ICANN Transcription

GNSO Temp Spec gTLD RD EPDP – Phase 2

Thursday 29, August 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 of the call are posted on the wiki page: https://community.icann.org/x/pKajBg

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, good evening, welcome, to the GNSO EPDP phase two team meeting taking place on the 29th of August 2019 at 14:00 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 Janis Karklins, Mark Svancarek and Ashley Heineman. They have formally assigned Steve DelBianco and Laureen Kapin as their alternate for this call and any remaining days of absence.

Alternates not replacing a member are required to rename their lines by adding three Zs to the beginning of their name and in the end, in parentheses, affiliation and their alternate at the end, which means you're 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 functionality such as raising hands, agreeing, or disagreeing.

As a reminder, the alternate assignment must be finalized by way of the Google assignment form. The link is available in all meeting invite e-mails.

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

AMR ELSADR: Thanks, Terri. I did update my GNSO statements of interest and thought I'd probably best declare it here now. I recently signed a fixed term consultancy agreement with CentralNic so I'll be working with them over the next few months.

My work with them is not ICANN- or gTLD policy-related at all, and the NCSG Policy Committee is aware of this. I should have no conflict of interest, and CentralNic are of course aware that I'll not be representing their interests in the GNSO or ICANN at all. So I just thought best to let you all know. Thanks.

TERRI AGNEW: Thank you, Amr. Seeing or hearing no one further, 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. With this, I'll turn it back over to Rafik Dammak. Please begin.

RAFIK DAMMAK: Thanks, Terri, and thanks to everyone for attending today's call for the EPDP team. Starting first with the confirmation of the agenda, as you can see, and what was shared two days ago. It follows the usual plan with regard going through different use cases and also starting with housekeeping.

So we can start with the first substantive agenda item, which is the welcome and housekeeping issue, and the first one will be an update from the legal team. I will ask León to give us an update about the work of the legal committee regarding the question they worked on. León, over to you.

LEÓN SANCHEZ: Thank you very much, Rafik. Good morning, good afternoon, good evening, everyone.

The legal committee went back to the table to continue discussing the legal questions that are now being submitted to the plenary for sign off and hopefully sending them to the legal outside council.

The first batch is comprised by four questions. These questions were circulated yesterday on the mailing list. I note that there have been a couple of comments on this question. I noted Farzaneh's comments, and we will be happy to add the question about the balancing test to our subsequent discussions within the legal team.

If there is no objection as per our procedure, and I believe the chair would be doing this, we'll be submitting this first batch of four questions to outside counsel in order to inform our discussions in our face-to-face meeting in LA.

So at this point, Rafik, there is nothing else to report, and I would of course welcome any comments or questions [inaudible] questions. Thank you.

RAFIK DAMMAK: Okay. Thanks, León, for the update. I see we have [Matt] and then Amr in the queue. [Matt,] please go ahead.

[MATT SERLIN:] Yeah. Thank you. And León, thanks for the update. I just want to thank the members of the legal committee for their work on the questions.

I did have a question. And León, in your update, you sort of touched on it, but my question really was just about the timing, and you mentioned that you want to have them submitted and answered back for discussions in Los Angeles. That really was my question, is, do we think it's realistic to get the questions submitted and the feedback back from outside counsel by the time we're in Los Angeles, which hat this point is just over a week away? Because obviously, I think that will greatly impact the conversations and discussions that we have in the face-to-face, and hopefully – I think all of our goal would be to get the information back so that we can have a more productive session,

but I'm just curious if you've already discussed with them the short time frame and if we think that's realistic. Thank you.

LEÓN SANCHEZ: Thanks, [Matt.] We did give heads up to Bird & Bird on the questions. They know that we will be submitting them any time now, and they replied that they are prepared to provide feedback as soon as possible. Of course, I cannot guarantee this will happen before we meet in LA, but the hope at least is that we will have this information ready so that it will inform our discussions in LA.

So Bird & Bird is aware, and they are willing to provide their feedback as soon as possible.

RAFIK DAMMAK: Okay. Thanks, León, for the response. Amr, please go ahead.

AMR ELSADR: Thanks, Rafik. Thanks, León. I know it's just been a week, but I was wondering if there was an update to the question we discussed last week, the one concerning using 6.1(b) as a legal basis, and the reference it made to the letter to the letter the European Commission sent to the ICANN board during the public comment period [on the] vote for phase one recommendations.

If there aren't, that's understandable. It's only been a week, like I said, but I'm just wondering if there has been any progress on that front. Thank you.

LEÓN SANCHEZ: Thank you very much, Amr. We did discuss the issue in our last call, and a couple of folks from the legal committee volunteered to narrow down the question because as you rightly pointed, it seemed to be too broad and it didn't provide a lot of confirmation as to what we would be expecting from the question.

So a couple of folks from the legal committee will be reverting to us with a suggested updated question, and of course, we will discuss this question with the plenary when it is ready for that. So that is the update we have on that question, Amr.

RAFIK DAMMAK: Okay. Thanks, Amr. Alan, please go ahead. Alan Woods.

ALAN WOODS: Thank you. Just a very quick question. Obviously, I still note my points [in the last] [inaudible] that I raised about [questions and purposes.]

But one thing that did jump out at me, and I just want to raise this for the legal team, specifically with regards to question three, [inaudible] "please provide any guidance for how to perform the balancing test for Article 6.1(f)."

Let's not waste money on that, because if you were to look at the [inaudible] on the city field, there is actually about five pages on the balancing test [especially looking in the] [inaudible]. So just

having a review of [inaudible] make sure that we're not asking them to answer the same question twice. But thank you.

RAFIK DAMMAK: Okay. Thanks. León, can you respond to this?

LEÓN SANCHEZ: Thanks, Rafik. Thanks, Alan. I see your point, Alan. However, I believe that – my sense is that the legal committee has concluded that it is important to ask the question. So if there is no objection, we would be submitting it, of course.

RAFIK DAMMAK: Okay. Thanks, León. Thanks for the update, and thanks all for the question. So I don't see anyone else in the queue, and as we said, in absence of a strong objection, we can send those questions.

Okay. So I see Marc Anderson in the queue now. Marc, please go ahead.

MARC ANDERSON: Thanks, Rafik. I guess I want to drill down on Alan's question a little bit more and maybe put the legal subteam members on the spot a little bit. I understand from Alan that we already got a detailed response and he doesn't believe we're going to get a different answer and that asking this again is a waste of time.

So I guess I want to understand from the legal subteam members, do they believe that there will be a different answer this time and

so it's important to ask the question again to try and get a different answer, or do they believe that the answer we got previously isn't clear or needs more detail?

I guess I'm trying to understand the difference in opinion here, and I think maybe I'd like to get a little more color from the legal subteam members that are advocating for asking this.

LEÓN SANCHEZ: Thanks, Marc. Well, the role of the legal committee is not to advocate for any questions to be asked. It's just to review the questions that emerge from the plenary and to try to craft them so that when we submit it to legal counsel, they are asked in the best possible way so that we can optimize the legal advice that we're getting from outside council.

Now, in terms of this question, we might have indeed received already some advice – or lengthy advice, as Alan has said in the chat – however, the legal committee believes, and that is my feeling, and please, anyone from the legal committee feel free to chime in if I'm not portraying this as accurately as we have discussed.

We have added some considerations that are intended to better frame the question to our outside council. So by submitting this question in its current form, we believe that we might get more useful answers that would inform our discussions in a way.

RAFIK DAMMAK: Thanks, León. Alan Woods.

ALAN WOODS: I just wanted to confirm that I'm not here to give [inaudible] that you didn't do this or did not do that. I'm just saying it is very much a standalone question at the end of a very long question, and it's also, "In the case everything you say before is not actually right, could you give us this?"

So it's not really [inaudible] perhaps could be something that would be considered. This is the whole point about giving it to the plenary so that we can point out these things. We're not looking for an answer specifically now, I'm just raising it with the hopes that perhaps we could save time, especially considering we only have a week before we need to really g I've it to them, or sorry, before we get an answer from them.

So again, I'm not being obtuse here, I'm just saying perhaps this is something that we can shave off.

LEÓN SANCHEZ: Thanks, Alan. It's noted.

RAFIK DAMMAK: Okay. Thanks, León. Okay, we have now Brian I think in the queue, but I guess we should close the queue soon since we still have other items for discussion. But let's hear from him. Yes, Brian, please go ahead.

[BRIAN KING:] Sure. Hi, Rafik. Thanks. I think I can try to address Alan's question and Marc's point. I was part of the legal committee. I didn't work on that specific question, but I think what we were asking for there is some guidance assuming a lot of the facts that were assumed in the kind of lead up to that question.

So I think what the question was intended to do was say, "In this specific case, how should the 6.1(f) test go?" And I understand Alan's point that we do have quite a bit of detail on the types of things that normally go into or that need to go into that 6.1(f) analysis from the other legal advice.

So if that clarifies what I think that part of that question was intended to do, I hope that's helpful. Thanks.

RAFIK DAMMAK: Okay. Thanks, Brian. So I guess we stand here to make a decision. León, do you want to add anything?

LEÓN SANCHEZ: Thanks, Rafik. No, nothing else to add, and thank you everyone for your thoughts, your comments. It has definitely been useful to guide the work of the legal committee and we will continue to work on the remaining questions, and of course, happy to welcome any new questions that arise during our discussions during our calls and our face-to-face meeting in LA. Thank you, everyone.

RAFIK DAMMAK: Okay. Thanks, León. Just to confirm, I think you said that the question suggested by Farzaneh will go to the legal committee for discussion or review.

LEÓN SANCHEZ: That is correct. I have replied to Farzaneh on the mailing list stating that we will be adding a question on the performance of the balancing test. Of course, we don't have the wording for that at this point because it's just been proposed by Farzaneh, but one of the things we will do in our following calls in the legal committee is to try to craft this question. Or if anyone from the EPDP team has a suggestion as to which would be the text that they would like to suggest for the analysis of the legal committee, then we would be happy, of course, to receive it and analyze it in order to revert to the EPDP plenary and have the question submitted to outside counsel.

RAFIK DAMMAK: Okay. Thanks, León. So I guess I heard a comment from many here regarding the question. I don't think we have strong objection, and knowing the timing that we should get response hopefully before LA meeting so that can be used as input, I guess we can move and send the question so the legal counsel know that it's coming and probably we can give a note about – I'm not going to say urgency, but to get a response as soon as possible.

Okay. I guess with that, we can move to the next agenda item, and this is a reminder regarding the question for Göran and the Strawberry team in preparation for the face-to-face meeting. I

would like here to ask Marika if there is any update or – I understand we're still waiting for more questions, but Marika, if you have anything to add, please do so.

MARIKE KONINGS: Thanks, Rafik. No, just to note that I think until now, we've just received a handful of questions. So just to encourage everyone to have a look there. Of course, if there's only a handful, that is perfectly fine and we'll allow – Göran as well as the Strawberry team – to prepare accordingly. But if there are any further questions you would like input on, it would be really helpful if you can add them to the Google doc.

RAFIK DAMMAK: Thanks, Marika. And I also note that there are still some comments in the related thread, so this will be more of a discussion at the leadership team level and to answer as soon as possible.

I see there's Marc Anderson in the queue. Marc, please go ahead.

MARC ANDERSON: Thanks, Rafik. On the subject of the Strawberry team, I want to highlight something Greg said in e-mail just before the call. I think he made a really good point. He pointed out sort of the importance of our session in LA and the timing of it, and the questions we might want to ask are really dependent on the type of update they have to provide for us.

So I think maybe it might be worth us reaching out to them to see if they have any information to provide to us ahead of LA face-to-face. If they have substantive updates since we heard from them in Marrakech, it might be good to understand a little bit ahead of time, and I might ask them different types of questions than if they have no substantive information or no significant changes since Marrakech and for example, have they or have they not met with DPAs since Marrakech?

So it occurs to me, after looking at Greg's e-mail, that there's a real good point in the types of questions and the nature of our interaction with them in LA really is going to be dependent a little bit on how much has changed since Marrakech and what type of information they have to provide to us.

So I'm not sure how to facilitate or bridge that sort of gap in understanding, but I just sort of wanted to echo what Greg has put in the e-mail before the call.

RAFIK DAMMAK: Thanks, Marc. The Strawberry team is aware that we want to engage with them and we are preparing the questions. I believe we can coordinate with them and prepare for the face-to-face meeting, and we can ask them for a written update prior to the meeting if it's helpful, and I think that'd give us a better understanding of what's going on, and if we can, we want to go further in some areas.

So I guess we can follow up with that to ensure that we have real dialog with them and getting useful updates. So we can take this

as an action item for the leadership team if there is no objection, and to prepare for fruitful dialog for the LA meeting.

Any comment or question on this issue or topic? Okay. Anyway, I think also we'll discuss with Janis and probably we can answer also into the thread just to clarify in any case.

Okay, if there is no further question or comment, we can move to the main part of our meeting, and starting with the first use case, [that's the second or final] reading. This is a use case from SSAC, and we should get an update regarding the changes or the response to the input that was received.

I think we'll ask here Ben – okay, Ben, you're in the queue already – to make a presentation and to respond to the comments. Ben, over to you.

BEN BUTLER: Thanks, Rafik. Thank you to everyone for reading through and providing comments on this. There weren't a lot of substantive changes. We especially want to thank Registrar Stakeholder Group for their comments as they were the most extensive, and frankly, we really agreed with pretty much every suggestion that was made there. So hopefully we can just move through this in a timely fashion and not have to take too much more time on this.

Just as a clarification based on the comment for section A, this is absolutely intended for network operators, either the one being attacked or the operator of the network that's doing the attack and not for third parties, unless they're the designated operational

security teams for either of the first two parties. This isn't intended to be for research purposes or that sort of thing.

We agree that the changes in section B, “maybe” is fine rather than “is required.” In section C, getting rid of the admin, that was an oversight, should not have been included in the first place anyway. So we’re just talking about registrant and/or technical contact.

Section D, again, this isn't a hill we want to die on. We agree that 6.1(f) is the appropriate basis in 99.99% of the cases, but had incldued 6.1(d) just to highlight that there are situations where critical infrastructure such as hospitals, power grids and so forth have been taken down by botnets, and in those cases, that critical infrastructure provider might be able to request disclosure under 6.1(d) because the health and safety of other natural persons may be at risk.

But if it is the case that people absolutely don’t want it to be in this use case, that's fine. Frankly, whether or not we include it in this use case, eventually somebody is going to make that request of data controller and cite 6.1(d) or 6.1(e) as the basis. It ‘s not that critical whether we have it in or not. So by all means, if people want to voice strong opinions on that, speak now or forever hold your peace, I guess.

Section E is just highlighting that Recital 49 specifically takes into account this situation and it’s why this is one of the core purposes that was kept in mind for this type of situation.

In section F, there was a suggested add to the safeguards applicable to the requestor. We agree with that addition and appreciate the Registrar Stakeholder Group putting it forward.

Same thing in section H with the suggested additional safeguard applicable to the data subject, must have their data protected in line with relevant data protection legislation.

There was also a comment on the safeguard we originally had in H. This was something that was included for the sake of informing our discussion of how these types of operational security concerns are typically dealt with, and we're saying that the owner or the registered name holder of the domain name that's being used in an attack may designate a third party to handle the back and forth with the network operator that is being attacked.

That doesn't, as Sarah pointed out, the envisioned scenario isn't that the data controller may disclose the identity of that third party, but rather that the registered name holder might hand it off to their technical resource team or designated agent.

So if we're limiting this use case to the possibility that the data controller, the registry or registrar in this case, may need to disclose, we can certainly remove that. it was just, again, to highlight that most of the time in these situations, the name on the registration data is likely not to be the person handling the back-and-forth to resolve the ongoing security threat.

On section I, safeguards for the access disclosure system, we're fine with the suggested edit to remove the "high-volume automated" and replace with "unjustified." The high-volume

automated is merely to say that the data controller or whoever's operating the SSAD in this scenario will obviously still need to have the ability to protect against essentially a DDoS of this resource by too many requests from the same party, which is mostly covered in the idea of rate limiting and so forth.

It kind of also does touch on section J, accreditation. Just noting again there is no current accreditation body that would adequately include the operational security community. As this process moves forward globally, I suspect somebody will come forward and try to create that sort of infrastructure, and if they do, awesome, but in the meantime, there is no way to satisfactorily accredit in this situation.

The other substantive change were some additional information required in section L. Totally agree with this. We had always envisioned that the person requesting the data would have to be able to produce log files or packet captures so that they can show that the domain actually is involved in the attack and therefore that may justify the disclosure of the data so that contact can be made.

I believe that is actually the last of the substantive comments. If anybody would like to discuss any of what I just breezed through in more detail, let's have the conversation.

RAFIK DAMMAK: Thanks, Ben. I see that Milton is in the queue. Milton, go ahead.

MILTON MUELLER: Yes. I don't want to quibble with you about legal basis, Ben. I agree that based on the direction we're going, the legal basis will essentially be declared by the person making the request, and if somebody thinks that it is a 6.1(d) rather than (f), they'll be free to do that and it'll be up to the responding party to decide whether that's a valid basis.

What I'm concerned about here is – if we can scroll back up to the bit about high-speed or high-volume automated, I don't understand why that was deleted, and your explanation for why it was deleted did not make any sense to me.

So to say something is an unjustified query is a very vague term and kind of normative whereas high-volume and automated is very specific in terms of it actually being an effective DDoS of the system.

So why would you delete high-volume automated, and who asked you to delete it?

BEN BUTLER: The suggestion to replace high-volume automated with unjustified came from Registrar Stakeholder Group. In reading this over again, and just as a potential way of satisfying both, instead of deleting high-volume automated, we could say high-volume automated or unjustified queries, because realistically, this SSAD operator will need to guard against possible overutilization of the system by high-volume queries as well as potentially in some way prevent people who are consistently making unjustified requests from wasting everybody else's time.

MILTON MUELLER: That would be good if you could include them both. We will have to discuss about that. I had another comment. It's going to be something we're going to have to discuss in greater detail later, but you talk about accreditation and about the absence of an entity that can tell the entire world who is a security researcher, and I think we both know, we're familiar enough with the cybersecurity environment to know what a tall order that is, to put it mildly.

So I'm just sending out a flag here that this whole notion of accreditation occurring through distinct external user groups is a bad model, and partly for the practical reasons that you've intimated here, that no such things exist, and you're effectively calling for the formation of completely new global institutions that have legitimacy and credibility across a group of stakeholders that is vast and not well defined.

But it also has problems simply in terms of the conflict of interest inherent in making an accredited – somebody enforcing accreditation or removing accreditation from a member of its own stakeholder group is just not a viable model.

So I don't think we should get tripped up on that at this point, but all of the use cases need to have and must develop going forward a coherent notion of who does accreditation, where it comes from, and the idea of the separate stakeholder groups doing it is not viable. We should recognize that now and start planning accordingly. Thank you.

BEN BUTLER: Thanks, Milton. Appreciate it.

RAFIK DAMMAK: Thanks, Milton. Thanks, Ben. Chris?

CHRIS LEWIS-EVANS: Thanks, Rafik. Ben, unfortunately I'm going to go back to B. I'd really just echo what Alan Woods I think has put in the chat. [D is] interested in the lawful basis of the disclosing entity, not the actual requestor. And I still have a hard time with D, full stop, but agree in that .1% or something chance that the requestor may be relying on a 6.1(d) basis, but I still can't see how a disclosing entity can rely on 6.1(d), because their processing activity for the disclosure of that isn't necessary to save someone's life.

So while I agree 6.1(d) for the requestor making a request, the disclosing entity, I just really don't get at all. And I think that's what Alan was saying in the chat as well. Thank you.

BEN BUTLER: Thanks. I appreciate that clarification and distinction. Yeah, we were including D for the sake of the requestor as far as a legal basis, not the disclosing entity. So we can remove that.

RAFIK DAMMAK: Okay. Stephanie, please go ahead. Stephanie, if you're speaking, we're not hearing you. Okay. I guess Stephanie has some mic

issue. Maybe Terri, can you help her and check what the issue? In the meantime, we'll go to Marc and then we'll circle back with Stephanie when she is able to speak. Marc.

MARC ANDERSON: Thanks, Rafik. I'm looking at chat. Both Brian and Alex have mentioned that the system would need to be able to handle high volume, or I guess Brian's saying that high volume might not be abuse of the system and Alex is saying that the system will need to be able to handle very high volumes of queries.

I just want to drill down, I want to understand this a little bit more, understand if that is a correct assumption, if our sort of collective understanding of this SSAC use case is that this use case will require high volumes of automated requests for nonpublic registration data, maybe this is something to throw back to Ben. Is that how this use case typically works? Does this typically involve high volume of automated requests for nonpublic registration data?

So I just want to make sure I have a clear understanding of that and that we all have the same understanding of what's required for this particular use case. Thanks.

BEN BUTLER: Yeah, I'm happy to elaborate on that. If we just think about the system formerly known as WHOIS, certainly not saying that the same personal data would be available, but the way it has – the problem that operators of WHOIS servers have typically had to

deal with is high volume, certainly something they have to be able to accommodate within reason.

Where the problem sets in and the protection that we want to cover with the language in this use case is, let's say requesting person asks for disclosure of data relating to domain name X and they do so once every couple of minutes, that's no problem. If they ask for the same data on the same domain 47 times a second, that's a problem, and these are the types of things that were absolutely happening.

We can envision use cases where the same entity might need to make a request for hundreds or potentially thousands of different domain names that are all involved in the same sort of situation, like say a botnet that has a large amount of compromised domains. That would be high volume, not necessarily repetitive, and something that would need to be accommodated.

So it's always somewhat of a fine line to balance a system that's highly available, but it is certainly possible to identify aberrant behaviors where someone's making too many of the exact same requests within a short amount of time that can actually g et in the way of other legitimate requests getting through. Does that explanation help any?

MARC ANDERSON: Thanks, Ben. Yeah, I thought that was helpful. Yeah, I think that's good color, and certainly for this particular use case, when a network is undergoing an attack, an attack is ongoing, you're trying to mitigate an ongoing attack, obviously this is a case where

you're looking for data quickly. So I think we all know and appreciate that.

And I guess as I was hearing your explanation, I was thinking to myself, is there a way to incorporate some of that into the use case? And maybe I'll just throw that as a challenge back to you. I think that's good information that enhances the use case, and if there's a way you could incorporate that, I think that would be helpful.

BEN BUTLER: Yeah, I can tighten up that language.

RAFIK DAMMAK: Okay. Thanks, Ben, and thanks, Marc. While I see we have now two Stephanie in the queue, we will allow only one to speak. Stephanie, can you speak now?

STEPHANIE PERRIN: I certainly hope I can, Rafik. Can you hear me now?

RAFIK DAMMAK: We can hear you, yes. Please go ahead.

STEPHANIE PERRIN: I do have two me's up there. I can't get the iMac to do the right thing in terms of sound, sadly.

I wanted to support what Milton was saying, with perhaps a bit of nuance. I do think it's kind of inappropriate for me to be attempting to explain to SSAC the difference between accreditation and authentication and authorization, but I do think we need to disambiguate these things.

Organizations will be coming forward, I'm sure, professing to not only accredit and recognize entities but to authorize them, and I think that that is quite a problem. At least if I were a registrar or a registry, I would not be accepting a third party's authorization to get the data.

But I think it is entirely possible that we could have a number of entities coming forward to accredit the identity of so-called cyber researchers and botnet fighters. But that doesn't mean that they would get automated access to the data.

So I just wanted to make that point. And please correct me if I'm wrong here.

BEN BUTLER: No, you're not wrong at all and I totally understand the difference between accreditation, authentication and validation. We were not supposing a free rein and automated access just because somebody is a member of a certain group.

We've hashed that out in other use cases, so I don't think we need to relitigate it. Just clarifying, that is not at all what we're anticipating.

STEPHANIE PERRIN: Yeah, so in this case I do agree with Alan's comment in the chat that accreditation might be quite useful as long as we're clear about how limited it is. Thanks.

BEN BUTLER: Yeah.

RAFIK DAMMAK: Okay. Thanks, Stephanie. Margie?

MARGIE MILAM: Hi. I apologize, I'm having really bad Internet issues today, so I may only be on the call for the rest of the call as opposed to on Internet. I just wanted to express my disagreement with what Stephanie and Milton have been saying.

I do think there is a place for accreditation. I think there need to be obviously reasonable parameters regarding accreditation, but accrediting security practitioners is very much something that can be done, can be done by people in the industry, so long as we set the appropriate framework for what needs to happen when there's accreditation and what kind of safeguards and protections need to be in place.

So I think that that's probably something we need to have a very fulsome discussion about in Los Angeles, but certainly from the BC perspective, we believe that accreditation for security practitioners is reasonable and possible, provided that there's a framework in place and protections and all that.

And if you look at the legal questions that were posed, some of the assumptions that are in the legal questions talk about some of the safeguards that we've had in mind.

So I just wanted to share that and indicate that I think that's something that we need further discussion on in Los Angeles.

RAFIK DAMMAK: Okay. Thanks, Margie. Milton?

MILTON MUELLER: Yes. And I apologize for the Georgia Tech whistle that you all apparently heard right outside my window. A bit of the industrial era legacy of Georgia Tech. But that being said, this issue of accreditation, I'm really surprised, because I think typically, the people who want more liberal access to WHOIS data seem to be arguing for some kind of a sectoral-based accreditation process.

I think people who ask for this, particularly in the context of cybersecurity investigators, clearly have no understanding of the field and the way it works. So I could be a cybersecurity investigator. If something happens to me or my department and I want to investigate it, anybody who works for my organization who has an IT infrastructure could be doing this kind of an investigation.

What I'm saying is you don't have to go to some kind of a global bureaucracy to say, "Please let me investigate." I'm saying you have a right to make an investigation inquiry if there's a sufficient legal basis for it, regardless of who you are and who recognizes

you. And if you're going to set up gatekeepers who tell people they cannot actually even make a query or a request, I'm really surprised that anybody would be advocating that.

What makes it even weirder in my opinion is that you're saying, “Okay, we’re going to accredit people.” That doesn’t guarantee them anything. It doesn’t mean that they actually get the data they're requesting. So tell me, what is the actual function of this accreditation process which is going to involve a massive bureaucracy that can recognize people from 200 different countries in various millions of organizations? What exactly do you expect to come out of this process? it really is a puzzle to me.

Now clearly, we don’t need to get too wrapped around this axle when we are talking about this particular use case, but the reason we brought it up now is when you talk about cybersecurity investigations, the field is not that formalized, and anybody can be a victim of a cybersecurity breach and anybody, as far as I'm concerned, should be able to make a request.

So why are we even talking about some kind of a professional, sectoral-level accreditation in this case? I just don’t get it.

BEN BUTLER: Just to hopefully try and keep us from getting too wrapped around this, yeah, there is a difference between this use case and, say, the other SSAC-presented use cases or a lot of the other security “researchers” or investigator use cases.

In this particular situation, our stance is that accreditation could be useful in some of these situations. It’s not something that would be

required in every one of these situations. Certainly, like you said, any network could be attacked, any registered name holder and their domain name could be used as an attacking party. But potentially in the case of, say, large network operators that do this on behalf of other parties. There could be a situation where the large parties that handle this on behalf of other people might have some sort of body that could accredit, that might help lead to some high levels of automation.

And again, automation does not mean free and open access for large trusted, known network operators. It doesn't close the door on small operators or one-off requests or anything like that. We didn't include accreditation as a hill we want to die on, this is just something that maybe down the lien could be used to help smooth out a couple of extra speedbumps in this process.

RAFIK DAMMAK: Okay. Thanks, Ben. I see a queue forming here, so we have James and Alex and Stephanie. So let's hear from then, and then if you want to respond or comment.

JAMES BLADEL: Thanks, Rafik. I can see we're spending a lot of time on this issue of accreditation, and I think the registrar comment was that having some sort of accreditation framework or a third-party entity would be useful. I think Milton has some valid points, but I think the alternative to not having any accreditation from an operational perspective means that we have to investigate the investigators

and make sure that everyone is who they say they are and this legitimately belongs under this particular use case.

I think that we should push off of accreditation or credentialing frameworks where they exist. If one doesn't exist, I'm not ready to say we should create it specifically for this purpose. But not having something like that to look at either means we have to open the doors to anyone who claims to be a security investigator in this case or checking them out individually, and that could take a lot of time and resources and also in the event of some sort of an urgency, of an attack, it could also delay any sort of remediation of that.

So I think accreditation is something that we need to consider carefully, but I would be opposed to throwing it off the table entirely. Thanks.

RAFIK DAMMAK: Okay. Thanks, James. Alex?

ALEX DEACON: Yes. Thanks. Hi, everyone. I agree with James. I also agree with Milton in the comment he made earlier that anyone should be able to request access to this data or request that data be disclosed. The IPC does not want a world where only accredited persons can request disclosure of this RDS data.

And as James says, we believe accreditation is an important aspect of what we're discussing, and our charter kind of explicitly

asks us to evaluate how credentialing can happen and how those credentials can be used.

An accreditation issued by an approved accreditor based on some policy – which I suppose we'll have to set and discuss at some point – can be very helpful and I believe is key to any future implementation of the so-called SSID. Thanks.

RAFIK DAMMAK: Okay. Thanks, Alex. Stephanie.

STEPHANIE PERRIN: Thanks very much. I just wanted to wrap myself around this axle again, because as Alex just said, credentialing, I think, is vital. If you're going to t registry to automate some of this response – and you do want to automate some of the responses as much as you can when you're talking about large-scale, fast attacks, but it would be useful for members, before we have this fulsome discussion that Margie was proposing that we have in Los Angeles, it'd be useful to look over some of the work that the data commissioners have done over the years when they were consulted on the subject of phishing attacks and anti-spam, because many jurisdictions have brought in spam laws and basically holding tanks for suspect data, and that's a huge privacy issue, and the data commissioners have offered their views on what is required.

I would note that that doesn't mean that the data commissioners necessarily got their way and that the existing holding tanks or

repositories of suspect e-mails are being properly managed or audited or any of the things that we're looking for.

But it'll clarify a lot of the issues here and disambiguate some of them. We're trying for something that is actually compliant with data protection law here so we can learn from this and improve on it.

And I think that we're going to have to spend quite a bit of time on this topic, but it's important. Thanks.

RAFIK DAMMAK: Okay. Thanks, Stephanie. Before I speak, Ben, do you want to comment or respond?

BEN BUTLER: No, I'm just taking in what everybody's saying. I agree. I think we've gotten a little bit off topic as far as going through this use case. The wider discussion about accreditation versus authentication and what everybody means is something I think we probably need to have at a wider level. But for the sake of this use case, I don't think it changes any of the substantive information in this use case.

RAFIK DAMMAK: Okay. Thanks, Ben. I guess we can close the queue here. Okay. Also, checking that discussion in the Zoom chat, and I think we are moving in the direction that it's better to discuss this topic of

accreditation and probably at the face-to-face meeting, and allocate enough time for that.

So if you recall – also, I think everyone is checking the zero draft – we have placeholder on those matters. So it probably will be useful if everyone maybe starts to – or some start to think about the proposal that can be helpful to feed the discussion in LA regarding this [inaudible] block.

I guess this is one action, but also, I think Ben, as you already responded, you took note of several comments and you will make the changes to the use case, if I'm understanding correctly. So I guess we are really close here to kind of finalize this one.

BEN BUTLER: Yeah, I'll make the changes that we discussed and agreed on and let staff know when it's done.

RAFIK DAMMAK: Okay. Thanks, Ben. Just checking if there is any further comment on the matter, but I guess basically, we went through the substantive or substantial changes.

Okay, so I guess with that, we are already on the last stage for this use case, and we can move to the next one. Can you share the next use case, please?

TERRI AGNEW: Marika, it appears you're sharing your entire screen, so your Skype and everything. There you go.

RAFIK DAMMAK: Yeah. Thanks, Terri. I guess if I'm not mistaken, the next use case is from ALAC, and Alan will go through it and give us update about changes and so on. Alan?

ALAN GREENBERG: Thank you very much. Actually, I'm going to make a few general comments based on the e-mail discussions and then turn it over to Hadia to go over the specifics.

There's been a lot of traffic on the list, and I wanted to try to summarize a few points. One of the issues that's been discussed a lot is whether consumer confidence is within ICANN's mission.

I claim that it doesn't matter. This is not an ICANN purpose, this is a 6.1(f) issue where we're simply providing access if the contracted party can make a balancing cased that says it's justified.

So whether it is in ICANN's mission or not is irrelevant. Law enforcement is not in ICANN's mission, but we might accept queries from law enforcement in another use case. So I don't believe the ICANN mission is an issue at all.

The second one we've talked about is content, and there's been a lot of discussion about what's on the website or something. Whether there's a website or not and whether the website content looks commercial is an issue that may have triggered the request by the user and it's an issue that the contracted party may consider when deciding whether to grant access or not, but it's not

an ICANN issue. It's a matter of how the contracted party choose to evaluate requests.

They may instead look at their contact information that they have on their customer and ignore completely what is in an e-mail on a website if such exists. It's a business practice of the contracted party, and it's not something that we're talking about. And certainly, we're not trying to decide that specific content implies access or implies disclosure. So I don't think content is an issue here at all. It may be something the contracted party considers, but that's their business practice, not an ICANN policy.

The third thing that's been discussed is whether this is a valid use case and whether we should reject it. As Amr pointed out in one of his recent e-mails here, one of his e-mails yesterday, regardless of what the EPDP decides, any user can submit a request. The contracted party is obliged to do a balancing test and see whether to grant that request.

So whether we call it a use case or not, it is a use case, it is something that may happen in reality. Making it a use case does not guarantee any level of disclosure, it doesn't presume that there will be any level of automation, full or partial. It simply says this is a case that may happen, and that's it.

We're not likely to make any rules about this one because it is very specific to the details that are provided by the requestor. It is a classic one where, to, I guess I'm quoting Alan Woods, where the details matter. This is something that is going to have to be evaluated based on the details presented, and we're not

presuming anything automated or anything implied by the fact that it is a use case.

So I really don't understand the concept of rejecting the use case when it's quite clear that it may happen regardless of what we decide on it. I'm rather surprised we've spent so much time on this. I would have thought it's one of these that is not likely to influence what policy we set at all, because we're not really providing guidance on the balance test. That's up to the contracted party.

So we can keep on talking about it a lot, but I'm not quite sure what we gain out of that. Thank you. And I'll turn it over to Hadia now. I see there's a question though.

RAFIK DAMMAK: Thanks, Alan. Maybe we can go first with the question, then to Hadia to continue the presentation. Okay, let's get to question first and then we go to Hadia and we continue with the queue later. So we have Marc and James. Marc, please go ahead.

MARC ANDERSON: Thanks, Rafik. Reflecting on what Alan said, I also think we've spent an undue amount of time on this use case, and based on what Alan said, if I understand Alan's statement correctly, he does not believe that this particular use case requires or is even intended to result in policy recommendations from this group, this EPDP phase two group.

So given that, and the amount of time we've already spent on this particular use case, is it a great use of our time to spend more time on it? I think at this point, we understand the use case. Whether we agree with it or not is obviously another question, but I think we understand the use case.

I hear Alan saying that he doesn't believe that this specific use case results in policy. So can we move on from this one and not spend more time on this use case?

RAFIK DAMMAK: Okay. Thanks, Marc. James?

JAMES BLADEL: Hi. Thanks. And just to be clear, I don't know that we were saying that we should reject this use case. I think what we were saying was that a lot of the support or rationales provided probably belong in other use cases, for example if there's some sort of abuse or fraud or phishing or networking attack or criminal activity, all that stuff falls under other categories.

When you tease all of that out of this use case, there's nothing left to approve, there's nothing left to reject. It's just kind of this empty thing that you've already kind of indicated is not related to content, is not really likely to result in any kind of policy.

So I don't think it's a question of rejecting this use case. I think what we're saying is if you take it and look at its component parts of each of the rationale, they belong in other places, and whatever

is left is really not worth our time. I think that kind of comports with what Marc Anderson just said.

I think that's why landing on this one is that there's really nothing left to talk about.

RAFIK DAMMAK: Okay. Thank you. I think Alan wants to respond here. Alan, please go ahead.

ALAN GREENBERG: Yeah, just a quick one. James, I don't think you or the contracted parties said rejected. Other people did, and I was reacting to that. Thank you.

RAFIK DAMMAK: Okay. Thanks. Any further comment here? Okay, so I understand Hadia will continue going through this use case.

HADIA ELMINIAWI: Okay. Thank you, Rafik, and thanks to James and Marc for their comments as well. As Alan said, there are no special policy recommendations associated with this use case. [inaudible] the use case, and maybe the only thing if we can scroll a little bit down [to the safeguards applicable to the entity disclosing the nonpublic –]

RAFIK DAMMAK: Hadia, sorry, we are losing your audio. It's going in and out.

HADIA ELMINIAWI: Could you hear me better now?

RAFIK DAMMAK: Yes. Much better.

HADIA ELMINIAWI: Okay. I would just like to scroll down to the safeguards applicable to the entity disclosing the nonpublic registration data. If we could do that, to the G.

Okay, so one of the safeguards that I've added – and that's not a policy recommendation, but that's like what a registry or registrar that expects such a use case should do. It should be in their privacy notice.

So definitely all controllers and processors would have a privacy notice, and the privacy notice would include the intended purposes for processing the data and the lawful basis.

And if they think that this is something that could happen, then it should also be in their privacy notice. And then I would go to the automation part and would like to say about this part, we've previously said that it is desirable but highly unlikely. I would change that to no, we do not think that it should be automated. However, if the registry or registrar wants to automate it, then it's up to them.

So I would [inaudible] to not be automated. And that's about it. Thank you. And again, we changed the use case. Maybe it was not clear in the beginning to some. It's about the domain names and not specially about the websites, definitely. Thank you.

RAFIK DAMMAK: Okay. Hadia, are you done?

HADIA ELMINIAWI: Yes, I'm done and open to any questions.

RAFIK DAMMAK: Okay. Thank you. Let's see if th4ere is any comment here. Okay, I don't see anyone in the queue. Okay, so I guess we have taken into account what was said in the beginning, but I see that we have Steve in the queue. Steve, please go ahead.

[STEVE DELBIANCO:] Thanks, Rafik. As I said in the chat earlier, the uniqueness of the use case can be understood in a phishing attack where the domain used in the phishing e-mail, the domain name does not resolve to a website. And I asked the question, isn't WHOIS about the only place I can go to learn who the registrant is for the domain name that was registered the address that sent me the phishing e-mail?

And if so, it still doesn't say this is a uniquely covered use case. It's in fact another use case covers it. And I do understand that if law enforcement authorities are investigating fraud, then that

would be covered by the use case we're going to deal with next. I get that.

But individual users, particularly within a company where they're being spear phished with very convincing e-mails long before law enforcement is involved, those individuals may use WHOIS to learn the registration behind that domain name. That argues for keeping the use case alive as an example of a factual description of something that happens that involves the disclosure of nonpublic WHOIS data.

It does not necessarily mean that we'll develop policy for it, as Alan has said. A use case has two roles. It describes a situation and it may normatively recommend what we should do about it. And if we don't normatively create policy, this will fall into the notion of making disclosure requests and counting on a 6.1(f) manual balance test to generate a response. Thank you, Rafik.

RAFIK DAMMAK: Okay. Thanks, Steve. Hadia, I think you want to comment here. Please go ahead.

HADIA ELMINIAWI: Yeah, I just want to strongly agree with Steve. No other actual use cases cover the part he just mentioned. And I see Amr saying in the chat that this could be covered by law enforcement, and definitely not. It cannot. Thank you.

RAFIK DAMMAK: Okay. So checking if there is any further comment or question. I guess the use case played its role here as to initiating some discussion and input, so we are taking into account all the concerns that were expressed on the mailing list and also today and the call. That will help us at the end for the next deliberation.

In the end, we are documenting those concerns, and taking note of them. And I'm asking here if you have any further element that you want to add and that we should document. I think it's a good time to do so.

I'm also trying to catch up with the Zoom chat. Okay. So I guess there is no kind of – as we have an agreement here regarding this use case, I would say that I think it's played its role for having this discussion, and clarifying the understanding from each side. We'll document, and that'll be in the annex or reference to the initial report.

But I guess here, we are reaching, I think, a situation where we need to move on. We are taking into account both sides, and that will be referenced. So unless there is suggestion otherwise, I think we should probably move to the next agenda item since we have only 40 minutes left, and try to go through a use case. [inaudible] the first opportunity to go through that use case to have more deep discussion on that.

Okay. I see no objection, so let's move to the next agenda item. This one I think was suggested by the GAC, and I believe Chris will present this use case. Chris, over to you.

CHRIS LEWIS-EVANS: Thank you very much, Rafik. Just very quickly before we go into this one, just wanted to cover our reason for having these two very similar use cases.

I think for ourselves, the purpose of this second one is to help us look at how different jurisdiction affects some of the policy recommendations we might need to make, the transfer of data and how that may affect the legal basis.

So that's our thought process when I was creating these two cases, so they are very similar. Hopefully we won't have too much to go through, but yeah, that's the reasoning behind these two cases.

Also, I'd like to add on this that LEA one, we obviously had some feedback from the registry group and from NCSG. I have updated that form and those updates are reflected on this. I haven't shared the first one just to stop any confusion between LEA 1 and LEA 2 at this point. So after the call, I'll share the updated LEA 1 as well.

So overarching purpose, there's a slight change from the one you've previously seen, and off the back of NCSG's comments, I've [tidied it] down a little bit. The use case, and the difference here between LEA 1 and LEA 2 is that investigating body and the data controller are in the same country and in the same jurisdiction. Realistically, that's the difference here.

Why the nonpublic data is necessary is the same wording, just slightly restructured to make more sense. If we scroll down to the data elements, that is the same as LEA 1.

Section D, so the lawful basis for this disclosure by the disclosing entity. Realistically, you have two reasons here. 6.1(c), so if a court order or other jurisdictional legal process – because obviously, every country may have different reasons that they can basically force a disclosing entity to disclose data, and that will be covered under 6.1(c). Otherwise, it would be 6.1(f).

The supporting info to determine the lawful basis for the actual requestor. In this case, because they're in the same jurisdiction, GDPR has a cutout for competent authorities investigating and prosecuting crime, and that's under Article 2.2(d). Obviously, there still needs to be a legal basis for them to do that, but that would be their national legal basis under which they are carrying out the investigation or prevention of crime in this use case. So that covers that.

Down to F which is the start of the safeguard sections. I've made quite a big change to the safeguards here. The one I shall send out later is a redline so you can see the changes there, but really, I've tried to firm up some of the language, make it more encompassing and add a couple of extra protections as well for the data subject and how the personal data is collected and processed.

I won't go through all of those at the moment. There is quite a few of them. I have done a fair amount of work on those, so it would be good to get some feedback from everyone once this is shared properly.

Going to G, again, this is the safeguards applicable to disclosing entity. Again, I've added a couple more from what was requested

from the registry input, and then there's a note there. There was one comment around how the rights to object [inaudible] would work from the registries.

We've been discussing that within the small GAC group, and hopefully we should have some language for that shortly. So that's just a little bit of a placeholder there that we will propose some language for that very shortly.

Section H, and I, are the further safeguards. Again, pretty much the same as last time but a couple of little additions. And accreditation, made a change here, again based on the [registry group,] and obviously haven't had a look at the SSAC one.

At the moment, I think we're in the same place. I think if we look at every single country and how they would do accreditation, do we have one accreditation body for every single country? Do we do it on a per country basis?

Either way, realistically that doesn't exist for every single governmental agency that can make these sorts of requests, so that is certainly something that would need to be looked at and no doubt will be discussion of the GAC of how that is achievable for that just there. And then the [expected] timings and everything else going forward is the same as LEA1.

[inaudible]. I'll be happy to answer any questions. Thank you.

RAFIK DAMMAK: Okay. Thanks, Chris, for the presentation, and as it was said in the chat, staff will put the document in a Google doc to make it easier and convenient to get input and comments.

Let's see the queue. We don't have anyone in the queue. I understand that maybe it was shared a little bit late or prior to the call so not everyone had the opportunity to review, but I think it's still a good opportunity maybe to ask some initial question.

I see that Marc will ask the first question. Marc. Please go ahead.

MARC ANDERSON: Thanks, Rafik. Chris, a question for you on your general purpose for this use case. When I first looked at this use case, I assumed this was a law enforcement use case for same jurisdiction. I guess my quick read I assumed that was the case, but then your explanation and looking at the lawful basis suggests that my initial understanding was incorrect and that really, you're looking at this use case to sort of tease out some of the challenges that law enforcement deal with when requesting access to data, both in jurisdiction and outside of jurisdiction.

So I guess I'm looking for you to maybe confirm my understanding – or my revised understanding, I should say – and maybe if you could expand on this a little bit. So I do think the cross-jurisdictional challenges with issues with law enforcement are one of the biggest challenges that we have to deal with as a working group. So maybe I can ask you to confirm my understanding and expand on that a little bit.

CHRIS LEWIS-EVANS: This use case, Marc, was just for a single jurisdiction, but then how we look at the differences between this one and the first one should help us understand some of those challenges between how we deal with different jurisdictional bases was my idea. Does that answer your question?

MARC ANDERSON: Sort of. I guess that was my initial understanding, is the previous LEA use case was more focused on outside of jurisdiction requests whereas this one was focused on same jurisdiction requests. But I guess I got a little confused looking at lawful bases where you include 6.1(c) and 6.1(f), which I would think 6.1(f) would be more applicable to cross-jurisdictional, not same jurisdiction. Is that by design? Or what's your thought process on that one?

CHRIS LEWIS-EVANS: Yeah. Thanks. Sorry, I understand now, I think. So the reason behind the two there is under different countries, we have different processes that we can follow to get access to data. In certain countries, you can't ask a commercial entity for data without going through some jurisdictional process so they would be tied to 6.1(c), but in others, such as the UK, you can ask and follow a process that doesn't necessarily compel them.

So you haven't undergone that process and therefore there wouldn't be a 6.1(c) on the disclosing entity. And if that was the case, then that would fall in the 6.1(f). So to me, that was the reason for having them both there on this case.

MARC ANDERSON: Okay. I got you. Thanks. Yeah, that's very helpful.

RAFIK DAMMAK: Okay. Thanks, Marc. I don't see anyone else in the queue. Okay, thanks again, Chris, for the presentation. We will follow our usual approach here. The staff will share the Google doc and we expect comments to be submitted by Friday, and Chris will come back with an updated version by next Tuesday so we can continue the work on this use case.

Okay. If no more comment or question, I guess we will move to the last part of our meeting and the last agenda item. Before checking if there is Any Other Business, otherwise we will [run up and confirm] for the next EPDP team meeting if there is no Any Other Business.

As a reminder, we will have an extraordinary meeting. It will be in a few hours, in fact, and that will be opportunity to go through the zero draft and getting initial feedback. I hope that everyone had a chance to review it. We are expecting comments and input on that zero draft prepared by staff.

Also, we'll have our next meeting as usual next week Thursday. That will be the meeting just prior to the face-to-face meeting in LA.

Okay, so let's confirm the action items and then we'll move to Caitlin to give us a quick review of the action items for today. Caitlin, one sec. I see that Amr raised his hand. Let's go to him

first and then we come back to the action items. Sorry for that. Yes, Amr.

AMR ELSADR: Thanks, Rafik, and apologies, Caitlin, for the interruption. Would you mind just quickly going over what the plans are for tonight's call? Speaking for myself, I won't make it and I won't be able to make it to the LA face-to-face either, so I'm wondering if there will be an opportunity between tonight and the face-to-face for some of us to submit comments on the zero draft or not. I'm just trying to get a better feel for what the process to deal with it might look like. So if you could highlight that quickly now, I'd really appreciate it. Thank you.

RAFIK DAMMAK: Okay. Thanks, Amr. I think Marika can respond to that and give more details about the plan for today's call. Marika, please go ahead.

MARIKA KONINGS: Thanks, Rafik. We have indeed scheduled this additional call to allow for some separate time to go over the zero draft. I think we'll just start by explaining what is in the document, and as well pointing out where current gaps still exist. And I think at least from an input perspective, we're hoping to hear from all of you how to best make use of this document in preparing for and developing the agenda for the face-to-face meeting.

I think as we outlined as well in the original proposed next steps and timeline that we shared – I don't know if it was last meeting or the meeting before – the idea is that after the call later today – and I think that may be either tomorrow or early next week, we'll launch a quick and dirty survey where we'll just ask people to rank based in order of priority of topics that they think need to be discussed at the face-to-face meeting and rank the different policy principles as well as building blocks that are included in the report.

So that will then help leadership as well as CBI to build out the agenda to make sure that we focus most of the time on those topics where people feel strongly that those need to be further discussed face-to-face.

Of course, that doesn't mean that topics that maybe are a lesser priority are considered accepted or adopted or agreed, but it's really more to be able to organize the agenda and carve out time for those topics that are deemed to where we can make most progress in a face-to-face setting.

Amr, I see your question. I think that is maybe also a question to discuss on the call later today . We now have a zero draft. I note that there have been of course some updates to use cases made, some further discussion has taken place.

I don't know if there is an expectation from the group that staff goes ahead and makes further updates prior to the face-to-face meeting or whether you expect this now to be basically a frozen document until we get to LA and then start the more in-depth conversations.

I think you may have also seen that there are some areas where there currently are gaps. We have kind of identified placeholder for topics that we just haven't really touched upon yet to be able to write anything meaningful on paper at this stage.

So I think a question might also be, are there potentially volunteers that want to write up proposals for those areas where gaps have been identified that need to be discussed?

And I guess another question is indeed, does the group already want to start providing input on the building blocks and the principles in a substantive manner so that that input can also be used to frame the conversation and discussion in LA.

So I think those are all the questions that we hope to discuss and get your input on the call later today, but of course, for those that cannot make it, please share that with your views with your team members so they can flag it or weigh in on the mailing list, because again, we're really looking here for your guidance because I think we're all hopefully on the same page that what we're really trying to do here is setting up the LA meeting for success and that we're able to get as much out of it as possible.

RAFIK DAMMAK: Thanks, Marika. Before moving to Caitlin – and sorry again for letting you wait for a while – I think for all the logistics questions relating to face-to-face meeting in LA, they can follow up later to respond to any specifics, and I think you already started to get the calendar invitations. So Terri, please follow up with all those inquiries [inaudible].

Okay, Caitlin, please go ahead.

CAITLIN TUBERGEN: Thank you, Rafik. I have captured four action items. The first is for SSAC EPDP team members to make the agreed upon changes during today's call to the SSAC use case and notify EPDP support staff when that's complete.

The second is for EPDP support staff to input LEA2 use case into a Google doc and distribute to the EPDP team. Next is for EPDP team members to submit comments for the LEA2 use case by tomorrow, Friday, August 30th, and then following that, GAC colleagues to update the LEA2 use case based on comments received by Tuesday September 3rd and to distribute to the EPDP team when available.

Thanks, Rafik. Back over to you.

RAFIK DAMMAK: Okay. Thanks, Caitlin. I think with that, we are reaching the end of our call for today. Thanks, everyone, and I guess we'll see you in a few hours. Bye, and see you soon.

TERRI AGNEW: 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]