protection. But we've also had discussions—it's at least been mentioned—the idea of automating Registry Lock. And I've even said at that time that, well , again, you have the same kind of problem that you have with the account at the registrar. Right? Which is that if it's automated and I lose control of my account, then it doesn't really matter whether the lock is present or not because I can presumably just turn it on and off.

So the implementation of a lock choice matters and there's a dependency on other security features. So it's important if we're going to go down this path of suggesting this that we fully capture those details and lay all of that out for proper implementation. Thanks.

ROGER CARNEY: Great. Thanks, Jim. And I'll just note that Registry Server Lock is mentioned down below further as a separate item. But to your point on the lock here, I think that's the key. Right? If we say that there's a mandatory "day" window—60-day today—if there's a mandatory locking, then realistically if someone gets a hold of someone's account it doesn't matter because it can't be transferred for 60 days.

And again, yes, they could remove a client-side lock possibly. But if the rule was, in the policy, that this couldn't be moved for 60 days, then I think that's where it gets into the discussion of, okay, if we're saying that has to happen, then that can be controlled multiple ways. And that may be that the registrar's doing it. But as you point out, that may get hacked or whatever it is.

But then if it's also done at the registry, then they would have to be able to get both ways done somehow. And I'm not saying it's not possible to do. I'm just saying it becomes more difficult task if you have to hack the registrant's account or the registrar's account and the registry's account. So just a comment on that, Jim. Thanks.

Jim, please go ahead.

JIM GALVIN: So I think I'll take a step back and more generally make the statement that the concern that I have with some of these stated security features is that there is a relationship between them and we need to capture that particular point and recognize that so that we can talk through the details. In particular, even the notion of the 60-day lock. In order for that to be effective, you're assuming participation by the registry.

And then again, there's a set of procedures that go around that being overly effective. If that's a problem you're trying to solve, then you have to make sure that you manage that feature in a way that provides service to the registrant. So for me it's about the dependency of the features.

It's challenging to talk about them in isolation, is my concern, because there is a relationship. And I just don't want to lose that point as we get through this whole process. Thanks.

ROGER CARNEY: No, Jim. And I think you're right. I think that is important. I think that's really important because we don't have the answer here yet, if we're going to make it that way or not. So I think those dependencies have to be known so that people can make that decision.

I'm not assuming the registry is going to do anything here or the registrar is doing anything here. To your point, once we know those things we can make that call as to which way that goes.

Whoever wasn't on the call last week, Zak had, I think, drawn the line in the sand because he said, basically, let's leave it optional for this to happen. But it being optional, let's make the process defined when you do either lock or not lock. So I think that one of the things that we're looking at is …

Anyway, I think that's Zak's the only one that put out there his opinion of "let's leave it as an optional feature." I didn't hear anyone say, "Let's make it mandatory. I think Zak got a couple plus ones last week on making it optional. But I think that's where we're looking at now.

Okay, let's go ahead and jump in. And maybe Caitlin can run through this document for us so that everybody gets a more holistic view of what's been started and, to Jim's point, where we can actually fill some things in.

Caitlin, do you want to take that?

CAITLIN TUBERGEN: Thanks, Roger. Certainly. And I think Roger provided a good overview of why we created this document, but I did want to note that staff went through the relevant ICANN policies and contracts do identify what kind of locking measures are required in different instances. And so there's a column where it says “Origin,” and we're guessing what the origin is in certain instances.

And in instances where we are unsure of the origin, we've marked out with an asterisk. So for example, in the first row, the origin, we believe, is a registration agreement where a registrar might, by default, lock a domain name. But that's not a requirement of ICANN, so that's the registrar’s choice to do that.

And of course the charter question is looking at, should all registrars be required to do this by default? Which is why this row is highlighted in purple.

But I thought it may be helpful to go through all of the types of locks that we've identified, noting that there may be additional locks that working group members are aware of that we didn't find. And by all means, that's why we have a Google document so others can contribute.

And also, if there are any errors in the notes or the origin or the length of the lock, by all means, we are looking for everyone's feedback to make sure that this is as comprehensive and accurate as possible.

So we already discussed the charter question and the mandatory locking by default. The next lock that we identified that most folks in the working group were familiar with is the post-Change of Registrant lock. That is required by the Transfer Policy Section II.C.2. That is a 60-day lock that happens after a registrant makes a material change to its contact information. And a material change is defined as a change to the prior registrant name, organization, e-mail address, or administrative contact e-mail address.

Some notes that we added to this lock is that if a registrar offers, a registrant may opt-out of the 60-day lock. There is no policy-mandated specific EPP code that's required to be set for registrars in this lock. They just have to make sure that once a change of registrant occurs, the registrant cannot switch registrars unless they have opted out of that lock prior to that change of registrant.

So moving along, the next lock we identified is a lock subject to a UDRP proceeding. That is a requirement in the UDRP rules, Rules 4(b). The length of the lock is the pendency of the UDRP proceeding. Registrants can't opt-out of that lock. So generally speaking, once a registrar receives notification of an active UDRP proceeding, the registrar is required to lock the domain name from Inter-Registrar Transfers through the pendency at that proceeding. And the UDP provider would notify the registrar at the end of the proceeding to unlock the domain, transfer the domain, etc.

If there is an Inter-Registrar Transfer request during the pendency a UDRP proceeding, registrars must NACK that transfer again because

registrars are required to ensure that no Inter-Registrar Transfers occur during UDRP proceedings.

I noted here that, again, there's no specific EPP code that registrars need to assign or set during a UDRP proceeding, but most registrars would typically apply the clientTransferProhibited EPP code.

The next lock is the Redemption Grace Period lock. That's covered in ICANN's Expired Registration Recovery Policy, Paragraph 3.2. This is not within the scope of this group, but this is just for sake of comprehensiveness. That lock last for 30 days following the deletion of a domain name. This is a lock applied by the registry operator. There is no opt-out. And during the 30 days following a deletion of a domain name, registries have to prohibit any Inter-Registrar Transfer requests , subject to the ERRP.

Next, we have the post domain creation lock. This is something that is included in some registry agreements. We have a registry representative in our group that noted that this is something that Verisign has as part of its registry agreement. It's also included with some other registries and their registry-registrar agreements.

Again, it's a 60-day lock. Folks that are familiar with the Transfer Policy might recognize this as one of the reasons that registrars are permitted to NACK a transfer, and that's because the name is locked pursuant to the registry's lock.

Staff had some questions here. We presume that in some cases when it's subject to a registry agreement, there is no opt-out of this lock. This

is a legacy requirement that some registries have baked into their registry agreement and it flows down to the registrar via the RRA.

Typically the EPP code set by the registry would be serverTransferProhibited. And just as a note, again this isn't a lock that's required by ICANN. ICANN doesn't mandate this across all registries and registrars, but again it's also not prohibited. As we noted during last week's call which cause some confusion, this is not applied consistently across registries and registrar. So there might be some user confusion when it comes to this type of lock.

The next lock is the post Inter-Registrar Transfer lock. That is also, we believe, subject to registry-registrar agreements or the registration agreement. It is also a 60-day lock. And, again, if a registrant transfers its name to another registrar, some registrars will lock it for 60 days pursuant to their RRA. It's also included as a reason that a registrar can NACK a transfer. Presumably, this was implemented so that a registrant can't just keep hopping along to registrars if there's some sort of issue going on. This would prevent that.

Again, in most cases, we assume there's no opt-out of this lock, but it depends on what the source of the lock is. If it's the RRA, there probably is no opt-out. But if it's just a registrar-applied security measure or choice, then maybe there is an opt-out.

Again, ICANN's contracts or policies don't specifically mandate this type of lock, nor do they prohibit the lock. So similar to the post creation lock, there is an inconsistent application across registrars which, again, might cause some confusion.

The last lock that we identified is the Registry Lock Service. This is something that we presume is also part of registry-registrar agreements. The length of the lock is indefinite.

And we noted that some registries offer an additional service where they will apply a registry lock or a server lock as an added measure so that the name can't be transferred. Even if the registrant goes into its client portal at the registrar and tries to transfer the name, the registrar would have to reach out to the registry to remove that lock. So there's an additional layer of security. Not all registries offer this.

And again, this would be something that if, perhaps, someone had a highly valuable name, they may want to apply an additional security measure so that if someone hacks into their registrar account they still won't be able to move the name without registry intervention.

So that concludes the locks that staff has identified. As I noticed as a disclaimer at the beginning, there might be some other types of locks that registries or registrars offer that are not included here. We did have a column that notes if the type of lock is in the scope of the PDP charter, but in terms of the additional security measures topic, as Roger mentioned a few times, the first column that's highlighted in the mauve/purple/lilac—call it what you'd like—row is the one that we are talking about in terms of the charter question that's identified for additional security measures.

So I think that will conclude my speaking portion of the chart. But the Staff Support Team worked on this together and we're happy to answer

any questions that folks may have. Thanks, Roger. I'll hand it back over to you.

ROGER CARNEY: Great. Thanks, Caitlin. I appreciate it. I see Sarah asked a question about row one and, I think, row six or something later on about the post creation locks. Just to be clear, row one is dealing with the registrar putting—and I think we say it here—typically a clientTransferProhibited upon registration. And really that lock, as this indicates, doesn't have a set period of time. Most registrars just put that lock on there for a security reason, just that one extra level of work that needs to be done to do anything with this domain.

And the later one is more talking about the 60-day locks like Barbara brought up last time that Verisign does on their new registrations. So it's two different time periods and kind of two different things happening there. That's why there are two rows.

Sarah, please go ahead.

SARAH WYLD: Thank you, Roger. Hi. Thank you so much to the staff team for putting that together and then walking us through it right now. I really appreciate it.

Roger, yes, that completely makes sense. And of course they should be two different rows. I just would really like if we could see the similar things side by side. Like if this were in spreadsheet form, I would move

the rows around. So here we have two locks that exists upon creation. Right? There's this purple one and then there's one lower down. So hopefully that can just be shifted around a bit so I can think about it better.

And then I do have questions. So my questions are, number one, in the Origin column, what does the star beside "registration agreement" refer to?

And number two, is this lock in the registration agreement or is it in the Transfer Policy? Because the additional note section says … Well, I think actually I understand why. It's because the removal is governed by the Transfer Policy but the ability to apply it is under the registration agreement. Is that the deal? Okay, thank you.

ROGER CARNEY: Thanks, Sarah. And I'll let Caitlin talk to that asterisk and what it means. Caitlin, please.

CAITLIN TUBERGEN: Thanks, Roger. And thanks for the question, Sarah. That's a good question since we didn't have a key of what the asterisk means.

Essentially the asterisk just denotes uncertainty on the Staff Support Team side. So in some cases we weren't sure if it was part of an RRA, the registration agreement. It's generally things that when ICANN Org isn't a party to the agreement and we don't have full visibility into the text, we were just venturing a guess. So if that's incorrect, by all means

please change that and make additional notes. But it's just because we were unsure.

ROGER CARNEY: Thanks, Caitlin. When we look specifically at our charter question a6, it is dealing with this first row. And if this lock that registrars do—[I'll just go ahead and tell you]—many registrars do upon creation, is should this lock be mandatory or optional or just allowed, I guess, it's probably the third option there. And I think if you look at it today, as Caitlin just mentioned, it is kind of just allowed. So it's not talked about either way, specifically. But I think that a few of the responses, early comments back, were looking at not making it mandatory but making it optional. And as I mentioned, Zack mentioned that last week as well.

So I would say specifically to charter question a6 and its specific question of should it be mandatory or not, I think what the working group is saying is that it should be optional or …

And again, I'll throw it out. Are we saying it should be optional or are we saying it just should be allowed? Which I think is the same, maybe? But I don't know if optional implies maybe if you do it, then you have to do something else. Where if it's allowed, then there are no other factors, I guess. I don't know.

But thoughts on that—saying that we're not going to make it mandatory or we're going to leave this optional; and if you do select this, what has to happen again. Obviously, if a registrar does lock it upon creation, one of the things they have to do that the current policy

talks about is remove that lock upon request by the registrant or give the registrant the ability to remove it themselves.

Okay, so again, a6 we're saying is optional. Any concerns? Comments? Questions? Okay.

And I think one of the big things here and one of the things we've talked about throughout the group is—thanks, Keiron—the registrant experience, trying to keep it as consistent as possible across registrars. So if we do leave this optional, I think the task for this group is to come up with the process that if it is used, what has to occur after. Meaning, obviously, like it does today that registrars have to give the ability to the registrant to remove it or remove it upon request. One of those options.

And I don't know if there are other things that we want. No? Yes?

Okay. Berry, please go ahead.

BERRY COBB: Sorry to rain on your parade for just a second. I think one thing is kind of clear from this chart, and for lack of repeating myself, I think it's clear that there's a fair amount of confusion about what locks do what until we had this table, and I don't recall necessarily the prior IRTPs going into this kind of great detail to parse these out.

But I am recollecting, I believe it was Zak's question from our last call, where he was referring to the 60-day lock as it relates to the creation of the domain name and how that is applied or applied inconsistently. And I'm wondering if there's maybe an opportunity to get some more

information about what Zak's concern is in that regard. Not that it's necessarily a part of our scope for this particular charter question, but I think it may help inform our deliberations when we get a little bit further down the stack, so to speak.

ROGER CARNEY: Great. Thanks, Berry. And I agree. It's interesting because it I think we've answered the question to a6, but I think the question itself kind of brought up further questions on the other locks. And as you mentioned, were we're going to talk about some of those anyway during our "reasons for denying," but there's no reason not to discuss them now and get them documented so that we have that available to us.

I don't know if Zak wants to jump on or not, but I think when you look at the registration cycle, that first 60-day lock that Barbara kind of confirmed for us last week happens. And I don't know if Jim can tell us if that's consistent for Donuts as well or not any of the other registries can tell us if that's consistent at their registries.

That first 60-day lack, consistent, is that a hard lock as it's mentioned in here? I think Caitlin mentioned that there is no way to opt out. Is there actually no way to opt-out of it if someone registers a name? Are their processes in place that allow it to be transferred even within that first 60-day window for those registries that have that? And again, maybe that's in the registry agreement. Maybe that's in the RRA. I don't know. But I just wanted to bring that forward so we can discuss it here.

Berry, please go ahead.

BERRY COBB: Thanks, Roger. And perhaps I'm still not going to be clear enough, but I think at least from a staff perspective what we learned from this exercise is that the charter question that prompted all of this would probably be slightly different in that it was confused with the denotation of the 60-day lock.

And that's really what kind of prompted me to make sure that we're being precise here. And it really does lead into the reason why this very first row is labeled as mauve or lilac, I think, is the technical color. And that really is the scope of what the intent of the charter question was now that we recognize that there is a separate lock that may or may not trigger that 60-day duration.

ROGER CARNEY: Great. Thanks, Berry. Okay, any other comments? I think Berry's getting this refined just to …

And I think it kind of leads back to Jim's discussion of dependencies. But as Berry mentioned, when this charter question was created, the discussion that we had from this charter question led down several different paths. And again, as he mentioned, this first row is very specific to the charter question. But answering those or going down those paths and understanding them is still important. And I think we'd still like to get those answers on the 60-day lock.

The charter question itself mentions both the 60-day creation lock and 60-day transfer lock, and also then brings this into the point that

registrars usually put a lock—and again, probably an indefinite lock—on domain creates at registration time.

I see there's a lot of talk going on in chat. Hopefully, answers are coming through. I haven't kept up with it completely.

Okay. I think that when we're looking at this, the charter question being specific to this first row here, it's the registrar lock that was put on here that wanted to be answered. So I think we've answered that, but I think we need to resolve the 60-day creation. And again, all the paths we took down the 60-day transfer, I think the 60-day transfer is less confusing. Though, obviously, there's the Change of Registrant 60-day that also affects that which has an opt-out which makes it a little more confusing. So there are multiple paths to go down.

Okay, so everyone clear on the different locks? Why they're there? What you can and can't do with them?

When we start talking about reasons for denying a transfer or the possible reasons for denying, this discussion is going to continue because several of the reasons for denying are these windows. And it may not specifically be a hard lock, as someone mentioned last week. It may be that someone's just watching the time and it's been within that window, still, so they're going to not allow it.

Again, that lock on the domain at the registry may not exist, but the time window still does. Quiet group today?

Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. So you're saying that with the NACK reasons and so on, if we end up in a scenario where we decide not to have the Losing FOA and we have transfers that go through directly, then the Losing Registrar will not be asked to ACK or NACK a transfer. So we don't have those NACK reasons anymore as we had in the current policy. I just wanted to flag that.

ROGER CARNEY: Great. Thanks, Kristian. That's important when we start talking about, to think about some of the decisions that we've made already. Or not even made, but have talked about. And we've always talked about trying to be as efficient in the process as we can be and obviously not get immediate transfers, but get transfers that flow through much quicker; and obviously, flowing through much quicker than you had to start. And the whole purpose of this is to start looking at the security and making sure that it's secure enough to allow those things to happen quickly.

But to your point, once the once the registrar has the TAC, the Losing Registrar loses that ability to stop the transfer. There's no stopping the transfer from the registrar's perspective. Obviously, the registrant doesn't have to go through with it, but the registrar can't stop it for any reason. And it's one of the reasons I think some people wanted to maintain the five-day request period, to make sure that they can validate those things up front before handing the TAC over.

The Losing Registrar could check that it's within or outside the windows and allowable before providing the TAC. But to Kristian's point, once the TAC has been presented to the registrant, for all purposes that domain is now transferred. Okay.

So we've talked about a few of the locks here—all of the locks that we have come up to and run into—but the section actually is about additional security. And I know that we've done quite a bit, actually. We've changed the Auth-Code considerably. We've changed one-time use. We've made it so that it's transfer-bound, that it only exists while the transfer's being processed. So we've added quite a few additional security things, but a lot of that's tied to, specifically, the Transfer Authorization Code.

Other ideas of additional security or additional—not even security, but mechanisms for enhancing the accountability, the traceability, the audit trail factors, things like that? Any additional things that we could be doing to improve this?

Anyone have thoughts on anything else? Everyone's thought-out on security measures or principles here? Again, I know we talked a lot about notifications and enhanced features on the TAC. One of the things we never really talked about is—I brought it up once or twice—is should we put in the Transfer Policy requirements around registrar and registry—certain logs that they must maintain for this process? Do we need to put that in the Transfer Policy? Thoughts on those.

Jim, please go ahead.

JIM GALVIN: Yeah. Thanks, Roger. This might not be the right place for this question, but I figured since you both said we're talking about locks and then we're talking about additional security measures, is this a place where folks want to talk more about multi-factor authentication and its potential role or non-role and in the overall account managing? Thanks.

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

SARAH WYLD: Thanks, hi. I'm not sure that multi-factor authentication is something that we want to include in our policy. As you know, it's very clearly related to being able to log in and access the account. And I think that's something that different providers have different methods for, and requiring it to any degree seems like a really big step for us to take. So definitely we should be cautious, and I'm not sure we should do that. Thank you.

ROGER CARNEY: Thanks, Sarah. Yeah, and when I think about it, it's one of those things where it's like, okay, I understand what Sarah is saying is that we don't want to control or force certain multi-factors on registrars. I mean, a lot of registrars do their own and have different ways of doing it. But maybe I can take Jim's point a little further and not really …

And I think we talked about it early on once or twice, not speaking of the registrar's portal or anything about two-factor because that does exist. And I know people ask if it should be required from registrars, and again, I think I go on the side of what Sarah is saying. I think that flexibility's important as different registrar business models have different needs when it comes to multi-factor.

But going along Jim's point, is there a multi-factor piece of transfers that's possible? And maybe it doesn't even make sense. Maybe it gets too complicated that when you transfer something and you have a TAC, is there something else that's needed to make that happen?

But again, does that get too complicated or does it add enough security that it makes sense to do? Just thoughts.

Jim, please go ahead.

JIM GALVIN: Thanks, Roger. In the spirit of just thoughts, I'm not trying to present anything in particular because I don't have a vested position here. But earlier one of the things I was emphasizing is, as we talk about security measures, one of the things that's important about security measures is that they also have to be thought of together. And we have to think about how they help each other when we'd like to think they don't typically hurt each other. But they do tend to help each other, and we shouldn't make assumptions about any one particular feature when it obviously has dependencies on other things.

So we have previously, in other meetings, had discussions about multi-factor authentication, and we are trying to focus just on transfers here. And I do believe that, at least in our discussions before, the sense of the room was that we didn't want multi-factor authentication on a transfer, per se.

So I'm bringing up the question again here, not in that context but in this context. And that is that some of these security features … I mean, multi-factor authentication is itself a security feature, and so whether or not its present may help. Or if it's not present, then it's neutral with respect to what we're doing. But you get a certain value out of multi-factor authentication that some of these security features that we're talking about here—these locks, their presence or non-presence. We worry about hijacking in terms of account things. I mean, if were to make a comment about the fact that accounts that have this protection have additional protections that mitigate hijacking, that may play it how we think about these other security features we've got going on here.

So it's more about taking note of the fact that it may or may not be present. And maybe we should say something about its presence during transfers if it exists rather than saying it should be or shouldn't be, but if it is these are the benefits you get of it with respect to transfers.

And I hope that's not too much, but just a thought to put out there in terms of completeness in what we're trying to document here. Thanks.

ROGER CARNEY: Thanks, Jim. Yeah. Just to go down your line of thinking is not to force a mechanism of multi-factor but mentioned the fact that that it adds to the security features of what we've already done if it's present or not and go from that.

And it's one of those where when you start talking about—and you can take it beyond registrars—but registrar portals. Some registrars require multi-factor on certain things and not on all things. So you can go in and make a change and it may not require a two-factor acknowledgement. But to change your name servers, maybe that does. But doing something else doesn't. You can update … I can't even think off the top my head.

But it's kind of like the banking system where you can go in and look at your account balance and stuff or transfer money between your own accounts, but when you transfer money to someone else's account, they require another authentication. So it's one of those where …

And again, I think you get back to the registrar models. Different registrar models have different use cases for those multi-factors.

Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. You know, it's funny that you say that sometimes people require two 2FA on something but not on something else. Because the thing I wanted to say was that in the current transfer process, I believe there's some wording around that it must not be more difficult to get

the Auth-Info TAC than doing a lot of other operations. And I can't remember the exact ones, but changing fields in the domains, I think.

And while I understand how we don't want to get it to be too difficult to transfer between providers, I think we might want to consider if we still want to have this requirement because, as you just mentioned, maybe someone would want to have 2FA on giving out the TAC but not on changing names servers. And at least that's something we should consider, not making it too difficult to make more security around it if a registrar wishes to do so.

ROGER CARNEY: Great. Thanks, Kristian. Yeah, that's a good point to bring up. I don't remember where exactly where that's at, but yeah, it's on the name servers. It can't be more onerous than the name server change. But obviously, if a registrar does two- or multi-factor on all operations, then it isn't any more onerous. But if they get more fine-grained, then should that still apply? I think it's a valid question.

Berry, please go ahead.

BERRY COBB: Thank you, Roger. And picking up on what Jim mentioned, as well as Sarah's comments in the chat, in terms of scope and creating or discussing/deliberating additional security measures as it relates to the Transfer Policy is considered within scope. Now there might be a question about how far it could be considered a consensus policy recommendation or not. And I think that's for the group to decide that

the vision would be whether this additional security measure is something that is enforceable from ICANN and, again, for the group to decide.

That said, when reviewing the GNSO Operating Procedures and working group guidelines, there's nothing that would prevent the group from making a recommendation around guidance or best practices, or at least making a notation that as part of implementing the policy, that perhaps—and as an inclusion to the consensus policy—that there is implementation guidance.

And as Jim noted, perhaps there is information of language that could be included that's not "consensus policy" but could help implementations of the policy understand the pros or cons or consequences of implementing two-factor authentication or not when making these changes.

So, put a shorter way, there is some leeway about introducing guidance to try to make attempts at enhancing the overall security apparatus of what the group is deciding here. Thank you.

ROGER CARNEY: Great. Thanks, Berry. And I think that, as Maxim put in chat, best practice/guidance is not a requirement, but it's still … I think the thing is that it's important to recognize the fact that multi-factor adds security to the features that we've already added.

As Maxim points out, obviously that wouldn't be required, but we can show that we recognize—and I don't know if we encourage it or not—

but we recognize the fact that multi-factor is a good practice on top of these additional features we've added.

Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. I just wanted to say that what we could consider to include in the policy is that it is allowed for registrars to require 2FA on the TAC even in situations where that registrar would not require 2FA on other actions on the domain. That should be within policy and something we could include in the policy. Thank you.

ROGER CARNEY: Thanks, Kristian. Good idea. Sarah, please go ahead.

SARAH WYLD: Thank you. Apologies. I think I'm basically going to repeat what a few other people have said. But I just want to emphasize that I do think it's important that we put boundaries on both sides of this. With the comparison to how difficult it is, or easy, to change the name servers, we can't make it too easy to transfer the domain but we also can't make it too hard. Right? We have to make sure that domain owners are able to choose their provider. Thank you.

ROGER CARNEY: Great. Thanks, Sarah. Okay.

Thanks, Jim, for throwing that idea out on the multi-factor. And I think maybe Kristian probably hit on maybe the crux or the way to address multi-factor in our Transfer Policy by allowing it even if it's a little more difficult than other operations. It's mentioned somewhere, and again I can't say exactly where. The main server change and the Auth-Code can't be any more difficult which would mean registrars technically couldn't apply anything additional to the TAC that they don't apply to the name server.

Okay, multi-factor. Thanks, Jim. Anything else? Does Jim have another one that he's thinking of back in the back of his head that's like, "Oh yeah, maybe …"

Anybody, really, any thoughts on additional things that we can come up with. And again, maybe it's not our policy like we're staying here, but maybe we just make sure that it's not blocked or not allowed.

Owen, please go ahead.

OWEN SMIGELSKI: Thanks, Roger. While we're on the topic of whether or not locks should be there, or additional security locks, I just wanted to … I know you probably know this since the registrars do, but I just wanted to let the rest of the team know that after this meeting we're planning, as part of the Registrar Stakeholder Group, to do a poll of the membership to see what various types of locks are desirable regarding transfer and creation. And then there's also what type of timing for those locks. So

just kind of a heads up, and we'll be able to share that with the rest of the team at an upcoming meeting.

ROGER CARNEY: Great. Thanks, Owen. Okay, any other additional questions? Additional security or …

Oh, Sarah's going to come up with a good one. Sarah, please go ahead.

SARAH WYLD: Thank you. This is I guess more of a process question. So I like that our charter is requiring us to consider security measures. I think that's great.

Did we brainstorm a list of security measures that we should consider all of them? Because so far we've talked about locks. We've talked about MFA. We talked about verification e-mails or notifications that something is happening. Those are security measures. If we haven't yet brainstormed other possible security measures to consider, that might be a good use of our time both on the e-mail list and in a meeting so that we can make sure that we have thoroughly considered everything. Thank you very much.

Oh, and also just to say I don't have other specific things in mind. I'm just saying we need to make sure that we cover everything we can think of. Thank you.

ROGER CARNEY: Great. And as Berry mentioned in chat, maybe we can set up a Google Doc with the brainstorming ideas of other measures. I don't think anything can be discounted. I think, throw in anything. And maybe it doesn't apply or doesn't work at this time, but maybe it's for future discussion or at least acknowledgement that it's there.

Jim, please go ahead.

JIM GALVIN: Yeah. Thanks, Roger. Jim Galvin for the record, for the Registries Stakeholder Group. I want to call out a question for clarity that jumped out at me as Sarah was talking. I agree with the idea of a list of which security features we're using, and she mentioned notifications as one. So that's an element of a security presence—notifications, making sure that people know what's going on and stuff.

But the thing that occurred to me is that Sarah jumped on the use of e-mail as a notification mechanism. And it occurred to me—at least I know that I missed the last week's meeting in particular—but we were very careful in prior meetings to not want to be overly prescriptive about mechanism to leave that option open for others. And I just wanted to call that out and make sure that was [still there].

I see that Sarah's saying in the chat "good point" so, okay, so I did capture that. Notifications is the feature that we don't want to lose track of, but we want to be careful about how prescriptive we are about what kind of notification and the mechanism by which it's achieved. Thanks.

ROGER CARNEY: Thanks, Jim. And I would argue that leaving that flexible actually provides a security enhancement. If we say it has to be one way, then it may be a little easier to abuse if we leave it open, especially with technology changes. If we leave it open, going forward could be definitely a security enhancement.

Before I let Owen go, I note that Caitlin had her hand raised. But she can't raise it [inaudible]. But I'll let Caitlin go before Owen.

CAITLIN TUBERGEN: Thanks, Roger. I'm actually reading a comment from the chat. And this is a comment from Steinar.

The comment is, "I am in favor of adding wording that describes a requirement for registrars to make access to their control panel in a secure way. Of importance is also the distribution of the TAC to the registrant-designated name holder. I find it strange that two-factor authentication is enabled for accessing a control panel and then the TAC is sent in an unsecured way (e-mail)." Thank you, Steinar.

ROGER CARNEY: Great. Thanks, Caitlin. Thanks, Steinar. Yeah, and I think that's exactly why Jim wants to avoid that discussion of how it's sent and prefers that distinction of "a secure mechanism" is better than saying by e-mail or by however choice you want to—what's the—carrier pigeon or whatever it is.

But Owen, please go ahead.

OWEN SMIGELSKI: Hi. Yeah, carrier pigeon. I support us discussing what other options are. Maybe a little brainstorming that could be included in the report. Again, Jim kind of stole my thunder there. We shouldn't be too prescriptive because what we've got today might work. Somebody might develop carrier pigeon technology in the coming years that might be better than the other secure methods. So maybe we can do something similar to what's in the 2013 RAA now about "using a secure method of transmission" or something like that but then kind of give some background and context to that.

ROGER CARNEY: Great. Thanks, Owen. And I agree. I think going down that … And again, we've purposely tried to avoid specifically mentioning a mechanism because e-mail can be secure if you put the time into it. But it definitely takes some work to make e-mail secure.

Okay, I know there's some chat going and a little bit of back and forth on how to include multi-factor, if it should be in this policy or not. Again, I'm not sure that we have a stance on requiring registrars to have multi-factor, but I think that we acknowledge as a group that multi-factor is a good security mechanism. We're not forcing anybody to use it or not, but that we recognize that.

Owen, your hand is still up. I assume that's old. Thank you.

Okay, we have five minutes to go. I think this is a good spot to wrap up. Berry mentioned that staff will generate a Google Doc for us to start brainstorming on. And I think Sarah through in chat several items as she thought about it—security mechanisms that we added or changed, updated. Especially, according to the TAC, we did quite a few different things there, but also the notifications and things like.

And I think that, as this group has done all along, we iterate through these things and we'll come back to a lot of them. And this additional security mechanism can be one of those where we chug along and we'll find something later on or we can identify as many as we can now that work out well.

So we'll do that and take a look at the Google Doc that was put together and add your thoughts to it between now and next week. And we can touch on that as we move forward.

Okay, four minutes to go. I don't know if we have anything else. Any questions/comments from anybody? Especially people that aren't into this every day like this working group is. Any comments from anyone else or does staff anything?

Oh, yes. Thanks, Emily. We do not have a working meeting next week. We're going to skip our normal Tuesday meeting next week and go with the following Tuesday. So it'll be two weeks from today.

Okay, anything else? Okay, great. Well thanks, everybody. And we'll talk to everybody soon, I'm sure. Thanks, bye.

[END OF TRANSCRIPTION]