ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2
Thursday, 24 October 2019 at 1400 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 are posted on the agenda wiki page: https://community.icann.org/x/BYYCBw

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

TERRI AGNEW: Good morning, good afternoon, and good evening. Welcome to the GNSO EPDP Phase 2 team meeting taking place on the 24th of October, 2019, at 1400 UTC.

In the interest of time, there'll be no roll call. Attendance will be taken by the Zoom room. If you're only on the telephone, could you please identify yourselves now?

Hearing no one, we have listed apologies from Ashely Heineman of the GAC and Mat Serlin of the RrSG. They have formally assigned Laureen Kapin and Sarah Wyld as their alternate for this call and any remaining days of absence. Alternates not replacing a member are required to rename their line by adding three Z's to the beginning of their name and, at the end in parentheses, their affiliation-alternate, which means you are automatically pushed to the end of the queue. To rename in Zoom, hover over your name and click Rename. Alternates are not allowed to engage in chat apart from private chat or use any other Zoom room

functionalities, such as raising hands, agreeing, or disagreeing. As a reminder, the alternate assignment form must be formalized by way of the Google assignment link. The link is available in all meeting invites towards the bottom.

Statement of interest must be kept up to date. If anyone has any updates to share, please raise your hand or speak up now.

Seeing or hearing no one, 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.

With this, I'll turn it back over to our Chair, Janis. Karklins. Please begin.

JANIS KARKLINS: Thank you, Terri. Good morning, hello, and good evening, everyone. Welcome to the 27th meeting of EPDP Phase 2. Traditional question: the agenda circulated on Tuesday, which is also in front of you, containing seven points. Is it the one we want to follow in today's meeting?

No objections. Thank you very much. So what has happened in the meantime since our last call? First, you all were copied on my e-mail to ICANN org, by which five questions that we identified were sent for answers on my behalf as Chair of the EPDP. I'm expecting answers may be provided by the Montreal meeting.

Secondly, we with the staff started preparations for the Montreal meeting. After this call, we will share an outline of our face-to-face meeting in Montreal. We ask that you review that proposal so that we can finalize and preliminary agree on it during the next call that we will have on Tuesday.

Then, as has been tradition recently, I would like to ask staff to display our building block sheet so that we can see how much we have progresses and how much still remains to be done.

[HEIDI ULLRICH]: Terri, if you can stop sharing, I'll share the building blocks page. Thank you.

JANIS KARKLINS: Thank you very much. As you see, we have progressed slightly but not much. So it's fairly white, which means that we need, really, to pull up our sleeves and do whatever we can in order to progress further. Hopefully today we will make some progress on important building blocks which are in front of us. So thank you.

Any comments at this stage? Any housekeeping issues?

I see none, so let us move then to the first substantive item: the accreditation building blocks (Building Blocks F and J) for continued second reading. Let me start by saying that, after our previous conversation, staff did a rather substantive reshuffling of the text, starting with bringing up front working definitions and making sure that we understand what we mean by using certain

terms in the text. Also, the process was fine-tuned as a result of our conversation last time.

After that, Alex, together with Milton – the initial pen holders on these building blocks – made also substantive edits and amendments to the text. It was done on Tuesday. I hope everyone had a chance to look through those proposals. Since I asked, I have not received any, let's say, opposition from a system point of view, from a conceptual point of view. I assume that we can work on the basis of this edited version.

For the sake of simplicity, I would like to invite Alex, while I'm thanking Alex for these edits and work/input provided, to maybe walk us briefly through the essence of the proposal. Alex, please?

ALEX DEACON: Thanks, Janis. I think the reorganization and the updates that staff made were super helpful. The additions I made to this doc were essentially, I think, additions that help clarify and detail some important aspects that were missing. Much of the text that I added came from the original doc that Milton and I did work on. So hopefully none of this is super surprising, but why don't I just go through the major points and describe the changes and the updates I've made?

First, if you remember, in L.A. the framework that I suggested assumed there will be multiple accreditation authorities. In that scenario, you would need a framework to accredit the accreditors. Since then, we've decided that, ideally, what we want is a single accreditation run by ICANN, I think, presumably, and that

accreditation authority would or could outsource identification functionality or function to third parties that would be vetting the identity and attributes, if you will, associated with requesters in the system.

This draft, again, started by staff, I think reflects that. When I went through this doc, I tried to make a few clarifications here and there to clean that up. So that's the first major change.

The second one is this concept of this distinction of credentials, this idea of an identifier credential which identifies a user itself. These credentials are usually of the form of username or password or some form of certificate.

Then we've defined a credential called an authorization credential. These are attributes, or claims if you will, that are associated or bound to an identifier credential. Essentially, while an identifier credential is static. alex@colevalleyconsulting.com, representing Cole Valley Consulting, presumably, would be the identifier credential. However, I would select separate authorization credentials depending on the request I'm making. For example, one day I perhaps would be submitting a request for an IP purpose, and the dynamic nature of the attribute credential, again, managed and issued by the identity provider, would allow me to assert that for one request. A few days later, I may then submit a separate request for, let's just say, a cybersecurity purpose, which would then assert different authorization credentials that have a cybersecurity purpose and the like and a legal basis and so on.

This is typical in these kind of authorization and authentication systems, that you separate identity from claims or authorization

credentials. So I think, in order to allow us the flexibility in the system moving forward, this separation is important. It turns out, as I noted in my e-mail, that the technology that's suggested by the TSG OpenID Connect supports this concept, this separation of an identity credential from an authorization credential.

Of course, all of those credentials, plus other information that may be included in the request, are used by the discloser, if you will, whoever that may be, to determine whether or not the request is authentic and valid, well-formed, and ultimately to decide whether to authorize a disclosure of non-public data. You'll see I've added those definitions up top. Then I tried to use them throughout the rest of the doc.

The next major change was trying to clarify the concept of revocation versus de-accreditation. We had overloaded the term "de-accreditation" to apply not only to requesters, to not only apply to identity credentials, but also to the accreditation body as a whole. I found that confusing, so I made up dates to define the term "revocation," which we actually had done. Revocation applies to the revocation of a single identity credential by the accreditation authority, whereas de-accreditation applies to the full accreditation authority itself. So revocation impacts a single user of the system. De-accreditation is what I call the nuclear option. It basically invalidates any credential issued or managed by the accreditation authority. So hopefully that was helpful. It was for me at least.

While I was out and after I came back, I was able to listen to last Thursday's call. I looked through the information of the previous calls. There are several times where people asserted that accreditation is just about identification. I think in L.A. the

discussion we had made it clear that, in order for accreditation to add value and to justify and accreditation scheme at all, it needed to be much more than that.

So, if you look at the benefits of accreditation section – if you scroll down, Marika, or whoever is controlling this – I tried to flesh that out a bit. In addition to identifying the requester, I outlined how these authorization credentials are of benefit. These are essentially the assertions by the identity provider regarding attributes associated and bound to the requester. These are things like the purpose of the request, the legal basis of request, or an indication or an assertion that then user identified by the credential is affiliated by some accreditation authority, or perhaps now better worded as the identity provider, etc. These are all things that are more dynamic but are still required for the discloser to actually determine whether authorization can happen or not.

Another benefit – I think an important one – is this concept of the definition or the creation of a baseline code of conduct that essentially establishes a set of rules that contribute to proper application of data processing laws, including the GDPR, for the ICANN community. This list in, I guess, I, if you scroll down a bit, basically is an outline of what needs to be in a code of conduct. I took that from the European Data Protection Board regarding their guidance as to the creation of code of conducts.

I think that is about it – oh. The last thing is I chatted quickly to Marika while I was making these updates. There's a lot of detail here which I think is important for us to get right. However, I know in this document we have an implementation guidance section, so it may be that some of these details are better placed down there.

But for now I just stuck them all up here in the policy section. As we refine this, I think we may want to determine which, if any, of these details are better placed at the bottom.

I'll leave it there for now. I'm happy to answer any questions.

JANIS KARKLINS: Thank you, Alex, for this input. Now let me propose that we go first to the [inaudible] question: is there any, let's say, opposition still or doubt that the proposed mechanism is not feasible? After that conversation, if there will be any doubt, then we will go, really, section by section very quickly. We have plenty of new material, and most likely we will not be able to do a line-by-line reading but rather section by section. Then I will ask anyone who wants to provide any input or editorial suggestions to do it by Friday so that we can compose new text, aiming at approving it or stabilizing it on Tuesday, prior to the meeting in Montreal. That was maybe a little bit ambitious, but since we have been talking about accreditation already four times, I think it is feasible. So any conceptual difficulties?

I see no requests, so then we will go section by section, starting with the section of definitions. Let me take all terms starting with A. Any issue with the first seven points?

No requests. Any issues with the working definitions of credentials?

James?

JAMES GALVIN: Thanks. No issues or objections. I just wanted to, I guess, thank Alex for his work here because we've been conflating this identification and authorization so much. So separating the credentials, I think, is very helpful. So thanks for that.

JANIS KARKLINS: Thank you. Milton?

MILTON MUELLER: Just wondering if Alex could elaborate a bit. I tried to ask a question about this way up in the chat. The authorization credential he describes further down as a bunch of assertions. Then there's some language under G which talks about how these credentials might be used. We're still dancing around the nature of automation here. So can you describe for me in more detail how you think this authorization credential plays into the automation debate?

JANIS KARKLINS: Alex, would you like to start?

ALEX DEACON: Sure. Happy to. G was a section that I think was in our original doc and then the subsequent updates. I found it odd that this section was in the benefits of accreditation, but instead of deleting it, I left it there. I tried to – perhaps I failed – distill down the discussion we had in the separate threat around automatic

disclosure. So I think there's still some work that needs to be done here.

In terms of your questions, Milton, the way it's going to happen is that a request is going to be made. There's basically three major parts to it, as I see it. One is it'll be signed, if you will. It will be associated with an identity. This is the identity credential. This basically allows the discloser to determine who the request is coming from.

The second set of information is going to be these authorization credentials. These are the signed or validated assertions, not directly from the requester but actually asserted by the identity provider and the accreditation body. These are basically third-party or identity-provided assertions that are sent down or associated with the request.

The last part of the request is essentially the body. These are the other details, I think, in Building Block A that describe the nature of the request and the like. When this request is received by the discloser, whether it's ICANN or someone else, they need to validate the request as a whole to make sure it's properly formed. They need to validate all of the information to make sure that it meets the policy with regard to completeness. Then they go through and there's going to be some logic where they will look at the identity, the set of authorization credentials, and the details in the body of the request, with which they could then determine how to process, if you will, or authorize if or which data is disclosed.

How that happens I think we haven't gotten into. We could think about exactly that logic and put a flow chart together, but it would

be based on a combination of the purpose, the legal basis, and the like. How that is automated and how much of that is automated I think depends on the identity of the individual, the claims, and the authorization credentials that are included in it, plus the data that's provided by the user.

I don't know, Milton, if that helps, but …

MILTON MUELLER: Well, I feel like you're still a bit too vague for comfort on the question of what this possible automation consists of. I think the authorization credential being separated from the identifier credential is a good thing. It contains these assertions. But how these assertions get vetted and responded? It's just not clear to me how that could ever get automated.

ALEX DEACON: Well, the vetting and the creation of the assertions, as you mentioned in the chat, are all auth credentials. That happens by the functionality in the accreditation authority and identity providers, assuming those are leveraged. So the vetting of that information of those credentials happens there. Then, when a request is made, they're attached to the request and sent down to the requester. Then it's the requester's job to determine, based on all of that information … Again, the goal is to ensure, based on our policy, that as much information is provided as possible to give the disclosure the opportunity to properly respond. How much of that is automated we're debating, and how far that automation goes we're currently debating. I was under the impression that, without

getting into that separate discussion, there could be situations where that would be sufficient to respond without human intervention to a request.

I think, in terms of this building block, we just simply need to just define the framework of how all this information can be gathered to ensure that a sufficient … And to make sure that, when it is received by the disclosing party, it's helpful and useful and gives them the opportunity to process the request [if] they want.

MILTON MUELLER: You've made a lot of progress here, Alex. I think I'd still want to revert to something more like the original wording [inaudible]. But on the whole, I think we're making progress. Thanks.

ALEX DEACON: Thank you.

JANIS KARKLINS: Thank you. Let me take the next comments. Hadia, Alan G, and Mark Sv, in that order.

HADIA ELMINIAWI: Thank you, Alex, for putting all this effort. My suggestion is to not talk about automation at this point. Here those [inaudible] are talking only about accreditation. Maybe sticking to this part now is better. Technically speaking, would automation be possible? Well, yes. Technically it would be possible, but whether it will happen or not is another thing.

To talk about the authorization credentials, my understanding, Alex, is that, ultimately speaking, authorization credentials would also include authorization to a certain set of data according to the purpose and the identity, regardless of who does what.

So I just want to confirm this, that the authorization credentials include also authorization to a certain set of data.

JANIS KARKLINS: Thank you, Hadia.

HADIA ELMINIAWI: Ultimately, it will include that.

JANIS KARKLINS: Thanks. Let me remind you that we're talking now about working definitions, specifically on credentials. Alan Greenberg?

ALAN GREENBERG: Thank you very much. In response to Milton – I know that's not what we're talking about, but I think it's important that we stop that discussion now and have it when we actually are going to be talking about [what] automation is possible – I just wanted to make it clear. Certainly in my mind no automation is guaranteed but we are expecting relatively large numbers of request for data and there are likely to be patterns in them. It may be possible, once we determine what those patterns are, that some kinds of requests end up being automated because they're repetitive and we know what the results will be. That may not be the case. That's what

we're going to have to discuss. But let's not pretend that we're getting five request in and they're all going to be completely different and there's no way of understanding patterns. Patterns are important in this business. Thank you.

JANIS KARKLINS: Thank you. And I think that the policy recommendations differ a lot from implementation, as well as ongoing management of the system.

Mark Sv, please, followed by Volker.

MARK SVANCAREK: I agree with everyone who said that this is just definitions and that we should talk about the implementation a little bit later. I did want to emphasize, though, that I see this a chain of decision points: were you able to log in, did you follow the protocol, is the payload complete? Eventually you get to the point where it's like, does this require human intervention or not? We haven't defined how that's actually going to work. I do see the authorization credentials as being part of that decision. I'm asking for some data that's different from what I'm authorized. Something like that. I think there could be a number of red-flag items or events that push you down one chain of a decision tree versus the other chain of the decision tree. I still envisage, even if you go down the algorithmic path, that there is still a decision point there. So, even if you down the augmented path, there's probably still another decision on whether or not to give you the data or not.

I don't know whether it's appropriate to talk about that level of detail right now – probably not – but I just wanted to put that idea out so that we could perhaps have a little bit more comfort as we proceed out of this section and into the next section. Thank you.

JANIS KARKLINS: Thank you. Volker?

VOLKER GREIMANN: Thank you, Janis. Two points. With the authorization for certain data, as Hadia suggested, I don't think that's necessarily something that should be baked into the identifier or authorization or credentialing. That's something that very much depends on the reason why the requester requests certain data. [That's] part of the request, not the part of the authorization.

In regards to what Alan suggestion, I certainly agree that certain aggregated data may lead to certain patterns, and these patterns are important. I just wonder. Once certain patterns have been detected, maybe the requester should contact the registrar directly. They'd be able to help them with a request outside the SSAD and thereby make a certain response. That would probably be easier for both us and the requester to respond in that manner outside of the SSAD system. If it's a bulk request, I'm certain that we should be able to accommodate that, and most registrars would be able to accommodate that. But I don't think that's something that we should necessarily have to bake into the SSAD. Maybe foresee certain channels or path to that end that would be outside the SSAD but leave the SSAD for the low-

volume requests and have the high-volume request for bulk data in a different path. Just an idea.

JANIS KARKLINS: Thanks. I didn't hear any specific comments on credentials. Let me take down now this part until the end of the working definitions. So, revocation, de-accreditation, identity provider. Any issues with those?

Okay, not requests. Good. Now, once we are done, in principle, with the working definitions, we'll go to the recommendation part. Here let me take Point A and Point B. I think we have gone through them, and that should be already approved. The understanding should be reached on A and B.

Sarah, do you agree with me?

SARAH WYLD: Thank you. Good morning. I'm hearing a lot of feedback on my own line.

JANIS KARKLINS: Yeah, it's a little but funny. But still we can understand you.

SARAH WYLD: Okay. Thank you very much. We did submit some comments earlier this week on the previous version. I'm just not seeing those comments reflected in this version of the document, so I wanted to check in about that. Specifically we had left a comment on this

Point A regarding whether non-accredited users can make requests for data in this platform. I'm going to just paste that into the chat to make sure that everybody has had a chance to consider that comment. Thank you.

JANIS KARKLINS: Thank you, Sarah. Marika, have the registrars' comments been taken into account in your version?

MARIKA KONINGS: Thanks, Janis. We did note in the e-mail that, in order to make this a more cleaner version, we did delete all the comments. But they're still visible I the older version. I believe that was also a point that was discussed on the previous call. At least staff's understanding was that, from earlier conversations, many felt that an accreditation framework should not prevent those from not seeing a benefit of accreditation or having a one-off request being excluded from using SSAD.

So I think it's a good point to have that conversation if that sentiment has changed or whether the group believes that it should be exclusive; basically that the only way to access SSAD is through the accreditation framework. Of course, if that is the case, then this principle would need to be changed. But, as I said, this assumption was made based on, I think, our original conversations. Many seemed to feel that there shouldn't be a requirement to make use of SSAD.

JANIS KARKLINS: Thank you. Sarah, are you satisfied with the explanation?

SARAH WYLD: I'd like to defer to my colleague, James.

JANIS KARKLINS: Okay. James?

James?

JAMES GLAVIN: Sorry. Thanks for flagging that, Sarah. I think that a lot of the substance of registrar comments particularly went to that question of whether or not unaccredited users could use this system. I think it is a foundational question and I think we need to tackle it. First of all, we should point out that it's not assumed – at least I don't assume – that registries and registrars wouldn't continue to operate some form of RDS lookup service on their websites, perhaps not standard or perhaps not displaying non-public information or providing a mechanism to access non-public information.

So I want to make sure that we're not trying to solve for the universe of potential use cases in SSAD because SSAD, I think, is meant for a particular category of uses and also is meant to standardize those uses and those responses. So I think that accreditation starts to lose its value if we say, "Yeah, jump through all these hoops. Pay these fees. Do all this other stuff. Follow these rules. Abide by this code of conduct as we saw in the

previous building block. But, if you don't have of that stuff, that's okay. You can come in anyway." Then I think I start to scratch my head and say, "What are we doing here?"

Now, we can't even talk about the possibility that there might be services that pop up that take and aggregate a lot of single or one-off users and bundle them into some sort of an SSAD accreditation, like a reseller or something like that. There's all kinds of possibilities that might be solved, but I think eliminating accreditation and just allowing anyone to use the system is probably not the way to go. Thanks.

JANIS KARKLINS: Okay, thank you. Though, honestly, James, I thought that we had a number of discussions here and there was a divergence of opinion in that situation. Probably we cannot go for restriction but we need to open it for everyone with the understanding that accredited entities' requests will go through the system in now time, and, for those who have not through accreditation, the first step will be to basically accreditation, not calling it accreditation but clarification of identity, ticking all kinds of boxes of the code of conduct and so on. That would be a much slower process, also associated with some fees that need to be paid for doing this request. But I don't have any specific opinion on that, and I'm happy to accommodate. If we can converge on that system, SSAD could be used exclusively be accredited entities and individuals. That's perfectly fine.

Let me take Alex and then Alan Greenberg.

ALEX DEACON: Thanks, Janis. I think, on this topic, when Milton and I originally thought this through – I'm just digging up the original Google Doc that we put together – we suggested that there were at least three ways to deal with, I guess, non-accredited users. You could spin up a new identity provider in this new framework for their specific use. The second one is you could allow them to self-identify and self-assert the content of their request. That has impacts, clearly, on how the discloser processes them and the like, but I think that's a possibility. These are essentially requests that have credentials that can't be validated easily. Then the third one, which I'm seeing we suggested in our original doc, was that unaccredited users could continue to use the reasonable access mechanism defined in Phase 1 Recommendation 18. There may be more.

I think there are ways for us to accommodate non-accredited users and in a way that hopefully still adds value to those requesters and users and whoever is going to be doing the disclosure. Thanks.

JANIS KARKLINS: Thank you. Alan Greenberg?

ALAN GREENBERG: Thank you very much. An unaccredited user in this process clearly is not going to have access, or none of the automation assistance tools will be used. So clearly it's going to be slower, if it works at all.

The real benefit, however, is that it's tracked and logged so that, later on, if a data subject says, "I want to know who has access to my data," if a non-accredited requester was successful ultimately, then it would be there. it would be logged, it would be all tracked, and we have all the information. So it becomes a single source for addressing the data subject's queries, among other things, and for audits and all sorts of things. So there's strong benefits of going through the system, even though it may be a different path through the system. Just being in the system means you have a certain control over it that I think has very strong benefits. Thank you.

JANIS KARKLINS: Thank you, Alan. I still hear that we cannot completely rule out a situation when somebody non-accredited is wishing to send in a request.

I see Chris and Milton. Chris?

CHRIS LEWIS-EVANS: Thanks, Janis. I think within the GAC we said a couple times that we really want to a centralized, uniform mechanism for everyone to gain access to the data that has a legal basis to do this. I think, as James said, really the main question here is, is that mechanism provided by a Phase 1 recommendation, which could possibly not be uniform, with each registrar having a different system to gain access to that data? Or is there a way easily of producing a stream to the SSAD that allows a uniform mechanism to do that?

So I think, certainly from my [inaudible], that's some of the considerations we need to think about while we're considering this. Thank you.

JANIS KARKLINS: Thank you. Milton?

MILTON MUELLER: I just want to say that I was one of the people who said that anybody should be able to use the system and that accreditation should not be necessarily. I really have changed my mind on that. As we get deeper and deeper into constructing this thing, I think we really have to insist that the SSAD itself does have to be used only be accredited users. I guess we can still leave the door open to a non-standardized request. That is something completely outside of the SSAD in which maybe somebody walks up to GoDaddy's headquarters in Idaho and knocks on the doors and turns in a request on a piece of paper. I think we can't rule that out, but I think, for the SSAD, we have to be consistent and standardize across the board. There will be all kinds of strange arbitrage going on if we try to create different sets of rules for accessing that system.

JANIS KARKLINS: Okay. Then let me ask a question because that's really fundamental now. Is there any opposition to that we continue talking about use of SSAD only by accredited entities and individuals? Because, again, that is a systemic issue. So we need everyone to be on the same page. If we cannot be on the same

page, then we need to go on the lower denominator. We create a fast track for accredited and we create a slow track, which includes steps that accredited entities should go through before the request is examined.

Margie, Laureen, and Marc Anderson, in that order, please.

MARGIE MILAM: Hi. The one thing that I think might encourage us to allow an unaccredited access to the SSAD is that these issues of evaluating GDPR and other privacy laws across the world as they apply to registrants is really complicated. I would think that whoever is running the SSAD, if it's ICANN in this case, will develop an expertise in what's a legitimate request and what isn't. You'll get much more standardization from that because of the experience that ICANN has and will have as it's evaluating all of these requests.

So I think that's a useful thing and I think it doesn't mean that, if someone comes through without an accreditation, they get a speed of a result or that they get any kind of automation in the same way that an accredited person would. But I do see value in having at least that door open for the unaccredited folks. That way, ICANN's expertise and approach to addressing those issues would be consistent across all requests.

JANIS KARKLINS: Thank you, Margie. Of course, we can think of an interface. Then the first question is: are you accredited? Yes/no. Yes? Provide your credentials. No? Then it's another track saying, "Please

provide proof of your identity." Then you go through a completely different path than those who have credentials. They go straight to the topic.

Laureen, please?

LAUREEN KAPIN: Thanks, Janis. I think that, leveraging on what you're saying, it's very important for the public at large to have a consistent and efficient mechanism. That doesn't mean it needs to be as efficient as these accredited users. There are many reasons why it wouldn't be. But we would very much opposed to not having a centralized, uniform system because then we would be devolving into a scenario where the public, which is especially ill-equipped to know how to make these request and even to whom to make these request, is put in an even less informed position because they will have to abide by the multiplicity of systems that individual registrars and registries might put into play. If we're going to have a uniform and centralized mechanism, it would make sense to leverage that to have a separate, albeit likely slower and more complicate path, for the public to be able to access that system as well. I'm not sure I understand the arguments disfavoring that approach.

JANIS KARKLINS: Thank you. Marc Anderson?

MARC ANDERSON: Thanks, Janis. I'm raising my hand on the question. I understand this discussion is about whether or not SSAD must allow access to accredited and non-accredited users or if we should restrict access to just accredited users. I guess, like Milton, I find myself thinking, as we get more and more into the building of what this SSAD system is, how it's going to work, and what it's going to do, the more, really, you're going to need to be accredited to be able to use it, just from a pure, practical implementation standpoint. So I find myself leaning towards supporting a position that you must be accredited to use the SSAD system.

Referring back to the e-mail I sent previously that Brian King mentioned in chat, I think it's important that SSAD be available to anyone. Really getting back to Laureen's point, there should be a single centralized place that anybody can go. So, if we agree that SSAD must be restricted only to accredited users, I think it's important that accreditation be available to everyone.

JANIS KARKLINS: Thank you. Actually, that is what I was trying to say. [So if you go, "A non-accredited would go,"] then, if we could not provide credentials, it goes to the slow track, which starts with basically identification of the identity of the requester. Then the requester needs to provide some information that is verifiable. Once that is verified by somebody who is running the business, then it gets back on [further to] SSAD, and then the request is looked at by merit. So one can say that this bypass or that slow track is maybe slightly simplified accreditation because it assumes that the one-time requester would not be coming back for any other request. But we would not discriminate against anyone to be able to use

the system because that is also an issue that we may face at the end.

Let me see. Georgios and Mark Sv. Georgios?

GEORGIOS TSELENTIS: Thank you. Regarding this question, I think there is an issue also of accountability. I see in the accreditation that there is a necessary part of identification of the requester that has to be done. This doesn't mean that the SSAD is not available. It is available to people to ask the questions. But, to my understanding, down the road, the system has to have a sort of accountability. If we don't have at least the minimum part of identification of who asks the question, we cannot go back and give the necessarily safeguards for accountability further down the road of how the system might respond later on.

So I think it would be good to provide a low entry point for simple requests, but there are minimum safeguards that have to be at least in the system to know who's asking the request to start with. I don't know if we can build this inside the system at this time or leave it for implementation later on. From the discussion so far, I'm inclined to say that at least the minimum part of identification from the accreditation process needs to be there for everybody that uses this system. Thanks.

JANIS KARKLINS: Thank you. Mark Sv?

MARK SVANCAREK: I've always been on the opinion that SSAD should be an accreditation-only system while I also recognized that there were unaccredited people who would need to request this data. But as I listen to this conversation here, I'm realizing that that requires us to actually make two things, which seems like a really bad idea. So now I've come back to where I think a lot of other people have come to, that everyone should be accredited but there can be lower bars to some sorts of accreditation. Then, in my proposed decision tree that I mentioned earlier, that would be one of those red flags that would push you down, as Janis said, the slow path. I think that is the human intervention path.

So I think I'm going to throw my support behind the idea of a lower bar of accreditation. But everyone needs to be accredited. Thank you.

JANIS KARKLINS: Okay. Can we agree that the users of SSAD should be accredited but then those who do not have accreditation may submit request for disclosure with the understanding that they would go through a simplified accreditation procedure for one of the requests? Then, if they would decide to send another request, they would go through the same procedure, and that would be the same verification of identity and signing of the code of conduct and so on.

Amr, are you in agreement?

AMR ELSADR: Hi, Janis. Well, I would ask the question that I posed in the chat. I don't see any practical advantage to even a one-time requester

not being accredited. I just saw Brian's comment in the chat, and I'm not sure that I understand the difference between accreditation and advanced accreditation. I would assume that a requester who comes in once and never comes in again would have to go through the practical steps involved with accreditation anyway and [so would] become accredited one way or the other.

Now, if that requester never comes back to try use SSAD, then obviously its accreditation would not be renewed and then would simply fall out of the system, I guess, one way or the other. But I don't understand what problem we're trying to fix here by trying to say that someone comes in once doesn't need to be accredited. That person would have to go through the same steps, so what is the issue with a one-off requester being accredited? I'm just trying to understand what the concern or the problem is. Thank you.

JANIS KARKLINS: The thing is that the process of accreditation generates the benefits for accredited entities like passwords and then the easy access and so on, which would bring them immediately to the core of the system. Their request will be treated immediately. But those who do not have accreditation would need to provide their identity, and this should be verified. They would need to sign the code of conduct or tick the box of the code of conduct, becoming liable if they violate that code of conduct or potentially may become liable if they violate. But they would never receive neither password nor anything else. So then they would need to pay, and then their request would be looked at and answered or rejected.

So that's the difference between simplified verification of identity and fully-fledged accreditation, where accredited entities will use SSAD many times throughout whatever period of time.

We really need to wrap up this conversation. Milton, Greg, and Alan.

MILTON MUELLER: Janis, I just wanted to take issue a bit with your attempt to wrap things up in a summary. I think that you are still talking about two separate systems rather than a uniform system. I don't think that's where we're going right now. I think where we're going is more what Mark Sv identifies, which is you lower the bar for accreditation a bit in terms of ease, but everybody has to be accredited fundamentally on the same terms. They would have the same, for example, [AUP]. I think that's where we're heading.

It's also possible to define the parameters of accreditation basically in terms of number of requests in ways that would accommodate individual users without breaking uniformity or standardization. For example, you could say, "This accreditation gives you two requests, and that's it. And you disappear from the system." But the terms of which accreditor [are] exactly the same as Facebook.

I think that's where we have to go with this. I can just see all of the tricks and all of the automated systems and all of the arbitrages that's going to take place if we try to create different tiers for individual users. People who are not really individual users will

start to try log as individual users if they think they can get easier access and so on and so forth.

So I think we have agreed that we want uniformity and we want to everyone to be accredited if they're using SSAD. The question is just what are those accreditation mechanisms? [inaudible]

JANIS KARKLINS: Thanks, Milton. Greg?

GREG AARON: That's where I am, which is we're trying to add way too much complexity to this system. It's much more straightforward if all users are accredited. They go through a similar process. This system is designed to serve people who will have a regular or semi-regular use and therefore think it's worth going through an entire process to get accreditation. A halfway accreditation isn't really an accreditation.

We can also keep in mind that people who have a one-time need can go offline. They can make their request directly to the data controller. The only advantage of trying to go through this system is that that gets tracked somehow. I think we can tell people, "If you have a one-time request, this is how you do it. Go contact the registrar," or whatever.

This hybrid system offers a variety of problems. Still, everybody is going to have usernames and passwords and some sort of credentials. We're making it way too complicated. Thanks.

JANIS KARKLINS: Thank you. Alan Greenberg?

ALAN GREENBERG: Thank you. Although I think there are benefits to having a single pass and tracking even if it's handled differently. I'm ceasing to care at this point. However, I'll note that, if we go passing "everyone must be accredited," then, remember, we've also decided, I think, that accreditation is a fee-based system. If we're now imposing a potentially large fee and maybe a significant amount of time on accreditation for a one-time user, I think we're going into a problem area. Thank you.

JANIS KARKLINS: Thank you. I see that there is no common understanding of this; one that we can converge that there should be accreditation for, let's say, frequent users of the system. An unanswered question is how we deal with potential one-time users of the system. So there is an understanding that they also should go through the accreditation, but accreditation may be the lower bar accreditation. Probably we need to think how we can reflect it in the policy recommendations. In principle, probably we need to converge on an understanding that each user of SSAD would be accredited in some way.

Can we agree on that type of assertion?

Greg, I understand this is your old hand up.

Okay, we will think how to reflect that, then, in the text. So, Point C and D. Any issues?

Alan Woods?

ALAN WOODS: Thank you. I have a small nitpick with D. Just reading it the way it is, it says, "The decision to authorize disclosure of registration data based on the validation of the identity credential" – oh, I can't even speak. Sorry. But it's the next [thing], saying "any other data contained." It's pedantic, but the "any other data" contained, as far as I'm concerned, is probably going to be the heavier lift on this. It just seems to relegate into something that's mere in significance in comparison to the identity credentials and the authentication credentials. I don't mean to just point out an issue, but I think we should probably put more ways on the other "any other data" and not consider it merely as an afterthought. That's my view on that. Thank you.

JANIS KARKLINS: Okay. What's your proposal then, Alan?

ALAN WOODS: As I said, I'm on the fly here. I just want to literally get that any of the data is much more important than just those two alone. So I don't actually have writing. I thought we weren't going to be on the fly but –

JANIS KARKLINS: Okay. You will then provide [inaudible] [by Friday].

ALAN WOODS: Yeah.

JANIS KARKLINS: Okay, thanks. Alex Deacon?

ALEX DEACON: Hi. Just to reply to Alan there, I think we could definitely improve that text, perhaps replacing the part of the text that you raised, Alan, with something along the lines of "[End] data as required in Building Block A." That may do the trick. It basically says we've set policy with regard to important data that needs to be included in the request and that also needs to be included. Anyway, maybe we don't want to wordsmith, but that was just my thought.

JANIS KARKLINS: Thank you. Let's see now. The benefits of accreditation, E and F. Any issues with E and F?

I see no requests. Then let's see whether we can get lower down. Amr?

AMR ELSADR: Thanks, Janis. On E, it's factually correct, I think. I'm not sure if there is a benefit. And if it is a benefit, for whom is the benefit. It seems more like a feature to me than benefit. I would assume that

it would benefit whoever is operating the SSAD as well as the requester if they keep coming back for more disclosure requests. But I'm not sure. It depends on why we're putting this up here.

JANIS KARKLINS: I think here we are trying to say why accreditation is needed and what that gives to the requester. So that's the meaning or the title.

AMR ELSADR: Okay. [inaudible]

JANIS KARKLINS: Nothing more than that. Can we scroll down and see what's next on G?

Alex, your hand is up.

ALEX DEACON: Based on our previous discussion, perhaps at least the last part of G … Maybe it's best if it's removed from here and placed in this new building block that we have for – I forget what we called it – automation. Thanks.

JANIS KARKLINS: Okay, thanks. Amr?

AMR ELSADR: Thanks. I'm just wondering, when we use the words "validate" or "verify" in this context, whether it's similar to what we understand it to mean when we talk about some of the RDS requirements on contracted parties. So is SSAD meant to only validate the identity credentials, or it is also meant to verify them? Because I think that would make a big difference. I always thought it leaned more towards verification of identity rather than validation of the credentials. So it would be helpful if I hear other people's thoughts on this. Thank you.

JANIS KARKLINS: Thank you, Amr. Alex?

Alex, could you explain?

ALEX DEACON: Yes. Thanks, Amr. Yeah, I think we could do a better job of being consistent. Maybe I can take an action to define the term. Essentially what I think – well, at least was I trying to describe here is that, when a request is received, the identity credential will need to be checked to ensure it's correct and well-formed and not revoked. So perhaps we need to define the term of "validation" or "verify" and just clean up the text to ensure everyone knows what we're talking about.

JANIS KARKLINS: Thank you. Thank you for volunteering by Friday. Let's go to , which is the baseline for the code of conduct. Any issue with this one?

Alex, your hand is up again. Please go ahead, Alex.

ALEX DEACON: Again, just to set this up, I think it's important that we end up with – you'll see I used lower-case code of conduct in quotes here. I think we need to define and document how this accreditation body is going to work in a way that will allow us to meet or obtain a code of conduct in the future. As I mentioned, I went through the European Data Protection Board's document regarding code of conducts and tried to distill to this list – here's tons of information missing here – of items that will need to create when we spin up this accreditation authority. My hope is that, once we've done that and fill in the details and document all the processes and all the things that are a requirement under those guidelines, we'll be in a good spot to get a code of conduct in the future for when we think it makes sense. Thanks.

JANIS KARKLINS: Thank you. Alan Woods?

ALAN WOODS: Thank you. Actually, Alex may have just answered my question. I was going to offer words of caution against code of conduct unless we are walking full-on into the concept of, what is the code of conduct as stated in the law? I think that there's an element that we would be hoping to do that. if that is the [conflict] behind that, then I have no problem with it. I was just going to utter words of caution. Thank you.

JANIS KARKLINS: Thank you. So no substantive comments on this. Good. Now let's see whether we can look at J on accreditation authority on new points. Any issue with that?

Alex, it's an old hand, right?

ALEX DEACON: It's an old hand.

JANIS KARKLINS: So no hands up for J. Now K. It's self-evident. And L?

Making no request for the floor, let us move down on revocation and abuse: M.

No requests. O?

No requests. P and Q?

Milton?

MILTON MUELLER: I think we're just going to have to alter or eliminate that reference to submitting an SSAD request as a non-accredited organization based on—

JANIS KARKLINS: Yes, that will [inaudible]. Staff, I would like to ask you to note and then subsequently delete.

Okay. De-accreditation of the accrediting authority. Nuclear option.

Milton?

MILTON MUELLER: I would want to add something like a systemic failure to actually enforce [AUPs] or some kind of … I'm not sure what "An audit failure can't be remedied" means exactly. Does this mean that they continually fail audits? In that case, I like that. But I think the wording should be clarified. These SLAs – were those defined anywhere? Have we referenced SLAs between accreditation authority and ICANN or whatever nameless entity that accredits them? So, yeah, this needs work. It's pretty obvious. It says "others." Whoever wrote this – I guess it was Alex – knows that this needs to be thought through a little more and fleshed out. So that would be something.

JANIS KARKLINS: Thank you, Milton. You'll have [a change] by Friday, also to contribute to this reflection in writing.

James?

JAMES GALVIN: Hi. Thanks. I was looking at Bullet Point R. You caught me multi-tasking here, so apologies if I've missed this elsewhere. My question is, if we de-accredit an accreditation authority, does that by nature revoke the accreditations that they may have issued or

that may be persistent under that authority? I'm thinking here of an analog with, for example, an SSL certificate where, if there was something wrong with the certificate authority, we would probably revoke the certificates associated with that authority. Have we covered that somewhere or provided some recommendations that accreditations be revoked or transferred? How's that going to be handled?

JANIS KARKLINS: No, we haven't discussed it because this is very new and this has just been proposed.

Let me talk Marc Anderson first and then Alex.

MARC ANDERSON: Thanks, Janis. I think this is maybe a question for Alex. On [inaudible], if you have a concept of graduating penalties but not on the accreditation authority itself – at least, if you do, I'm missing it – I would think graduating penalties would work for the accreditation authority as well. Any thoughts on that?

JANIS KARKLINS: Thank you, Marc, for your question. Alex?

ALEX DEACON: Hi. Just at a high level, before I answer Marc's specific question, this [RS] does need some work. Originally I just had that first bullet point: All the audit failure that can't be remedied, assuming that all of the important aspects of the accreditation body would be

covered in the audit, would probably be grounds de-accreditation of finding a new accreditation authority.

The SLAs – I was just trying to have more than one bullet there. So that may be premature, but I think, at a high level, we need to think more about this and flesh this out.

I think also that we need to clean up some of the details. Well, we need to clean up this section to make sure it's in line with our assumption that there'll be a single accreditation authority and multiple identity providers and the like.

Marc, sorry. Can you repeat your question?

MARC ANDERSON: Thanks, Alex. I was just wondering why you didn't include escalating penalties [in] the accreditation authority section like you did in the section for accredited users. I would think you'd want it in both places. I guess that's basically my [inaudible].

ALEX DEACON: I agree. So we could clean that up, I think. Absolutely.

JANIS KARKLINS: Okay. You volunteer, Alex, to do that, right?

ALEX DEACON: I will put it on my list.

JANIS KARKLINS: Thank you. Let's move on then to "Accredited organizations and individuals must agree to …" There is a wrong numbering. Any issue with that?

No issues. Alex, it's your old hand. Let's see now on fees. Would these principles be acceptable? Of course, in the implementation phase, there will be more on the fee structure. Here it is just the principles by themselves.

I have Alex, Sarah, and Brian.

ALEX DEACON: I think my comment here was that, while this important information, it probably should live in our fees building block and not also here. Thanks.

JANIS KARKLINS: Thank you. Sarah?

SARAH WYLD: Thank you. My hand is up to say the same thing. We agree with the proposal that this should be moved to the fees building block. Thank you.

JANIS KARKLINS: Brian?

BRIAN KING: Thanks, Janis. No disagreement with either of the previous two comments. I would wonder here if a footnote is applicable since we seem to be in agreement that everyone should be accredited in some way or to some extent here, that, without changing B, if [there]s] some sort of automated accreditation where the requester perhaps just validates their e-mail address and clicks to agree with the AUP, that cost of accrediting a one-off user would be minimal. So a one-off requester would not be charged an accreditation fee. That might be an appropriate footnote here. But we can do that when we move this, too. Thanks.

JANIS KARKLINS: Thank you, Brian. I have no issue moving it to the fees building block. The only question in my mind is whether we need not to leave at least one fundamental principle – that would be, for instance, in A – and then adding there that the remaining issue about fees would be addressed in the fee building block. Something like that. Otherwise, if we do not list here an accreditation that this is will be based on a cost recovery system, then we're missing an important point in this context. That's why.

Would that be agreeable?

Okay. We will leave simply "fundamental affirmation" then, but accreditation will be part of the cost recovery system as described in the building block on fees. We will move the rest to that building block.

Technical capabilities. Any issue with the technical capabilities?

Marc Anderson?

MARC ANDERSON: Hey, Janis. Thanks. I think it's a little bit premature to get into the technical capabilities. Also I added this comment this later, but I think it's probably more appropriate to have the technical capabilities in the implementation guidance. At a high level, really what I think we're saying is that there must be a mechanism for the RDAP, the SSAD, and the disclosing entities to communicate with each other. We already know that RDAP is likely the tool for facilitating this. So I think we know that there needs to be interoperability between the different parts of this, but the actual language that we need is hard to say until we've defined it a little bit further. I also think that is probably implementation guidance, not policy recommendation.

JANIS KARKLINS: Okay. I think that this was one of the charter questions, if I'm not mistaken, that we need to answer on interoperability.

Hadia, please?

HADIA ELMINIAWI: Thank you, Janis. I would tend to agree with Marc that it is quite difficult now to say what's really required here. But, for sure, yes, the standardized [inaudible] disclosure should be able to recognize accredited requesters, then that's something we want to happen. Also, RDAP should be able to identify the accredited users as well. As far as we know, RDAP already does.

The other thing that, at some point in time, we should need to look at – maybe not now because many of the elements of the system are still unknown – is who gets what. For example, we decided that, with accreditation, there comes some credentials, unique identifiers, and then authorization credentials as well. If you have, for example, the contracted parties not the ones making the decision and maybe the disclosure is through some other entity, then for sure it's not necessary for them to have the credentials.

However, they would like or want to have the credentials. I think this is a policy issue, like who should get the credentials if it is not necessary to get the credentials? It's something that the policy should decide, not necessarily here or now. But at some point in time, we should be able to do that. Thank you.

JANIS KARKLINS: Thank you. There is a suggestion to move the technical capabilities into the implementation guidance part. We would, for the moment, put that in brackets and not discuss it now. Now let me see very quickly, on implementation guidance, if there are any specific issues on implementation guidance as it is now on the screen?

Marika?

MARIKA KONINGS: Thanks, Janis. Just as a general point – I think Alex already noted this as well – I think it would be good, as the group reviews the overall structure of the document, to look into if there are any elements that are currently in implementation that really should

belong in the policy recommendation section, or vice-versa. So I just wanted to make that general note.

JANIS KARKLINS: Thank you. What I would like now to suggest is I think we have made enormous progress in building this common understanding of accreditation. Now we need to do a little bit of wordsmithing. I hope that, next Tuesday, we will be able to stabilize this building block and look in more detail [inaudible].

What is my suggestion? First, I would like to ask staff to clean up this text – what we reviewed today – put the numbering in the right order, and accept all [Marc's] changes and things and publish the clean version of the text after the call immediately for the benefit of the team. So team members, starting with Alex, work on the new clean version of the text that will be put out by staff and provide all editorial suggestions – I don't know; is that a Google Doc or how will it be organized? – by Friday so then the staff can review and propose a final version of the text for reading on Tuesday. So that is since we are meeting on Tuesday. This will be the last meeting before Montreal. It would be good if we could review that over the weekend and post the final version of the accreditation building block Monday morning before the call on Tuesday. So that's the proposal from my side.

In absence of any objections, let us now move to the next agenda item, and that is Agenda Item 5: terms of use, disclosure agreements, and privacy policies (in other words, Building Block M). Building Block M was developed by Hadia working together with staff, if I'm not mistaken. Now the text is on the screen. I

would like, since this is a first reading, to invite any comments of a general nature that team members may wish to make.

Hadia?

HADIA ELMINIAWI: Thank you, Janis. I just want to note that the staff put together some general notes. Those actually might be enough. I just below started to be more specific. We don't necessarily need that, but I just put it as an idea. Thank you.

JANIS KARKLINS: Thank you. Any comments of a general nature related to Building Block M?

Brian?

BRIAN KING: Hey, Janis. Thanks. One comment is that, if we're going to be talking about the terms of use, I think it makes sense for us just to draft the terms of use. I think that for two reasons. One is that, if we're going to have consensus on what this system is going to look like, the terms of using it are going to be material to that consensus. Two, I don't have to do this twice. If the intended exercise here is that we come up with some concepts about what is going to go into the terms of use and then in the IRT or elsewhere, the terms of use have to be drafted again. Let's just do it once. So that was initial thought. I welcome other perspectives on what we're doing here. Thanks.

JANIS KARKLINS: Thank you, Brian. Are you volunteering to put pen to the paper?

BRIAN KING: Totally.

JANIS KARKLINS: Marc Anderson?

MARC ANDERSON: Thanks, Janis. There's some general principles here in Building Block M. The first thing that really jumps out at me is that it's not very clear on exactly what point in the process we're talking about. Would these be terms of use/disclosure agreements/privacy policies that would apply when a perspective user signs up for or is accredited through an accreditation body? Or are these things you agree to at the time you access the SSAD system? Or are these things that are intended to apply when your terms of use would apply to a disclosure request?

Based on the conversations we've had, I think we've talked about all of these concepts. I think we've talked about how, once you're accredited, you agreed to some things as part of your accreditation. I think you also agree that some of these things are intended to apply at the time as part of your access to the SSAD system. Still others are intended really as terms of use for disclosure of the data when that disclosure occurs.

But that really doesn't come to me in reading through the document. So I think that's really my feedback on this: it needs to be a little clearer on exactly what we're intending this recommendation to apply to.

JANIS KARKLINS: Okay. There should be a reason why this building block was suggested in the first place. Let me see if staff could remind all of us where this idea came from.

Marika?

MARIKA KONINGS: Thanks, Janis. I just scrolled down to the language that's also in the building block that we've taken from the worksheet. As you may recall, we originally outlined all the topics and items that the group thought needed to be addressed and aligned them as well with the specific objective around what we were hoping to address in relation to that topic. I think we also flagged the mind map questions or the charter questions that were related to that. we also included some of the TSG questions that might help inform the conversation and provide links to relevant information that might be helpful to inform this discussion. So that's where this originates from.

I do know that Marc put in here as a comment as well that – I'm not sure if all the [questions] have been answered, but my assumption is, once we've answered the other building blocks, that some of that may also find its way then into this building block. I think, from our side – again, to think we asked for

volunteers a couple of times to help us with this one – as no one stepped up, we took a first stab. It's fairly general, indeed, I think, as people have noted what's in there.

So one of the things the group may need to decide or want to decide indeed is how specific do you want to get at this stage. Is it sufficient to say that the relevant terms of use and disclosure agreements and privacy polices need to be put in place that are informed and build upon the recommendations that can be found in the building blocks and that is something then that is further worked out in the implementation? Or [inaudible] a suggestion: does the group feel that it wants to hold the pen on those here in this phase of work? If so, what is the best way to do that?

I hope that provides the additional context here for why this item is here. Again, I think one of the questions is, how much detail do people think is needed in response to this building block? Or is it sufficient to know that appropriate arrangements need to be put in place, and the basis for that is the recommendations that can be found in all the other work the group has done?

JANIS KARKLINS: Thank you, Marika, for these explanations. Marc, did Marika answer your question?

MARC ANDERSON: I think her explanation supports my question, not answers it. I think my question maps back to those foundational questions and questions in the charter. As Mark noted, they haven't really fully been answered. I think Marika's final question – to what degree do

we need to define these things in policy? – is a very relevant one that we haven't really tackled yet in this group. That may be the first question we really need to come to agreement on: what do we need to have included in the policy, and how explicit does the policy need to be? Terms of use are likely to vary from entity to entity and jurisdiction to jurisdiction. I'm not sure how much we can or should be defining that explicitly in the EPDP. So that might be a good first place to start.

JANIS KARKLINS: Thank you. Let me take other comments. Margie?

MARGIE MILAM: Can you hear me?

JANIS KARKLINS: Yes, Margie. We can hear you.

MARGIE MILAM: Okay. Thank you. I share a lot of the same concerns that Marc mentioned. I think Marika did support the questions that there really isn't an answer here.

My concern with the language we have here is that it may be inconsistent with what we've done in the other building blocks. So I think, at a minimum, if we're going to provide more clarity in this building block, we wait until we've finished all the rest because then I think some of the questions that we're still working through – like, what are the purposes? Is ICANN going to be the controller

– we haven't really resolved yet. So it's really hard to do this right now.

I'm not sure I'm comfortable leaving it for the implementation team, but I don't think that means we have to write the whole policy, either. We could say something like, "The privacy policy needs to include, at a minimum, these items." But I don't see how we can even clarify it right now until we've done all that other work.

Marc is exactly right. Each entity has to comply with local law, so the privacy policy in the end – the full text – isn't something that either this team or the implementation team would do. But we could at least point out things that should be in there once we finished all our work.

JANIS KARKLINS: Okay. Then my take is maybe that we need to put aside for the moment this building block and see where we get with others and then come back to it and see what type of information or recommendations we could put here. At the same time, on terms of use, maybe it would make sense to start slowly gathering input. Since Brian volunteered to maybe make a first stab on terms of use – even it may vary – [we could] put a skeleton of terms of use together that we could look at at one point down the line.

Would that be acceptable? Brian, would you volunteer to do that?

Brian?

BRIAN KING Hey, Janis. Sure, I'd be happy to do that if the group wants to go down that path. I don't want to waste my time if we're not going to do it, but, yeah, I'd be happy to you.

JANIS KARKLINS: If you think – I think that there will be a need for terms of use in one way or another, then at least I said not yet the full but just the skeleton (what that could entail, what are the major elements of that type of agreement).

BRIAN KING: Okay.

JANIS KARKLINS: Thanks. Let us see now the next building block: purposes and user groups. Marika?

MARIKA KONINGS: Thanks, Janis. I just wanted to provide a little bit of context as to why we group these together and the status of both of those. I know we're running to the end of the call, so maybe there is one where people can think about it and come up with some good suggestions because, as you may recall, we had some initial conversation, both around purposes and user groups, in the L.A. face-to-face meeting. I think, for user groups, we said, "Let's park that and maybe come back to it once we've gone through accreditation and decide whether or not we still need to define

user groups or whether accreditation in one way solves for that issue." So I think that is one question.

On purposes, as you may recall, we originally had language in here that tracked with, I think, the categories we had identified for the use cases, which we immediately flagged as well that that was something that wasn't developed for that specific goal. I think, in the face-to-face meeting, we discussed if it's worth looking at this from a different perspective and use more of the lawful bases as a distinguishing factor or linking that to the purpose. I think we've maybe gone back to that as well. I think you all know we went through this exercise of having a sheet in where we ask input. It's maybe something we do need to look back on at some point, but I don't think we got a clear answer whether that would be the approach to take here.

One question I think at least I have from my side is, are we actually spinning our wheels here by trying to answer the question on purposes? I think some are confusing this as well with the exercise we did in Phase 1, and we may need to talk about it here differently. Are we really talking here about – I think it's something we've resolved for in some of the other building blocks – that a requester needs to provide a rationale for why he or she thinks or needs access or disclosure of that data? Is that what we're really talking about? If so, I think we could potentially refer here back to the other building block and indicate what kind of information would need to be provided.

I don't know if the group would even be comfortable to say – this may not be something that can be done now, but I think someone alluded to it on the call earlier as well – that, over time, whoever is

running SSAD may see that there are indeed standard rationales that are provided or similar rationales that are provided for why people request the data. That might be something that could then be prepopulated in a kind of form that is filled out so that that could potentially triage requests in an easier way. Again, I don't know if the group is at a stage where we feel we could identify those rationales. Again, I think we may want to move away from purposes here, as I think that's maybe too tied to what we did in Phase 1. As I said, maybe this is something where we've answered the question by referring to the information that needs to be provided. Maybe it can be tied to something that can be reviewed over time to see if there is indeed standardization possible. I think Thomas has spoken about this as well: there are certain scenarios that are repeated over and over again, and, as such, some further automation or standardization can be built in. But it may be something that only occurs over a certain period of time once you have experience with the rationales that are actually being submitted.

So I think that's something we just wanted to flag. I know we're getting to the end of the call. Of course, I'd be very happy to hear what the group thinks about these specific two building blocks and how to move forward with those for inclusion in the initial [inaudible].

JANIS KARKLINS: Thank you, Marika, for this explanation. What would be the reaction to the text that is on the screen? Reaction, comments, of a general nature?

Margie?

MARGIE MILAM: Hi. I did take a look at this. I don't think we would be comfortable with no specificity on the purposes and having it track what GDPR requires under 61 in the different letters. As you guys may recall, in Phase 1 the BC did dissent to the original Phase 1 report. The main reason for that was because there was no specificity on the purposes. So I just want to flag this from the group – we can talk about it on the next call – that this is something that my constituency is particularly interested in. So I'd like to, on our next call, explore whether it's possible to go to the listing of specific purposes in some way, at least the main categories that track what we submitted in our use cases. Thank you.

JANIS KARKLINS: Thank you, Margie. Milton?

MILTON MUELLER: Of course, I don't agree with what Margie just said, but my concern about this language is just language. I'm unclear about certain words or certain phrasing. "The EPDP team recommends that requester must be able to identify at a minimum its function." "Its function" is referring back to requesters. Do want to say "their function" or "the SSAD's function"? I'm just unclear about the language here. It's throwing me off as to what this actually means.

Of course, each request should identify the anticipated lawful basis under which the disclosing entity is expected to request, I

think, the data. But I'm not sure I understand that first part about function and processing and who it's referring to. Maybe Marika can answer that.

JANIS KARKLINS: Thank you. Marika?

MARIKA KONINGS: Thanks, Janis. I'm not sure if I can answer, but just to note, I think this was language that was suggested during the L.A. face-to-face meeting. I think it was Chris who put this forward, so he might be a in a better position to answer that question if he still remembers what the rationale. But I think that first part went also to the notion that it may not be possible to specifically have a list of all the reasons for why the data is requested to be disclosed but that it must be provided. It is something that needs to be included. I think this language also noted that, together with that rationale [that] we should also identify and anticipate a lawful basis, again, to help the inform the controller to make a determination on whether or not that lawful basis applied, whether that rationale – in which category that would fall and do the appropriate evaluation of that.

So I think that's where it originally came from, but I don't know if that answer's Milton's question. But I hope we can then look into this further.

JANIS KARKLINS: Thank you, Marika. Alex?

ALEX DEACON: Hi. I just wanted to say again that the IPC also believes that being more specific with regard to the purposes and the policy is important. I'll note that, assuming again that we're building a system to process and categorize these requests, it'll be important to know what that list is so they ca be properly implemented and turned into assertions or authorization credentials that are backed by a future accreditation authority. Again, I agree with Margie here. I think we can't be vague here. We need to be specific as to what purpose is associated with each request coming in. Thanks.

JANIS KARKLINS: Thank you. We're four minutes before the end of the call. Certainly, we need to revisit this discussion further. But in order to do that, let's listen to Brian first. Brian?

BRIAN KING: Thanks, Janis. I'm just going to give the second half of the IPC position on that. This is where Alex and I play well. He gave the technical reason why the specificity is important, and I'll give you the legal reason. Article 5 of the GDPR requires that type of specificity when the data is collected from the data subject. So that's in the comments on the Google Doc there, too. I just wanted to make that point here. Thanks.

JANIS KARKLINS: Thank you. In order to progress in this conversation, probably we need more input from different groups in the team. I would simply

like to invite them maybe to provide editorial suggestions by Monday, not to be confused with the accreditation part, which would be by Friday. So by Monday. Then we would make a point during the next meeting.

Another point that I would like to make, going to Montreal, is that probably we need to think also to provide input or any other input that members would like to provide. In this respect, I would maybe like to ask Marika to tell us if there is any specific deadline that staff would like to have for any inputs going into Montreal. Marika?

MARIKA KONINGS: Thanks, Janis. Shortly after this meeting, we'll be circulating the proposed agenda for the ICANN 66-related EPDP meetings as we discussed earlier this week. Staff would like to propose and suggest that all input, apart from the deadlines that we've discussed today on specific building blocks, on all other building blocks should be provided by Wednesday, the 30th of October, at 21:00 UTC at the latest. That would allow us to use it as a cut-off date and really then prepare between basically Wednesday and the start of Saturday's meeting to have a very clear overview of what are the specific outstanding issues or concerns in relation to all the building blocks and help us build then approach to each of those. Of course, we understand that that is relatively short to get us to Montreal, but we hope that everyone agrees that we need to try and take the most of our face-to-face time. By having all that input in by Wednesday, I think that will really help us in having a very productive and constructive conversation.

So that is specifically the ask from the staff side. As I said, we'll send out the proposed agenda for ICANN66's [inaudible] meetings, as well as this specific deadline, shortly following this call.

JANIS KARKLINS: Most likely that would include also those new building blocks that we have identified that need to be developed further, like logging and auditing and all the new building blocks. Right, Marika?

MARIKA KONINGS: Yes. Correct. I'll also flag that we'll just create a separate Google Doc for those: policy principles from the zero draft. I think, as you may recall, the original schedule had us starting to look at those as well before getting to Montreal. But we didn't do that. But I think we still may want to have a look at that, so we'll also create a Google Doc for those so people can start providing their comments as well to those.

JANIS KARKLINS: Thank you. Marc Anderson, your hand was up.

MARC ANDERSON: Sorry. I clicked Raise Hand by accident.

JANIS KARKLINS: Okay. Thank you very much. I think at least I have a very good feeling of the outcome of this conversation in terms of

accreditation. Alex, thank you very much for your input that helped us to move in the right direction. I encourage everyone to look once again an provide editorial input on the fresh text that will be circulated immediately after the call by Friday. Then we would come back on Tuesday, aiming at basically concluding the stabilizing accreditation bit before Montreal.

So thank you very much. I wish all you a good rest of the day. This meeting is adjourned. Thank you.

[END OF TRANSCRIPTION]