ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2
Tuesday, 29 October 2019 at 14:00 UTC

Note: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.
Attendance and recordings of the call are posted on agenda wiki page:
https://community.icann.org/x/L5ACBw
The recordings and transcriptions are posted on the GNSO Master Calendar Page: http://gnso.icann.org/en/group-activities/calendar

TERRI AGNEW: Good morning, good afternoon, and good evening. Welcome to the EPDP Phase 1 Team Meeting, taking place on the 29th of October 2019 at 14:00 UTC. In the interest of time, there will be no roll call. Attendance will be taken through the Zoom room. If you're only on the telephone, could you please identify yourself now?

We have apologies from Ashley Heineman and she is formally assigning [inaudible] for her alternate fort this call. Alternates not replacing a member are to remain on the line by adding three Zs to the beginning of their name, and in the end in parenthesis, their affiliation-dash-alternate, which means you are automatically pushed to the end of the queue. To rename in Zoom, [inaudible]. Alternates are not allowed to engage … Oh, no. It may just be my audio. I apologize in advance. I'm trying not to move, just making sure I can get a clear audio.

To rename in Zoom, hover over your name and click "rename". Alternates are not allowed to engage in the chat, apart from private chat, or use any other room functionalities such as raising hands, agreeing or disagreeing.

As a reminder, the alternate assignment must be formalized by the way of the Google assignment link. The link is available in all meeting invite emails towards the bottom of the email.

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 any assistance updating your statement of interest, please email the GNSO secretariat.

All documentation and information can be found on the EPDP Wiki space. Please remember to state your name before speaking. Recordings will be circulated on the mailing list and posted on the public Wiki space shortly after the end of the call.

Thank you, and with this, I'll turn it back over to Janis Karklins. Please begin.

JANIS KARKLINS: Thank you, Terri. I saw that you do prerecorded messaging. It seems that you are reading it every time. So, thank you very much for reminding us. Team, good morning and good evening. Welcome to the 28th meeting of EPDP Phase 2 team.

Traditional question. Agenda in front of you now on the screen. Is there anyone who cannot agree to follow that proposed agenda during the call?

It doesn't seem to be the case. Then we can start with housekeeping issues. The first of them is some information that ICANN Org shared with the team through me the document that has been sent to European Data Protection Board containing questions in relation to UAM model.

So, the document is lengthy and I hope that some of you already had the chance and others will have a chance to read the document very carefully on the way to Montreal. And before opening any discussion, I would like maybe to encourage team members to think if there is any questions – clarifying questions – that team may wish to convey to the CEO, the President of ICANN, upon his invitation that could be further submitted to the European Data Protection Board.

Again, I would not like to open any substantive discussions on this document now but we will do it certainly in Montreal. For the moment, if there is any questions or clarification, that would be time to raise those. I realize Milton. Please go ahead, Milton.

MILTON MUELLER: Hello, everybody. So, I was on the impression that we had a liaison from the Strawberry Team sitting with us in most of our meetings and that we were going to be given a look at this before they send it to the EDPB. It doesn't seem like that happened. So, this is a procedural question. Just what's going on with this?

JANIS KARKLINS: Thank you, Milton. I recall, during our Los Angeles meeting, the Strawberry Team said that they would be very hesitant to share with the team questions prior to sending them off, but they promised to share them as soon as they would be sent out to the Board. So, as a result, I think this is in full consistency with information we received during the previous engagement in Los Angeles. I see Alan Greenberg, Amr, and Chris Lewis-Evans, in that order. Alan?

ALAN GREENBERG: Thank you very much. My comment is very similar to Milton's. My recollection is different from yours and I have let to look at the transcript to see if my recollection is imagination or not. I remember Elena saying that they did not feel comfortable sharing the document with us prior to sharing it with their EU partners who are helping to refine it and they didn't want to share it before their partner, their support group, had seen it, but that we would see it prior to sending to the Data Protection Board. Our memories seem to be somewhat different. Thank you.

JANIS KARKLINS: Now when you are saying this, Alan, yeah, I recall you're right. So, this is what we were told, indeed. Amr, please?

AMR ELSADR: Thanks, Janis. I have a lot of impressions of what was in that document but I'm not going to go through them all now. But since I won't be in Montreal with you all, I just wanted to share my kneejerk reaction to the document as a whole. My suggestion would be that we do not attack any questions to this report at all. In fact, I think it would be wiser for the EPDP team to distance themselves from this document to the extent possible. I think there are a lot of assumptions that ICANN Org has based its rationale for proposing the UAM that they are proposing and a lot of these assumptions are [inaudible]. So, I don't think that they reflect any consensus within our team at all and I would just recommend that we not try to … Since this process has been moving in parallel with ours and with little to no consultation from us, I would recommend that we not formally engage with it and the European Data Protection Board in any way. So, I just wanted to share that now. Thank you. And I'd be happy to send more details on my thoughts on this when the time is more appropriate. Thanks.

JANIS KARKLINS: Thank you. As I mentioned, I will propose to go through the document and discuss it in substance during the meeting in Montreal Saturday m morning, so in one of the first sessions. Maybe if you want to share it, that would be time to do it, for that moment. Alan, I think this is your old hand. Chris Lewis-Evans, please.

CHRIS LEWIS-EVANS: Thank you, Janis. Just a quick one for me that I think might be helpful for the whole group is I know in LA there was talk about when the next EDPB meetings were, when this letter was going to get considered, but obviously that was dependent on when the Strawberry Team got this letter out. So, I think it may be helpful for us as a group to be able to consider this with some timeframes attached to it, so when they expect responses back and their next steps. So, be able to help us look at the document in a better picture. Thank you.

JANIS KARKLINS: Thank you, Chris. I think, in Montreal, we were told that the procedure, how the Board would look at the questions. So, they would send it to the expert group and the expert group would review them, propose an answer – a draft answer – to the Board and then Board would sign it off. The timetable, if I'm not mistaken, was sometime during the month of November, since the expert group is meeting sometime in mid-November. So, this is my recollection. And as you saw from the email, CEO suggested that he would share whatever response he will get with the team as soon as he will have it. Georgios, please. Hello there, Thomas.

GEORGIOS TSELENTIS: Yes. I wanted to add a little bit on the information about this process. You recall well that there was a need for prior consultation before getting the whole document to the Board. So, what happened was also my colleagues that have possibility with [inaudible] have possibility to talk informally with the Belgian DPA who is the DPA responsible to deal first with this matter. They forwarded the document after making some very editorial remarks on this. So, practically what was sent was what ICANN Org was having there in the initial draft.

So, this was sent to the Belgian DPA, hoping to have what initially was the idea have an informal first look on this before reaching the European Data Protection Board.

Now, because the time of this process was compressed now and I understand that ICANN Org wanted to have, if possible, some answers from the Board before Montreal meeting, in my opinion, this would be unlikely but this is why I understand ICANN Board sent this document at this stage and at this form before last Friday. I don't recall exactly the date where they sent it.

So, the status is as follows. The Board is now – the European Data Protection Board and the Belgian DPA are informed about this. Now, how they are going to respond [inaudible] which timeframes, for me it's unlikely to happen in time before our meeting. So, it's unlikely that we have an answer. If we do, and we have even the informal reply from the Belgian DPA, I asked my colleagues in [inaudible] to enlighten us and I will look forward to any response that I find that might be useful to the EPDP. That's for the process. Thanks.

JANIS KARKLINS: Thank you, Georgios, and it would be appreciated if you could share whatever insights you have in terms of possible timing of the reply. Even informal indication what would be the [inaudible]. Thomas, please, you have [inaudible].

THOMAS RICKERT: Thanks very much, Janis. I would like to put on the record that I am not happy with the way this went. I do recollect the discussions that we had in LA and I think it was we explicitly asking for the document to be shared and we learned that, at least in the first [inaudible], immediately we wouldn't get it, but it was my understanding that we would get it prior to it being dispatched to the European Data Protection Board.

There's a lot of talk in the ICANN community and with the Board about volunteer fatigue, volunteer burnout. I think this is exactly what nurtures this notion. It causes frustration for volunteers that spend hours and hours of their time on these projects to then see that their efforts are being bypassed by the [inaudible].

Also, there's a lot of talk about protecting and defending and advocating for the multi-stakeholder model at a global level, not having parallel initiatives with potentially contradictory approaches undermines the multi-stakeholder model big time.

So, as a group, I think we need to discuss – maybe not today but maybe in Montreal – how we're going to deal with this. I think it's important for the global community to note that, if at all, our group is at the steering wheel when it comes to policy making, and if we agree that it is our group and not some other group to determine policy, then we should I think put out a statement clarifying that. Otherwise, we might come up with a report at some point and folks say, "Okay, but there was this other document, so which one is decisive? Which is the document that shall govern the community and the contracted parties?"

So, I think – or I hope – to have made this sufficiently clear. I'm extremely frustrated with this approach and I think that we need to put something on the record clarifying that this document has neither been reviewed, nor endorsed, by a group and that the outcome of our group might potentially undo or [inaudible] paper. Thank you.

JANIS KARKLINS: So, thank you, Thomas. Look, let me maybe suggest the following. Indeed, we may feel some frustration that there are is a follow-up process. From other side, we knew from the very beginning that there is a Strawberry Team, that they are working on something. We have been interacting. Also, we knew that Board has given task to CEO to clarify one possible model – or feasibility of one possible model.

From the very beginning, also, all of us, we were cognizant that we are working with developing a standard where UAM potentially might be one of several options. So, I don't think that this is completely contradictory.

We may end up taking elements of UAM. We may be ending up not taking anything from UAM. It depends. So, we are not yet there. We are asking questions to ICANN Org about centralized model versus decentralized model, where the decision of disclosure should be made, what implications that may have on liability of contracting parties and so on.

So, all this is because we are developing our own thinking, our own model, and I would say if the Data Protection Board will come with a very clear-cut answer, so we will simply consider that answer and we'll factor in, in our own process. So, this is how I see the situation we are and I am personally looking forward to interaction with the Strawberry Team in Montreal.

What I would like maybe also to ask team members, starting with Amr who will not be in Montreal, maybe you can formulate some questions you may wish to ask the ICANN Org in advance, as well as think whether there is any questions that as a team would like to ask to European Data Protection Board. I heard some team members already saying that we should distance ourselves from this report but that does not exclude that we cannot ask questions to European Data Protection Board, especially when we are invited to do so by the CEO.

Again, it's entirely up to us to define a course forward. I'm looking forward to this conversation in Montreal. I recognize Milton.

MILTON MUELLER: Yes. Janis, I just want to explain why I don't think we need to be devoting a lot of time to this, particularly in Montreal or in our face-to-face meeting. I think I disagree with your approach to this procedurally.

We've been told that this team is not a parallel process that is preempting what we do, and yet every action that has been taken is in fact a preemptive and non-consultative step. So, I think since the questions that we ask of this entity will have no impact on it does, and since we have to do our own work, which will have impact and which will ultimately be the deciding factor of the policy, I don't understand why we are even engaging with this bootleg process. I just, really, I'm beginning to resent the time being spent on it and any kind of interaction of the sort you're suggesting seems to me to legitimize this bootleg process which has no legitimacy. Thank you.

JANIS KARKLINS: Thanks. We'll factor that in, in our planning. Thomas, your hand is up or it's an old hand? I see it's an old hand. So, let us move maybe then … Margie?

MARGIE MILAM: I do share some of the concerns about not having shared this before talking to us. But on the other hand, I don't think I agree with what Milton has said, that it's a bootleg process and doesn't have impact on us. If we actually get answers to the questions, I think it would affect our process and it would affect what we come up with in the policy. So, I just want to encourage us to keep an open mind and see what comes from it.

Again, I don't agree with the way it was conducted, but if we do get answers, it might actually help us.

JANIS KARKLINS: Thank you, Margie. Alan?

ALAN GREENBERG: Basically, what Margie just said. We may not like how it was done. We may or may not disagree with what was asked but we will likely get some feedback from the Data Protection Board and I don't think we can ignore that because that's relevant to our work, whether we liked how it was created or not.

So, distancing ourselves from the report and saying we're going to ignore the answers doesn't make any sense at all to me. But how it was done does, as Thomas was saying, indicate a certain disdain for the multi-stakeholder model and our involvement.

I understand the timing issues and, at the very least, it should have been sent in parallel or given us 12 hours' notice or something like that, just as a courtesy. Thank you.

JANIS KARKLINS: Thank you, Alan. Greg, did you try to raise your hand? You don't need to speak if you haven't. So, Amr, your hand is up.

AMR ELSADR: Thanks, Janis. I just really disagree with what Alan just said and Margie before him. I think any responses that ICANN gets from the EDPB, if it gets any response at all, will not be helpful to us because I believe it is based on all these premises that I don't see the EPDP team having any consensus on. I think ICANN really did a number in terms of laying out the context for the UAM as well as the questions that they're asking – in many cases, proposing strange ideas like that the UAM is actually a benefit to the registrant in one way or another, when I just completely don't agree with that premise. And whether I personally do or not, there is formally no consensus within the EPDP team to that effect.

So, any responses we get will basically be to premises that just [inaudible] exist. So, I very much support Thomas's earlier recommendation to draft up a statement to the effect of distancing ourselves from this document and playing out exactly where it is that EPDP team is right now, as opposed to the way ICANN Org has portrayed that. Thank you.

JANIS KARKLINS: Okay, thank you. Look, we will have a chance to have this conversation further with Strawberry Team in Montreal and I would suggest that we now turn to our next agenda and that is accreditation building block and see how far we can get today with this particular building block. I see Marika is trying to show a picture of the building blocks. There, unfortunately, hasn't been change. We have made progress, and actually I would like to recognize the activity of team members in following the proposals for accreditation building block and it is my hope that today we will be able to stabilize that building block in principle.

So, let me now ask secretariat to put on the screen the accreditation building block text.

MARIKA KONINGS: Janis, if I may.

JANIS KARKLINS: Yes, please. Yes, Marika, please, go ahead.

MARIKA KONINGS: I just wanted to flag that, as we discussed on the last call, we have added an additional Google Doc for the policy principles. As you recall, those were in the zero draft and we haven't had a chance yet to discuss those, so we're hoping that by adding them here, you'll at least all have a chance to review those by Wednesday, as you know, especially flagging which ones are really not necessary for inclusion in initial report, which ones may be missing, or which ones are no longer aligned with other work that has been undertaken in relation to the building blocks.

I also wanted to note that we have followed up with a couple of you that had action items in relation to some of the other building blocks. We're trying to get all that language in and update the building blocks accordingly, so that you hopefully have a final version and [inaudible] really hope to get all your input in by Wednesday at the latest and we'll basically cut off comments at that time and use that input as the basis for discussions in Montreal.

JANIS KARKLINS: Thank you, Marika. Let us now go to the building block F. I would also like to ask team members maybe at this stage, not really editing and wordsmithing. For the moment, it would be extremely important to get all the concepts right and understandings correct. So, therefore, I hope that we will be able to go through the document swiftly since a number of proposals have been made, so now we need only to see whether they meet consensus or common understanding. Then maybe also answer questions if needed.

So, with this, let me turn to the first five points, starting with A, accreditation, accreditation authority, accreditation authority auditor, identification, and authorization. Any particular issues with the text on the screen?

There is a question from ICANN Org and I at least actually want to outline that question or do you want me to read it out? [Eliza] is asking how accreditation authority may be implemented. What is the purpose and role of accreditation authority? What are criteria for selecting accreditation authority? Does EPDP team envision the role to be played by ICANN Org or this role that must, may, should be contracted to a third party. Alex?

ALEXANDER DEACON: Thanks, Janis. I read this question last night and had a few thoughts. I think that there's still some work to be done in cleaning up the language in our shift from my original framework which assumed multiple third-party accreditation authorities, to our current model, which is, essentially I think what we are saying is that the accreditation authority is going to be – that role is going to be managed and played, if you will, by ICANN Org.

Whether ICANN Org wants to outsource that to a third party I don't think really is our business, but I think if we think about – if we agree that it is ICANN Org that is going to be playing this role, there's probably still more work to be done with regard to cleaning up the language. A picture always helps, at least for myself who is more visually oriented, in terms of how this all fits together, similar to what I did earlier in our previous thinking about this topic.

One thing that occurred to me that is missing – again, I think I'm giving myself more work here – is that we've agreed, I believe, in principle, that there would be a single accreditation authority run by ICANN Org and they would be able to outsource to I guess zero or more identity providers to help them with the vetting and validation of identities. So, I think we probably need to flesh that out a bit.

So, those are my thoughts with regard to this question and I guess I'd be curious to hear from others, especially regarding whether we just need to state out – be explicit that ICANN is going to play this role. Thanks.

ALEX DEACON: Okay. Thank you, Alex. Marc Anderson, please.

MARC ANDERSON: Thanks, Janis. I support Alex. His explanation is pretty much in line with how I understand it. I think he said ICANN would be responsible for this role, which I think is important. Ultimately, what we're envisioning is they have responsibility for this. How they actually manage it, whether they subcontract parts of it out to other people, whether they hire a vendor or have somebody develop a software or system to do it, I think that's fine, as long as ultimately ICANN is the responsible party for this particular role. So, I think that's at least how I've understood our discussions and deliberations to this point.

JANIS KARKLINS: Okay. Thank you, Marc. So, any opposing view on this? I see none, so then you have an answer to your question. Any other comments on As? I see none, so let's then go to credentials. Alex?

ALEX DEACON: Yeah. One of the actions I took last week was to clarify the terms validate, validation and verify and verification. So, you'll see … I don't want to jump ahead, Janis, but this kind of relates to the credentials section here. You'll see I defined those terms, which I won't read out, and I went through the doc and kind of scrubbed it to make sure we were using them consistently. I guess I urge everyone to take a look and make sure they're comfortable with those definitions, which again I leveraged from an RFC on security definitions, so it's "standard" I guess in the industry here and we are sticking with [their] suggestions with regard to these terms, valid/validate/validation and verify/verification. Thanks.

JANIS KARKLINS: Thank you, Alex. Any reaction? Milton?

MILTON MUELLER: Just a quick EM. Alex, you got a thing with capital Vs or was it, you just said, a slip-up in your global search and replace. There's something funny about that. Not a [inaudible].

JANIS KARKLINS: Yeah. Okay. Thanks.

ALEX DEACON: Can I just respond? So, wherever we have a … What I tried to is wherever we have a defined term – so, validate, for example – and I use that defined term in the text – so, for example, the definition of credential, or later on, I use the capital V – so it was clear that everyone knew that we were using the definition that we have defined here in the doc. I've seen this used quite often in other docs. Not too sure if it's happened at ICANN. I think it's helpful, but if we don't, then we could change it.

JANIS KARKLINS: Okay, thank you. Now, [revocation], the user accreditation. There was no change. So, de-accreditation. There was a question on the accreditation and answer. Any issue with the text in yellow? Seems no problem.

Identity provider. No … James? Please, James, go ahead.

JAMES BLADEL: Sorry, Janis. I apologize that I was a little late in finding the right window to raise my hand, so thanks for your indulgence. But going back to de-accreditation authority. Just noting Sara had posted a comment from the Registrar Stakeholder Group that we really think that there's a lot more that needs to be discussed and fleshed out here, particularly what happens to those credentials that have been issued by an accreditation authority and what a process would be either to revoke or reassign those credentials. I think there's a lot of missing pieces under this bullet point.

I'm okay if we don't dive into those right now, but I think that we do need to flag them for follow-up. Thank you.

JANIS KARKLINS: When you say follow-up, you mean implementation or you mean later stage, James?

JAMES BLADEL: I believe implementation. Correct.

JANIS KARKLINS: Okay. So, that's easy. Everything we can push to implementation, I think it saves our time. But you're right. There are … And also, I recall, actually there is a comment that de-accreditation of accreditation authority should be really a last resort. There should be also some remedies put in place in case there is some elements that need to be improved. I see Hadia and then we'll move on. Hadia, please.

HADIA ELMINIAWI: So, I do agree with the point that Sara raised and what James also was referring to. But I would say that, yes, it is an implementation issue, but we should put a few lines that refer to protecting the accredited users if de-accreditation to the authority, and especially if it would be one only accreditation authority. If this happens, what happens to the accredited users? So, maybe we could put a few lines that ensure that there won't be a point where all accredited users have no means through which they can access the system. Thank you.

JANIS KARKLINS: Okay. Thanks, though we're in the definition section. So the action or recommendation sections are below. We will get there.

So, identity provider. James?

JAMES BLADEL: Thanks. Just to respond to Hadia, maybe we do need a little bit more work here because I think Hadia is correct but it would depend upon the circumstances and the nature of why the authority was de-accredited. It is possible that their universe of accredited users contains perhaps some invalid, or even fraudulent, credentials. So, that's why we are drawing some parallels with things like SLL certificates. Whenever an authority is compromised, you have to take a look at all of the credentials issued by that authority and some of them may be revoked or transferred.

Look, I think we flagged it as this is something that we really need to spend a little bit more time on, either here or in implementation, but I don't want to hold up today's call because our time is limited today. Thanks.

JANIS KARKLINS: Thank you. I asked staff to put note and keep that issue somewhere on the agenda. Alex?

ALEX DEACON: Yeah. Thanks, Janis. Just quickly, I'll just state something I put in the chat. If ICANN Org is the only accreditation authority, then perhaps the concept of de-accrediting ICANN from that role doesn't really make sense. And again, as I mentioned earlier, maybe the focus should be on – again, I'm overloading terms here but de-accreditation of any third-party identity providers it may use. Again, I think we need to think about this. I agree with James. There's a little bit more work to be done here.

JANIS KARKLINS: Yeah, but we have the letter in the text, the de-accreditation of accreditation authority, and then this is subpoint Q that we will get there. And there are a number of issues that we will respond to the concern that James raised. So, let us wait until Q and move on, on the rest. Identity provider. Georgios?

GEORGIOS TSELENTIS: I don't know if it helps to use a little bit what we have in the previous bullet point where we say about revocation. So, I understand that de-accreditation is probably the complete and maybe severe, let's say, action by which we revoke definitely the accreditation authority from its powers. So, could we go towards a suspension or something which is softer until further notice or something like this? I don't know if people believe that would solve the problem instead of going to this discussion about whether de-accreditation and who does the de-accreditation under which conditions. I'm just wondering if this can solve the issue.

JANIS KARKLINS: Yeah. Now, look, let us move on and once we will get to subsection Q, then we can discuss whether we de-accredit or change the term. Then we subsequently [inaudible] would change the term in the definition. So, any problem with identity provider? Revocation? Validate, validation? Verify, verification? Okay, so then we are done with this subsection of definitions.

Let us now move to the recommendation part. So, A, it was modified by staff based on our previous conversation that the SSID can be used only by accredited users. Any issue with subpoint A? Marika?

MARIKA KONINGS: Thanks, Janis. Just to flag that there's actually – not a comment from [Eliza] to the sentence preceding point A in relation to the reference to framework. So, her comment is, "ICANN Org has questions about how to implement the concept of a framework. Can the team clarify what the relationship is between the policy to framework and the SSID?"

JANIS KARKLINS: Okay. Alex?

ALEX DEACON: Yeah. Again, this may be text that we can remove, assuming the decision has been made that ICANN Org is going to be the accreditation authority, then basically you don't need a framework. We just need a policy for that accreditation authority and we could clean up the language accordingly. Thanks.

JANIS KARKLINS: Okay, thank you. Alan Greenberg, followed by Marc.

ALAN GREENBERG: Yeah, thank you. I think this needs some clarification saying we only support accredited users or organizations or individuals, and then say it somehow accommodates one-time users. One single request lacks clarity. It's not clear if they must go off to the side and accredit themselves before making the request or exactly how that would work. So, I think this needs some level of clarity to explain how it accommodates individual users, which also must be accredited. Thank you.

JANIS KARKLINS: Thank you. I will take Marc's comments. Marc Anderson?

MARC ANDERSON: Yeah. I note that Alan is responding to A and Alex and I are both trying to respond to [Eliza's] question. I guess I think I agree with what Alex said about framework but I want to make sure I understand exactly what [Eliza] is asking. It sounds like she's wondering what does the word framework mean in this context. We're recommending that ICANN establish a framework and I think she's asking, "Well, what do you mean by framework?" But if [Elize] is on the call, maybe it would help if you could clarify or provide a little more context on exactly what you're asking.

JANIS KARKLINS: Okay, thank you. I think that Daniel will step in. Daniel?

DANIEL HALLORAN: Thank you, Janis and Marc. Can you hear me?

JANIS KARKLINS: Yes. Please go ahead.

DANIEL HALLORAN: Okay. I think [Eliza] is not in a place where she can talk right now. I think, Marc, [inaudible] understand that we're trying to understand what's the difference. You've got these building blocks. They'll eventually become the policy recommendation. Then there's the separate discussion about a framework and it wasn't clear to us who makes that framework and when and where that happens in the context of the PDP and the implementation work. That would be something for the IRT to do or for ICANN Org to do. Basically, what would be in this framework and what's the purpose of it aside from the policy and ultimate documents that constitute the SSID? Thanks.

JANIS KARKLINS: I feel that this is a little bit synthetic discussion. So, building blocks. We're using building blocks to develop, to take a chunk out of the whole construct we're talking about and working specifically on building blocks which will ultimately turn in policy recommendation. All of them begins with EPDP team recommends, and then the policy recommendations follow.

So, [inaudible] a construct – working construct – that we're developing for the sake of convenience during our work. It may stay as SSAD, but ultimately, it may be called differently at the end. So, these are not really issues of substantive nature.

So, answering Alan's question, I think – or at least how I was [inaudible] that and I didn't hear any objections last time when I presented that idea – that if the request is filed through probably some kind of interface, answering question, "Are you accredited?" if answer is, then the path goes to the one side saying, "Okay, if you are not accredited, then please provide A, B, C, D," whatever documentation. Then that would be processed and a decision on accreditation, the [lighter]-scale accreditation would be taken. And only after that, the request would be processed.

So, for the accredited organizations, entities, individuals, they would answer in this interface, "Are you accredited?" Yes. And then provide your whatever credentials, typing in or synchronizing with the device, and then request goes straight for processing. And a sentence here is suggesting that this is a kind of slow track and the fast track for accredited and non-accredited users. I see Marika's hand is up and Daniel is not satisfied with my explanation. Marika, please, you go first.

MARIKA KONINGS: Yeah. Thanks, Janis. Just to note, I think, maybe to address Alan's comment. I think it might be an easy fix in the last sentence to add accreditation to requirements or at least the accreditation requirements for regular uses of the system and a one-time user of the system may differ. So, hopefully, that adds clarification [inaudible] to accreditation is required for both, but there may be differences in what criteria apply for regular users versus one-time users, which I think you just described very well.

JANIS KARKLINS: Okay, thank you, Marika. Daniel? Oh no, that was an old hand. So, with Marika's explanation, are we now okay with the subpoint A? Okay. With B, we are fine. With C?

So, there was, again, a question from [Eliza] concerning ICANN Org question about how this principle for the [inaudible] might be implemented, preferably seems to indicate that that may not be a requirement. Can you clarify? Alex?

ALEX DEACON: Yeah, thanks. I'll take an action to go through and scrub the document to remove the concept of a framework and make it clear that it's ICANN Org responsibility here and it is a requirement, assuming people are happy with that. I think it would clarify and put a fine point on what we're trying to do. Thanks.

JANIS KARKLINS: Okay. So, with that understanding that Alex will take out the framework and we'll work on assumption that ICANN Org would be accredited, accreditation authority. So, can we move further on D? Any issue with D? No requests. So, E? Verifying identity of requestor. Marika?

MARIKA KONINGS: Thanks, Janis. Just know that we still have must here in brackets, but I'm assuming at this stage that we can remove those. I believe that is something that the group is agreeing on. If that's incorrect, let us know, but otherwise we'll go ahead and remove those brackets.

JANIS KARKLINS: Marc Anderson, please. Can we remove brackets?

MARC ANDERSON: Different comment.

JANIS KARKLINS: Okay. But think about brackets as well. Go ahead.

MARC ANDERSON: Thanks, Janis. This may be a comment for Alex since he's going through and cleaning some of this up but this section, for me, I think reads a little weird because it's called benefits of accreditation and so it's a little unclear what we're trying to convey from an implementable policy standpoint in this section. So, I don't know if that's something I can throw to Alex to clarify on his rewrite or not.

JANIS KARKLINS: So, I think this [inaudible] response. And actually, the information is not new, but this is response to the discussion why we are doing the accreditation at all. So, what's the purpose for that? And that is attempt to clarify what we will try to achieve by accreditation. But Alex, maybe you have better explanation.

ALEX DEACON: Thanks, Janis. No, I don't think I have a better explanation. What do I think? I think there are … I'm trying to say this in a way that doesn't sign me up to do too much work between now and the meeting in Montreal. I mean, it could be that benefits of accreditation section B moved above the line. I know the EPDP recommends that. But I think there's a lot of recommendations in this benefits section that would need to be specified, either way, perhaps just in a more concise kind of policy setting kind of way. So, I could try to do that if we think it's helpful.

JANIS KARKLINS: Let's talk a little bit about it. I said, for me, we had the conversation whether accreditation is purely the verification of identity of a requestor or it is something slightly more than that. I think we are in agreement that that is slightly more than that, than just verification of identity. And this section, particularly F, sub-bullet, try to explain what is this little bit more than simply validation of verification of identity of a request. Marc, followed by Hadia.

MARC ANDERSON: Thank you to Janis and Alex both for your responses. I agree with both of you but I was looking at just E. E doesn't just describe the benefits of accreditation. We're saying one of the benefits is verifying the identity of the requestor. That's fine but then it goes on to say the accreditation framework must verify the identity of the requestor resulting in identity credential. That's a policy recommendation describing the benefits of accreditation.

So, I think Alex and Janis, you're both right. I agree with what you are saying. I just think here in this section, we've sort of mixed in policy recommendations with an explanation of what the benefits of accreditation are. I think that's what my intervention was trying to point out.

JANIS KARKLINS: Maybe instead of changing or rewriting the whole section, we simply need to think about changing the word benefits, addressing the accreditation. Any suggestions? Hadia, please.

HADIA ELMINIAWI: So, I think we all agree on the bigger picture of this block, of E and F, and the benefits of accreditation. I think it's only how we put them or arrange the stuff in this block.

So, my suggestion would be to have the benefits of accreditation short and clear. For example, E would be verifying the identity of the requestor, full stop. And then F would be management of authorization credentials and also [inaudible] to the associated attribute or whatever with the requestor.

Then, move the part that talks about the authorization, that talks about what authorization credentials are, or what authorization credentials might convey to another part, as well as moving the part that says accreditation framework must verify to another section as well.

So, just keep the benefits of accreditation clear and short and move the other parts that talk about the authorization and details or other parts of the framework. But this, other parts of the framework somewhere else. Thank you.

JANIS KARKLINS: Okay, thank you. Let me think maybe about what to do with the benefits on substance of the proposal. Is there any issue on subpoint E, with the understanding that brackets would be removed? Brackets around "must" will be removed.

Okay, on F, any issue with the subpoint in F? There's also on the next page. Okay, no requests for the floor. Marc Anderson, please.

MARC ANDERSON: Thanks, Janis. I don't want this to sound like an objection because I think what's in here is pretty good. But I just want to note that some of the sub-bullets on F under "benefits of accreditation" I see as things that won't necessarily be disclosed when you're obtaining accreditation. There are things that may just be disclosed at the time of the disclosure request.

For example, assertation of the legal basis of the requestor – the second sub-bullet point there. That's probably not something you'll be able to say with 100% certainty at the time you're requesting or obtaining accreditation. That's probably something that goes in at the time of the disclosure request.

I hesitated to raise my hand on that because I think … Generally, I think this is a good section but I think that that's something that we need to be aware of that these are things that aren't necessarily known at accreditation time. They only be known as disclosure request [inaudible].

JANIS KARKLINS: Thank you, Marc. Alex?

ALEX DEACON: Yeah. Just to respond to Marc real quick. I think you're right. These assertions kind of happen on the fly. I forget the term I used in my email a while back. But it is still I think within the realm of the identity provider to assert these things on a case-by-case basis for each request.

Then, I just wanted to point out another pair of square brackets on that page here, Janis, where you're highlighted. This one here. Assertions regarding agreement to the disclosed data for the legitimate and lawful purposes stated.

There was a discussion I believe with Amr and others around whether a request can contain or assert a single purpose or multiple purposes. I think we landed that multiple purposes would be okay but I just wanted to raise this. If that's the case, then we can remove those brackets. Thanks.

JANIS KARKLINS: Okay, thank you. Alan Greenberg, please?

ALAN GREENBERG: Yeah, thank you. I guess I sort of assumed that if these assertions were associated with the identity, that effectively, they would be passed on as defaults to save someone from having to do it. So, even the main purpose might be identified in the identity provider. I normally do intellectual property ones. That doesn't stop me from changing it to a cybersecurity one when I'm actually doing the submission. But any system these days has defaults and minimizes the amount of redundant information you have to type in each time. So, I think these are reasonable things to carry, although they're not necessarily how it's going to be submitted. Thank you.

JANIS KARKLINS: Okay, thank you. Hadia?

HADIA ELMINIAWI: I raised my hand basically to speak about whether we say purposes or purpose. The difference here, if you have authorization credentials for many purposes, then if you are actually to use those credentials at some point in time for disclosing a particular set of data, that would not be possible.

But if you have the authorization credentials linked to one purpose, then you can actually define a set of data that could be linked to that purpose. It's just a thought. Thank you.

JANIS KARKLINS: Thank you, Hadia. You see, sometimes when, for instance, if you register an enterprise [inaudible] registry, you need to say that my enterprise will be dealing with certain things and then you list those things. And the enterprise gets registered and license issued or permission given. And then if that enterprise is willing, for instance, start providing financial services, so then that would fall outside realm of the license issued at the time of registration. And I think we can look in this accreditation phase that, for instance, if an organization seeks accreditation, they can file a number of purposes what they would be doing, like we can think of big multi-national who would look after several things. So, that's my interpretation of these assertions that needs to be made during the accreditation. James?

JAMES BLADEL: Hi. Thanks. I admit to being a little confused here from hearing Alan Greenberg's recent comment. It sounds like that a credentialed user could select purposes that were potentially not associated with that specific credential. Then I'm also kind of taking on board the example that you provided of an enterprise that might have multiple functions or multiple purposes.

My question to the group is does it make sense in those situations for a person or an organization to have multiple credentials specific to those purposes? And I'm saying this because I believe in order to maintain the value of accreditation, that we have to have users essentially pick a lane and stay in that lane and not necessarily say, "Once I've got my credentials, I'm in the system now and then I can then select whichever purpose I believe applies to this particular situation." I don't know that's how I envisioned this. I assumed that there would be an entrance for IP purposes, an entrance for cybersecurity purposes, an entrance for law enforcement purposes, and so forth, and that if someone wanted to come through a different doorway, that they would have a separate credential for that.

It may be that I had misunderstood where we're going with this but that's my concern. Thanks.

JANIS KARKLINS: Okay, thank you. Marc, please. Marc Anderson, followed by Alex.

MARC ANDERSON: Sorry. James has given me a lot to think about. I'm just going to drop my hand for now.

JANIS KARKLINS: Okay. Alex?

ALEX DEACON: Yeah, thanks. James, I think, in practice, linking – [inaudible] linking – an identity credential with authorization details, which the latter of which the authorization details are more dynamic, is just kind of bad security practices.

I'm envisioning that there would be a single door that would be opened, if you will, with a combination of keys and the keys would be, "Who are you?" That's the identity credential and, "What assertions are you making with regard to your request?" And based on that, the discloser, whoever that may be, will be able to properly process the request.

I think we can limit, if it makes sense, during the accreditation phase, limit what purposes a specific user may have the ability to assert, if you will, in a request. But I think it would be a mistake to require users to manage many combinations of identity credentials based on what they're asking for. This is way in the weeds with regard to implementation. It's much better to keep those concepts separate and give us some flexibility in implementation in the future. Thanks.

JANIS KARKLINS: Thank you. Alan, followed by Hadia.

ALAN GREENBERG: Thank you very much. I think I support what Alex was just saying. I'm not 100% sure but I was assuming the reason that we separated authorization credentials and [inaudible] is a single identity might have multiple authorizations and they would have to pick which one, or perhaps ones if we're allowing multiple reasons n a single request, to be asserted.

I was just saying, when I was talking about default, not that you would automatically be getting something. Just that the system … It's really an implementation issue to make these systems as smooth and user-friendly as possible. But I think it's really important that a single identity may have multiple authorization credentials. Otherwise, what's the purpose of separating the two?

To use James's example of a driver's license, well I can have a driver's license which allows me to drive a truck and a motorcycle. I don't need different driver's licenses. Thank you.

JANIS KARKLINS: Thank you, Alan. Hadia, followed by James.

HADIA ELMINIAWI: So, I get what Alex is saying. I was thinking, if you have, just what Alan was saying, if you have actually one identity and then you have multiple authorization credentials, then you can pick from those credentials, and maybe at some point at time we think that it is legal to automate, then you could use those credentials to access your data [inaudible]. And that's actually the benefit of having – maybe not the only benefit that we could have from having multiple authorization credentials is to have a faster and a quicker disclosure to the data if required.

Also, one thing. I think we shouldn't try to technically cripple the system just because we are afraid from some policy decisions that could happen if the system is more capable technically. Thank you.

JANIS KARKLINS: Thank you. I will take James as the last one.

JAMES BLADEL: Thanks, Janis. And thanks to Hadia, Alan, and Alex. Look, I think we are agreeing with each other in different languages, if that makes sense. I understand there to be one and only one identity per user and I understand that that identity can have multiple authorizations and that's my analogy of a US driver's license.

I think my concern is each authorization should be tied to a single purpose. So, if you have multiple authorizations, you're both an IP attorney and a cybersecurity researcher that you [inaudible] that those authorizations would be tied specifically to those purposes and you wouldn't cross-pollenate, I guess, if you had multiple authorizations. You wouldn't cross-pollenate and say, "Well, I'm going to use my cybersecurity credentials to access this as an intellectual property purpose," or something like that.

So, I think we're all agreeing with each other here that single identity is a one-to-one relationship and identity has a one-to-many relationship with authorizations but authorizations have a one-to-one relationship with purposes. Thanks.

JANIS KARKLINS: Yeah. Thanks, James. Indeed, we are saying more or less the same thing. Maybe we simply need to think how we can rephrase the [inaudible] of this point to make it very clear and maybe I will ask Alex and staff to think about and to fix the language because I see that, in principle, there is no systemic disagreement. So, there are a few things in brackets. In the lower part, there's a section regarding prevention for abuse, [inaudible] requirements dispute resolution [inaudible] process and so on and so on.

So, what we do with those, can we remove those brackets? Alex?

ALEX DEACON: Yeah. Thanks. One of the things I did when I went through this is take a look at the registrar's document that outlines what it requires when submitting a phase one request for disclosure. So, I think it's important that those requirements are covered in the policy here, and I think things like Power of Attorney and others were things that I noticed that were in that registrar policy which I'm not an expert on but not in here.

So, I would ask the registrars if they could just confirm that the requirements in their doc are covered here. I don't want to get to a point where it's not. If that's the case, then I think we can or should remove these square brackets, but some confirmation from the registrars would be super helpful. Thanks.

JANIS KARKLINS: Okay, thank you. Any reaction to Alex's question? James?

JAMES BLADEL: Yeah. Thanks. We've got kind of a depleted team here from registrars, so I will have to take that back. Sorry, Alex, I can't give you a quick answer. But we'll take that back and get comfortable.

JANIS KARKLINS: Okay, thanks. So, maybe we need to think about the upper part, to type up the language in order to make sure that we are using James's analogy of the driver's license with the multiple categories, permissions, to ride the different vehicles and rephrase that upper part and make it clear. And I would suggest that this is an action point and we go to G, validation of identity credentials. Any issue with this?

So, no issue. There, we can take color off?

So, the Code of Conduct, next page. Should [inauible] initial? So, I. All is clear. J, K? No requests for the floor. L? I think that's L and that was already agreed before we rewrote. P? So, I think that this was …. There was an issue. There was some traffic and exchange on the email how we deal with abusers of the system. Alan Woods?

ALAN WOODS: Thank you, Janis. This is one of the issues that we raised in the Registry Stakeholder Group, just specifically with regards to revocation policy for individuals and entities should be under graduated penalties.

Personally, I have a lot of issue with that concept, just purely because revocation, if somebody has been proven to have misused the data, there should be graduated for that individual user. If we're talking about the accreditation authority, then that's fair enough. That's avoiding the issues that we were talking about earlier and thus the accrediting entity might have graduated penalties to avoid things such as everybody losing access and once and there might be mitigating circumstances for that.

But, for the actual user, if they are found to be in breach of any of the things that they've said – the representations that they have said – they should have their access revoked. I just want it on the record. Thank you.

JANIS KARKLINS: Okay. Thanks, Alan. Any issue with Alan's statement and point of view? Brian?

BRIAN KING: Thanks, Janis. No, I agree completely with Alan. One of the questions – and maybe we can handle this on the email list or further in Montreal but one of the questions I had was about the note that the registry submitted. And I think we agree on principle but just curious how we think it might work. How could the contracted parties know that someone had been de-accredited and might then come around the backdoor knocking for one-off access in a request to the contracted parties. It sounded like the registries were interested in that kind of feedback loop or some information. I'd love to know how folks think that that could work in practice. Thanks.

JANIS KARKLINS: Thank you, Brian. Probably then [N] needs to be reworded in light of Alan's request. Let me take now Volker.

VOLKER GREIMANN: Yes. Thank you, Janis. Not able to answer Brian's question right now but one further thought occurs that taking a page from the book of what applies for contracted parties with ICANN at the moment is that if an entity is revoked, this revocation [inaudible] future accreditation should probably also be extended to any officers or employees of that entity, just to make sure that they don't set up another entity that just does the same thing again. Thank you.

JANIS KARKLINS: Okay, thank you. Alan? Is it an old hand, Alan?

ALAN WOODS: It's actually a new hand. It was in response.

JANIS KARKLINS: Yeah, please, go ahead.

ALAN WOODS: It's a response to Brian's thing. It's probably jumping a bit onto [P] so I'm happy to hold in queue until then if you want.

JANIS KARKLINS: No, please, go ahead.

ALAN WOODS: Oh, okay, thank you. So, the reason why this concept of a feedback loop is only important because it is specifically mentioned in P saying that revocation does not prevent the previously accredited individual or entity from submitting a request. The fact of the matter is that by stating it in this, we are creating an expectation and we are also providing a means by which people saying if you go to the SSID and you enter your credentials, it's revoked. Well, then, just go to the registry and the registrar and they'll probably give it to you anyway. That is of major concern to me because that is providing an administrative workaround to a revoked entity or a revoked credential.

So, we either take out P completely, because that is not a concept that we are in any way comfortable with, or if you want to leave to in P, well then, there must be a feedback loop to the registries and the registrars where a person's credential has been revoked.

Personally, I think the easier one is take out P because it probably is the easier thing to police. I agree with Brian. It's a very difficult concept. But we cannot be tacitly approving, as I said, an administrative workaround of the revocation of a credential. Thank you.

JANIS KARKLINS: Okay, thanks. Margie?

MARGIE MILAM: I think that's a good point of view from Volker and others. If you have a company that has users that are accredited, remember this is the only system to be able to get access for any meaningful way. So, I feel like it's a bit much to say that the entire organization credentials are removed or unavailable anymore because of one person.

I understand Alan's point of view that if someone violated the law that they should be revoked. But on the other hand, a lot is gray. There may be areas where it's not clear how the law applies, so it may not be egregious. I just think it's a bit punitive to say that it's all or nothing. I'm thinking that if we link the revocation to at least a specific user rather than the entire entity, that probably works better.

JANIS KARKLINS: Okay. Any reaction to Margie's argument? Brian?

BRIAN KING: We support. The thing that I would point out, really, is that based on the types of accreditation that we can have, that we've discussed and agreed to here, is that users can be accredited - or I'm sorry, an identity credential can be issued to either an organization or an individual. So, maybe the sweet spot is that individual accreditations could be revoked based on less showing of abuse, whereas to revoke an organization level type accreditation, that more might be required. Just a suggestion. Thanks.

JANIS KARKLINS: Thank you. I think that the language, which is now proposed, takes into account both those points of view and with the finetuning, specifically verification policy for individuals and verification policy for entities, may be a way forward. But let me take Volker and Alan Woods.

VOLKER GREIMANN: Yes, thank you. I have a slightly different opinion than Margie. I think revocation of credentials is something that probably would only happen as a final step or last resort. Basically, when that organization really has messed up with their request and has a proven track record of use of requests. Therefore, I think, in that case, the blanket ban on the entire organization is warranted because that organization has shown to be an abuser and we cannot be expected to say that this employee is a good one, this employee is a bad one. If you lie down with dogs, you wake up with fleas. So, if you go into the wrong [inaudible] and get de-accredited, then you have to face the consequences of that. If that means you have to find another [inaudible] … Yeah, that's it.

JANIS KARKLINS: Thank you. Alan?

ALAN WOODS: Who doesn't want to follow that? Yeah. I completely agree. I'm just reacting. You said is there any reactions to Margie's and my gut instinct was there were several reactions to what Margie said there because I worry about the concept of mixing up the idea of a principle-based law with gray areas in the law. We do not want to live in the gray areas of the law and I think there's enough cautionary tells out there that the gray does not work.

We need to look at this from a principle's point of view and the principle here is that if a person has been proven to have misused data, regardless of if their credential is for a particular entity and they can be seen to be tacitly responsible for that breach of that trust – and again, I'm taking James's words here, but this concept of the honor system.

If that trust has been breached, maybe we can think of a concept of some way of regaining that trust in some way with an awful lot of undertakings and indemnities and things like that. But to be perfectly honest, at the end of the day, if they have breached that trust, they should not be let back into that system. Again, we need to be focusing on the principle of the matter, not the gray areas, since I think that's a very, very slippery slope to be going down.

JANIS KARKLINS: So, how then … Let me take Mark SV and then Margie afterwards. Mark SV, please.

MARK SVANCAREK: Thanks. I think we should just think about how this works in practical terms. So, let's imagine that Microsoft's trademark group has some credentials and Microsoft's digital crime unit has some credentials and some idiot in the trademark group does some bad stuff. Now Microsoft is going to be, as an organization, legally liable for that bad stuff. And now we're going to talk about de-accrediting the trademark group. That seems very clear.

Now, if we start talking about also de-accrediting the digital crimes group, I think that there has to be some sort of mechanism for preventing that, for discussing that, for mitigating that, for allowing the digital crimes group to come back into the system as a trusted entity while kicking out the trademark group.

I think our policy is going to have to accommodate situations like that. So, while I understand that an organization who has an employee who has done the bad thing has to take the legal consequences of it, we have to realize that there are large organizations that are going to have multiple roles, different credentials, different tasks and throwing out the whole thing forever is probably not a good system. So, we just need to think about the practicalities of when we throw somebody out what recourse there is for that organization, saying that because Joe over in trademark did a bad thing, now digital crime unit can never ask for non-public data. That seems going too far, in my opinion. Thanks.

JANIS KARKLINS: Okay, thank you. Margie? James afterwards. Margie, please.

MARGIE MILAM: Sure. Thank you. I think Mark really hit it well. I don't think we were that far apart. What Volker said about there being organizational abuse or systematic abuse, that makes sense to me. But a one-off request that somehow is challenged, that's where I get nervous. So, anything that's gradual that has penalties, that has the ability to have increased obligations on them if needed, all of that to me makes sense and maybe we should be talking about what those things would be.

Obviously, I agree, if there's systematic abuse, that's a problem and we're just trying to find a way to address this properly.

JANIS KARKLINS: Okay, thank you. We maybe need to move on on this. Let me take James and Marc Anderson, in that order.

JAMES BLADEL: Thanks, Janis. I just wanted to go back to a comment from Mark SV to say thank you for laying out the real-world implications of these policies on large organizations. I just want to point out that that's what registrars are living under right now, that if, for example, a small affiliated accredited entity that GoDaddy has acquired has a reseller that does something bad somewhere on some far corner of the world and ICANN, in its wisdom, decided to de-accredit that, all of our affiliated registrars are handcuffed together and the 18 million-plus customers that GoDaddy serves would be at risk in that scenario. So, that's exactly what we're living under.

Now, I do agree with Margie that there should be graduated penalties, because as with the RAA, we saw the problems associated with this all-or-noting nuclear option when it comes to enforcement.

So, I agree that there should be graduated penalties. I'm not sure about the process of reinstatement for someone who has been revoked, particularly if they were revoked by they violated some privacy law. I think, ICANN, for example, has a number of provisions around individuals who cannot be contractors or officers of contracted parties that they've been convicted of financial crimes. I don't know that those black-listed individuals, if there are any, can be reinstated.

So, let's take a closer look at this. But I just wanted to point out to the folks that … Mark's example is a good one and it exists now, it exists today, and it's a reality for registrars. Thanks.

JANIS KARKLINS: So, thank you, James. I have been told that Stephanie is in line. She is in audio only. I'll take Stephanie and then I will make a suggestion on these two points. Stephanie, please.

STEPHANIE PERRIN: Thanks very much. I hope you can hear me.

JANIS KARKLINS: Yes.

STEPHANIE PERRIN: I have so many reservations with how this model is rolling out but I think I don't like any model now. But we'll just park that for the moment.

One of the most instructive cases for abuse recently has been Equifax which we are all stuck with on this continent as a third-party no contact with the individual purveyor of credit scored. And when they were caught selling identity information to identity theft rings, not only was there no really substantive repercussion, their executives got away with unloading their stock before they advised of the breach and were still using them, unless I've missed a news report where they went out of business and they're now not in the credit reporting business.

So, I would suggest that we have a parallel monopoly situation. If ICANN is proposing that it be the sole accreditation provider in this model that it's consulting on, there is a great risk that there will be insufficient audit of repeat offenders, that there will be insufficient repercussion. I don't even know what the proposed repercussions really are, other than knocking a division out.

And to use Mark's example, if Microsoft doesn't have sufficient penalties in place for non-compliance with law, policies, rules, standards, etc., then they certainly should be punished because a rogue operator should not be able to go bonkers in trademark section and put in all of these requests. There should be audits. And if Microsoft, as a huge company, cannot police its audit controls, then how is ICANN going to manage with smaller enterprises, where the risk goes up? I just don't see how this thing scales and I think it requires a pretty serious rethink. Thank you.

JANIS KARKLINS: Thank you, Stephanie. Mark, I think we can take this discussion offline, but if you insist, please go ahead.

MARK SVANCAREK: I'll go quickly. I just wanted to reassure Stephanie that, actually, we do have the processes in line that those people will be caught. I actually talked to one of the attorneys who's responsible for this just yesterday. So, yeah, they will be caught, but then at that point, we're dealing with something that's happened in the past. And if somebody in the AI group does something, it doesn't mean that somebody in some other group does something. That was [just my whole] point. But yeah, we do have those controls in place. Thanks.

JANIS KARKLINS: Thank you. So, let me suggest, it seems that subpoint N needs to be split in two parts – one on revocation policy for individuals who are accredited as individuals and then revocation policy for entities with the multiple individuals, maybe multiple [inaudible].

And if I may ask maybe Margie and Volker to think about this rewriting, that would be a great help. Would you be able to do that? Thank you.

We will start with the subpoint N in Montreal but let me now see what we do with P. There was a suggestion simply to delete P, if I understand correctly what Alan was suggesting. Any problem with deletion of P?

Then, another thing that immediately kind of made my spine trickle when Stephanie said that she has many issues and she cannot agree on many of the sections. Maybe I misunderstood you, Stephanie, and I really [inaudible] that I was wrong, but if that is the case, then we may have trouble at the very end when we need to endorse this policy proposal as a package. If you have issues that I have not announced, then we cannot address them in any way. So, again, I hope I misunderstood you, but in general terms, if team members do have issues with any of proposed text, please let those concerns known. Otherwise, you should not wait until end of the process. We need to know them now. Stephanie?

STEPHANIE PERRIN: One of the problems is the manner in which we're going through this because we are building a model, not a framework. Somebody mentioned the word framework earlier and suggesting that we … Defining it is difficult. It sure is. When you're building a system, a la Strawberry Team, a la whatever the other outfit was called – it wasn't called Strawberry, the technical study group. If you start by building it and without getting principles in place, then the whole thing is fluid. I can't even give you … I'm not going to do this work every week, as each new little gem comes sliding down the string of pearls here. I'm mixing my metaphors there. I hope you'll forgive me.

Now we have a new report which I unfortunately am getting ready for the meeting. I don't have time to review a 27-25 page document that we weren't consulted on, regardless of how slim it is in content, I still need to go over it.

So, you will get a full list of all my complaints soon, as soon as I an manage it, but it's not going to come before Montreal unless a miracle happens. And I really apologize for the crusty tone in my voice, but to put out a paper like that, to operate on parallel track without consulting the folks who are putting in four hours a week, not counting homework time – so call that 20 – is beyond an outrage. It's total abrogation of the multi-stakeholder model as far as I’m concerned. Thanks for listening. So, sooner or later, I’ll have a complete framework of my objections. Thanks. Bye.

JANIS KARKLINS: Thank you. Okay, so we are deleting P. Now let me see on Q. This is about de-accreditation of accreditation authority. I recall our initial discussion at the beginning where we were talking about definitions. So, now, this is the place were de-accreditation policy is described. So, no issue with Q?

JAMES BLADEL: Sorry. James with a late hand.

JANIS KARKLINS: Yeah. James, please, go ahead.

JAMES BLADEL: Yeah. Just to note that we need to flesh out a little bit more here what happens to the outstanding credentials that are in the wild and how those should be handled. We talked about that earlier, so no need to rehash that here.

But I also wanted to flag just a comment that Alan Woods – I think it was Alan Woods. Apologies if I get it wrong. But Alan Woods made earlier about making the distinction perhaps between de-accreditation for a violation of the access policies in terms of SSAD versus de-accreditation for conviction for violating privacy law.

I think that there are parallels that. For example, in the registrar accreditation and registry accreditation agreements with ICANN where there are graduated sanctions for non-compliance with the contract, but if you're actually found to be a criminal, a criminal organization, then that's a different matter and probably not counting as … I guess I would say, from a baseball metaphor, that would count as all three strikes versus any sort of graduated sanctions. That would skip you to the end.

So, let's talk about this one a little bit more, but I think that we should make a distinction between policy violations and criminal actions. Thanks.

JANIS KARKLINS: Okay, thank you, James. It would be useful if you could maybe provide your thoughts in writing as edits to this point Q or additions to point Q. Would that be possible?

JAMES BLADEL: Happy to do so. Thank you.

JANIS KARKLINS: It would be good before Montreal because it seems to me that, in Montreal, we will start with subpoint N – edited subpoint N – and then we will go further. So, Hadia's hand is up. Hadia?

HADIA ELMINIAWI: I'll quickly say that we need to address what happens to the accredited users once an accreditation authority has been de-accredited. Also, I would like to quickly note that Alex, at some point, said de-accreditation is the nuclear option. I will say that no nuclear options should be allowed to exist within the system. Thank you.

JANIS KARKLINS: Okay. Thank you, Hadia. Let me ask one question on T. Not [inaudible], but subpoint T. This is the redraft and I would like to take temperature on redraft of T. Any issue with T? James?

JAMES BLADEL: Just noting the comment from Sara on behalf of the registrars that we believe there should be some reasonable and practical limits, either during a session over a given period of time. For example, a thousand a day or something like that. That is not an artificial or an arbitrary barrier to accessing the system but that's to ensure that all users have equitable access to a system and we don't have heavy users effectively monopolizing the connections and the resources.

We say this because, perhaps as registries and registrars, we have a little bit more real-world experience than ICANN or the SSAD operator in just how these things play out in the real world with, for example, limiting connections or limiting sessions or limiting the number of queries. So, we just want to make sure we're clear that we believe that saying the request must be unlimited or will not be restricted, I don't think that that is something that we can live up to in the real world. Thanks.

JANIS KARKLINS: Okay. But that is implementation question, I believe. Look, I will take now both Marks and then probably we need to move on to the next agenda item because we have ten minutes before the end of the session. Marc Anderson and Mark SV.

MARC ANDERSON: Thanks, Janis. I was going to make a similar point to James. This language seems to prevent the technical operator of the SSAD system from protecting the system against abuse such as a DDoS attack. I think the language needs to be loosened up a little bit – a literal interpretation of that coming implementation time could be prohibitive.

JANIS KARKLINS: Okay, thank you. Mark SV?

MARK SVANCAREK: Yeah. I want to acknowledge James's point and concern, particularly a DDoS attack. That's a great example. I just think that we shouldn't get into too much detail here right now in bullet T because this really feels to me like it's part of the cost recovery mechanism. You know what SLA you can support when you know how you're paying for it. So, I just wanted to make sure that that's considered, whatever light you put into bullet T right now. Thanks.

JANIS KARKLINS: Okay, thank you. Two more. Greg and Margie. Greg? So, while Greg is getting online, Margie, go ahead.

MARGIE MILAM: Sure. I think that the language where it says accepts where the accredited organization poses a demonstrable [inaudible] to the SSAD is intended to pick up things like DDoS attacks. I think that's why we got that language. If you recall a few calls ago, we were talking about the SSAC paper – I think it's 101 – that talks about this. So, I think that was the concept we were trying to get at when we came up with that exception language. I'm happy to consider changing it to this because I do think that you want to avoid a DDoS situation but that's far different than saying that normal volumes of SSAD requests should be limited.

JANIS KARKLINS: Okay, thank you, Margie. Volker?

VOLKER GREIMANN: Yes. In general, I don't have any issues with that. I just note that unlimited requests, depending on how the system is built and how much manual interaction there will have to be and depending on the size of the registrar that is going to be queried in this method may cause a significant backlog, so there probably will be an incentive to keep the number of requests using the system to a minimum just to avoid any delays in further responses or in this response to your queries int the first place because I think nobody is served if it takes three months to work through all the requests that are currently in the queue and you have that kind of response time.

So, if you have large numbers of requests, then maybe we should encourage requestors to go through other routes and ask the registrar directly for that information instead of using the system because that might be a quicker way to get the results, rather than having a one-by-one review of every case. Thank you.

JANIS KARKLINS: Okay, thanks.

GREG SHATAN: Hi, this is Greg. Can you hear me?

JANIS KARKLINS: Yeah, Greg. Yes, please go ahead.

GREG SHATAN: Thank you. Again, I'll refer everybody to SSAC 101 which points out a problem. A couple of problems. One is sometimes requests will be episodic. All of a sudden, we'll see a problem with the domain names that a particular registry or registrar – security problem. There may be hundreds to thousands of these that need to be queried.

We have a problem when people will rate limit those. And if there is a problem at a registrar, we do think at SSAC that it's the responsibility of the registrar to be able to respond to those queries. If there's a problem in your space, we need to be able to make those queries. One way to avoid this problem is don't have problems in your space.

Volker's suggestion to go outside the system doesn't make sense. The system is designed to provide and facilitate these kinds of requests. Going outside the system strikes me as something that's going to be slower, in fact. So, the system does need to accommodate that kind of a thing.

Ultimately, what we need to avoid is having one party decide what's abusive or choose what it will fulfill and what it won't. I think a good suggestion out of SSAC 101 is if the requests are legitimate, they need to be handled. One of the things we're trying to do there is to say if the requester is illegitimate, then we'll have a problem. We'll need a process to deal with those and decide if that user should continue to be accredited. But having one party to decide how much they can handle and then shut off legitimate users is a problem. Thanks.

MARIKA KONINGS: I think we may have lost Janis.

JANIS KARKLINS: No, no, no. I muted myself. Sorry. I said that I really want to show you a Montreal program but we have about four minutes to go. So, I have Volker and James in line in that order and then we will go to the Montreal program.

VOLKER GREIMANN: Sorry, old hand.

JANIS KARKLINS: Okay. James?

JAMES BLADEL: Yeah, thanks. I'll keep this quick. Greg, I don't think anyone is disagreeing here. I think that what we're talking about is not individuals rejecting requests or rate limits by the receiving parties, but I think we're talking about the SSAD as a whole right now having some access controls. And I understand SSAC position. If a cybersecurity researcher submits 150,000 requests and I have one domain that I need as part of my investigation, how long is it acceptable for me to wait for the SSAD to process the request that came in before me that is taking up all those resources?

And I think it is relevant to the discussion about SLAs. So maybe if we talk about these things being SLA exceptions, maybe we can make some progress.

But I think the key here is that it's really not even a technical problem. It's an economic problem. The demands or the use or the intended use of the system is always going to exceed its ability to fulfill those requests. So, the question is, for the group, can we live with the backlog while those requests are being fulfilled? And if the answer is no, then we have to have some limits.

If the answer is yes and we can live with a backlog, then just let's – game on. Thanks.

JANIS KARKLINS: Okay, thanks. May I ask, James, you and Greg to get together [Friday] night and iron out the text that we could propose to the team as a whole, that we will revisit the subpoint T once we are talking in Montreal.

So, look, we again good progress and I think hat we have now much cleaner text. There were a few points that Alex said he would clean up, and then point N will be split in two and we will continue from point N when we meet next time in Montreal on this topic, and hopefully we will get through the accreditation block fairly quickly.

With this, I would like to ask to show the proposed agenda for the meeting, just to collect immediate reactions or …

So, we are meeting five times and then we have also a public meeting on Monday morning. We have a full day on Saturday, so where we would suggest that we address – we continue talking about building blocks. Then, we discuss with the ICANN Org the Strawberry Team, the status of where we are now with the request to European Data Protection Board. Then we also have the request coming from implementation team if I am not mistaken on terms of reference for the study on legal versus natural. And if we can scroll down … Yeah.

So, I would suggest that we use lunchbreak in order to engage with ICANN Org on this terms of reference where we would receive initial proposal and then we would gather reactions during the lunchbreak.

Now that we know where we are, we will populate this meeting agenda, with instead of building blocks, we will indicate exactly which building blocks we will take up in what order and what time and we will post it probably during [inaudible] you can have a chance to review it and mentally prepare for the meeting.

Then, we will have meeting on Sunday where we will continue building blocks, but at the beginning of the meeting maybe we will exchange a little bit on the Monday morning plenary meeting. I will show you slides that I would present in the plenary. And then we will continue with building blocks.

Then, on Monday, we have two sessions in a row. The first will be again on building blocks and policy principles if we will get that far. Then, the second meeting from 5:00 to 6:30 I would suggest that legal committee would meet on their topics since there has been a significant period without meetings. And then other team members could work in parallel on any outstanding editorial things that will need to be ironed out in face-to-face setting. I think that would be fair use of time from 5:00 to 6:30.

Then, on Thursday, I think we had only one meeting on Thursday, not two. Marika we spoke about it. We have 90 minutes on Thursday. So we would take stock on where we are and decide on next steps as a result of progress we would make in Montreal. So that meeting will be chaired by Rafik and I will be following from Geneva since I will be leaving Montreal Monday night at 8:00.

So, this is what I want to say on the suggested agenda. Any reactions? Any disagreement on the approach proposed?

Once again, here is Marika’s [inaudible]. We really need to stabilize and prepare for the face-to-face meeting, stabilize all the text. So, therefore, the solicitation from my side and from staff side is to provide any comments for Montreal meeting by tomorrow, 30 October. But they can be taken into account in preparation of the text that we will display on the screen during Montreal meet. So, please take that seriously. There is technological time the staff meets.

So, with this, any reaction? I see none. So, that leads me to thank all of you for active participation in today's meeting. So, to those who committed to do homework, please do it as quickly as you can. For the rest, have a good day and safe travels to Montreal. See you all on Saturday morning in Montreal. Thank you. This meeting is adjourned.

UNIDENTIFIED FEMALE: Thank you, everyone. Once again, the meeting has been adjourned. Please remember to disconnect all remaining lines and have a wonderful rest of your day.

[END OF TRANSCRIPTION]