ICANN Transcription

GNSO Temp Spec gTLD RD EPDP – Phase 2

Thursday 22, 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. The audio is also available at: https://icann.zoom.us/recording/play/Dz9ecn0qKfzBNhrK9_wOtKP6JRWlBsZzpYrFMizM2K9dwLgtWc88En9kQCDv7r8h

Zoom Recording: https://icann.zoom.us/recording/play/_C3cshFxF9YhurMSvAQ5PU3h8P73WCS-GDV-A7GUFH1ik6dhlgsPMFr0GETVtpSR

Attendance is on the wiki page: https://community.icann.org/x/oqajBg

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

ANDREA GLANDON: Good morning, good afternoon, and good evening. And welcome to the GNSO EPDP Phase 2 Team Meeting taking place on the 22nd of August, 2019 at 14:00 UTC.

In the interest of time, there will be no role call. Attendance will be taken by the Zoom room. If you are only on the telephone, could you please let yourselves be known now?

Thank you. Hearing no names, we do have apologies from Ashley Heineman, GAC, and Margie Milam, BC. They have formally assigned Laureen Kapin, GAC, and Steve DelBianco, BC, as their alternates for this call and any remaining days of absence.

Alternates not replacing a member are required to rename their line by adding three Zs to the beginning of their name and add in parentheses, “Affiliation – alternate” at the end. This means that 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 the chat apart from private chats or use any of the other Zoom room functionalities such as raising hands or agreeing, disagreeing. As a reminder, the alternate assignment must be formalized by way of a Google assignment form. The link is available in all meeting invite e-mails.

Statement of Interest must be kept up to date. If anyone has any updates to share, please raise your hand or speak now. If you need assistance updating your Statements of Interest, please e-mail the GNSO Secretariat. All documentation and information can be found on the EPDP Wiki space.

Please remember to state your name before speaking. Recordings will be circulated on the mailing list and posted on the public Wiki space shortly after the end of the call today. Thank you, and over to our Chair, Janis Karklins. Please begin.

JANIS KARKLINS: Thank you, Andrea. Hello, everyone. Welcome to the next meeting. I think it is 15th in a row. So agenda is on the screen, a bit ambitious. The question is can we follow it.

I see no hands up. I assume that this is the case. So then we will do it as suggested.

Housekeeping issues. As you see indicated on the screen, we have, the proposal is that we would circulate a zero draft to EPDP Team on 27th of August. This is done with the aim to see whether a zero draft could be used as a basis for our discussions at the face-to-face meeting in Los Angeles. So if zero draft is out to the mailing list on the 27th, then the proposal would be to have an extraordinary team meeting on Thursday, 29th of August. That would give two days to members to read and to, so say sleep over the proposal.

And after, and the aim of that extraordinary meeting would be to collect initial reactions and to see whether there is any member or any group of the team who would say that this is not acceptable and we need to reconsider. So, and if that will not be the case, and I hope it will not be the case, then the next step would be to conduct a brief survey which would indicate the most difficult or sensitive parts of the draft where we would need to maybe put more emphasis during the face-to-face meeting and then we would finally look at proposed work program for face-to-face meeting if the zero draft is accepted during the meeting, 5th of September. So that is the proposal.

And when I am saying “extraordinary meeting on 29th of August”, that would be in addition to our ordinary meeting that would take place on the [27th, 2:00 UTC].

As usually, on the 29th, an extraordinary meeting would then be scheduled at 8:00 P.M. UTC, reason being that next week I am taken with my day job and the ordinary meeting of 29th will be managed by Rafik. So this is proposal and I want to see if that would be acceptable as suggestion. Any reactions?

I see no hands up. I assume that that would be acceptable. Good.

So then we can now listen to the update from Legal Committee and Legal Committee met two days ago, on Tuesday. And if I may call on Leon to brief the team on the progress of deliberations of the Legal Committee. Leon?

LEON SANCHEZ: Hello, Janis. Good morning, everyone. Well, the Legal Committee has made some progress on identifying the questions that are ready to be sent to the plenary for sign-off and then following sign-off from the plenary, we would be sending them for outside legal counsel.

We have a first batch of questions that is only waiting for one anchor question that actually informs the currently identified questions and we will be holding a call from the Legal Committee next week and we expect to have these anchor questions sorted out by next week and that would put us in a position to send the first batch to the plenary for sign-off. And if we do get sign-off, I mean, assuming that the Legal Committee's responsibilities to craft the questions in order to send them to outside counsel, then we would be able to send the first batch ahead of our Los Angeles meeting for external counsel and provide them with some time to provide replies to these questions.

So other than that, Janis, I have no further updates. I thank all the members of the Legal Committee for their very hard work and, of course, our support staff for facilitating our discussions and keeping track of our work. Thank you very much.

JANIS KARKLINS: Yeah. Thank you, Leon, for the subject. Any questions, immediate questions, to Leon about the update? I see Alan Woods. Please go ahead.

ALAN WOODS: Thank you. Thank you, Leon, for the update for that. I just want to [inaudible]. After having read the proposed legal questions that were sent around, I'm not big on the [legality] myself. I think I just wanted to flag for my own impression and I haven't had many conversations on this because literally, apologies, I only read them about three hours.

I do feel that they are exceptionally specific and they are exceptionally qualified in the sense that there's a lot of qualifiers. There's a lot of ifs, ands, and buts, and "in the case of this", and I just want to caution against us creating a situation where the answers we get are just absolutely unintelligible or not able to apply in a more general scale of what we should be looking at as there are much more overarching legal necessity questions and questions asking very general legal questions and I just find them a little bit specific.

So I know we had time more to discuss this, but I probably would err just to take it away from just being such a specific view with those qualifiers because I think we might end up with a product that is not very helpful to us. Thank you.

JANIS KARKLINS: Thank you, Alan, for question. Leon, you have an answer?

LEON SANCHEZ: Yes, Janis. Thank you very much.

Thank you, Alan, for your comment. In the legal team, we are aware of what you are saying. Our job so far, I mean, when you try to craft legal questions for counsel to reply or to answer, you have a double challenge. You have to take care of the question not being too specific that it won't inform, but you also need to not to have [inaudible] so open or so general that would also imply a great amount of legal resources to answer, or there actually might not be an answer because it's too general and it is just impossible for a legal counsel to provide an answer that covers everything that the general question entails.

So these anchor questions that I was referring to will inform the rest of the questions which I believe you have already read. And these hopefully will inform the general discussion of this EPDP group and will be able to actually be applied to different situations under the overarching concerns that I think we have all voiced through the process. Thank you.

JANIS KARKLINS: Thank you, Leon. I have two hands up now, one of [Omar's] and one of Milton's. Amr, please go ahead.

AMR ELSADR: Thanks, Janis, and thank you to Leon and the rest of the Legal Committee for getting this to us.

On the flip side to Alan Woods's earlier comment, the last question, question three, seems to be – excuse me – rather vague and unspecific. For those of us who weren't following the work of the Legal Committee very closely, would it be okay to maybe shed some light on why you're asking this question? And maybe also consider adding a bit more context to the question itself so that when the question goes to [Bird & Bird], that they understand why the question is being asked. But if you could highlight some of the thoughts behind this question to us now, I'd greatly appreciate it. Thank you.

JANIS KARKLINS: So thank you. Milton, please.

MILTON MUELLER: There you go. Everybody, okay. So my question was just I noticed it in a couple of places, the questions refer to accredited parties and accreditation, and we've been having some pretty serious debates about what we mean by accreditation and there are significant differences. I just wonder if the people who drafted these questions were aware of that. That's all.

JANIS KARKLINS: Thank you, Milton. I think these are members of the team, and of course, they are aware that issues of accreditation have been mentioned but not discussed in that sense of there is no

agreement for the moment whether and how it should be organized.

Leon, would you like to answer [inaudible]'s question? Or let me see if there is anyone else who would like to ask questions to Leon.

So I see none. Leon, if you have an answer, please go ahead.

LEON SANCHEZ: Janis, thank you very much. Amr, to your question, what we discussed in the Legal Committee was that we do have a previous member from [Bird & Bird], but there was a letter from the European Commission that came after the fact of receiving Bird & Bird's advice.

So what we want to do with the intent of question number three, is to ask Bird & Bird to update or provide us with updates, if any, to their previous memo in light of the letter that we received on May 3 by the European Commission.

So what we want to do here is to avoid duplicating work that has already been done and only ask a question in regard to the feasibility of providing a [inaudible] in light of this letter. I hope that answers your questions.

JANIS KARKLINS: Thank you, Leon. I think we will have –

AMR ELSADR: If I can respond?

JANIS KARKLINS: Yes. Please, Omar, go ahead.

AMR ELSADR: Yeah, thanks. I'm sorry, Leon, but you basically just repeated the question to me. So everything you say I got from the text in the question itself, but what I'm really looking for from you right now is to really highlight what it is in the EC letter that you believe warrants this question going to Bird & Bird and asking them for whether a reassessment of their initial memo on 61b is necessary or not and maybe also explain that as context to the question to Bird & Bird themselves so they understand why the question is being asked. Right now it seems kind of really open-ended and vague and both us and them, Bird & Bird, are free to go ahead and interpret it any way they like and then provide whatever answer they like.

So what I'm really wondering is whether the Legal Committee might consider nailing down some points from the European Commission letter saying these are points in the letter that have led us to wonder whether your initial advice on 61b still stands or not. And maybe also, so we as the EPDP Team have some sort of expectation on what we might be hearing back from them.

So if you could relay to us some of these thoughts now, that would be great. If you can't, maybe follow this up with an e-mail. Thank you very much.

JANIS KARKLINS: So thank you, Omar. I think it would be probably more productive if the legal team would take into account your concerns and discuss them during the next meeting or in the run-up to next meeting, and then we would see whether question three should need any rephrasing or not.

If that would be acceptable, we would proceed in that way. And once we will get the full batch of the questions, then we would examine them. So thank you very much.

Let us now move to next agenda item and that is the second reading of the use case providers requesting access required to facilitate due process in UDPR and URS.

So we had the first meeting and then updates and exchanges on Google Doc and I understand that IPC has made all necessary arrangements or adjustments of the text. And if I may ask, maybe Brian, if you could talk a little bit about updates you are introduction in the document.

BRIAN KING: Sure. Hold on. Janis, can you hear me?

JANIS KARKLINS: Yes.

BRIAN KING: Excellent. So yeah, we only made a couple updates to the actual text of the document. There was some good thought in the comments, which we addressed most of. I see [Omar's] comment there, which wasn't there when I finished up last night so we can go back and revisit that too, to catch anything that we didn't catch.

So we could do a brief re-walk-through here if you'd like because, like I said, there are only a couple things that we changed in the actual text or suggestions to change in the text of the document itself.

So would you think a more productive approach would be to revisit the kind of substantive conversations in the comments or to go back over the document itself?

JANIS KARKLINS: No. Maybe you can walk us through the major changes you introduced based on the conversation we had last week.

BRIAN KING: Sure. Sure, yeah. So the changes that we made were really light in substance and I noted those by proposing that you'll see some strikethroughs in the document if we can scroll down in the document. So we removed 61a. That was a wise suggestion from last week that we took on board and we removed that as a lawful basis for the requester.

If we go down some more, we kept 61d. Probably worth making a point that we understand that 61c is going to be a far rarer situation versus 61d, and this is mostly going to be a 61b. I note

that Milton's point in the comments was that he thought that 61f was the only appropriate basis here and we disagree, so we can note that and move on.

Then later on, we made another update if we scroll down. This is a sharp catch by the registrars. We were talking about a data subject here, not necessarily the registrants. So we made that update.

And then if we go down, I want to say that process comment, if we can maybe click on that for a second, was something else that we addressed. Yeah, this was another kind of typo error that the registrars pointed out. So this is domain history needs to be filed by the individual.

So accreditation is a bit tough here because I think as far as I mentioned in the chat, we all kind of have different thoughts about what that means and the overarching comment here is still that first one that says "if helpful" so that's kind of the most important point here and then we have some kind of concepts below.

And if you go down, I think that might be the end of the substantive updates that we made here. Again, we had some good policy chats or discussions over to the right but I don't know if we want to go through all of those today. We're happy to take those offline and keep that conversation going there. I note that Amr is reasonable as always and noted that we didn't have time to look and respond to all of his points yet but we're happy to do that soon. Thanks.

JANIS KARKLINS: So thank you. So let us then try to walk through quickly the case and see whether provided changes are sufficient and we can live with this case as now displayed on the screen.

So starting with Sub-Section A, and the method is if you have a violent sort of opposition or complete disagreement, please raise your hand. Otherwise, not, and hopefully we can go through issues rather quickly. So Sub-Section A?

Sub-Section B? No hands up.

Sub-Section C. No hands up.

Sub-Section D and probably E, they go together.

BRIAN KING: Janis?

JANIS KARKLINS: Yes?

BRIAN KING: Just a note, I should have struck 61a there in Sub-Section D. So I could make that update later.

JANIS KARKLINS: Yeah, okay. Thank you.

I see Milton and Amr. Milton, please.

MILTON MUELLER: Yes. On E, I thought we had, in our discussions, established pretty clearly that this was a 61f, that there would … Wait a minute. This is the UDRP URS. Okay, so yeah. I think we still have an issue here regarding the contractual obligation which, as far as we know, doesn't apply to third parties, that is the registrant or the registrar don't have a contract with the people requesting the data. So I would like clarification from the contracted parties. I know what Brian thinks about this. I'd like to hear from them about what they think the legal basis is here.

JANIS KARKLINS: I muted myself. Sorry. I will take a few comments and then I'll ask Brian to answer. Amr, please.

AMR ELSADR: Thanks, Janis. I put this into the document but if Brian could just maybe shed some light on this now, that would be really helpful.

I'm wondering about the rationale in Section E on the use of 61c as a legal basis here and it's not exactly my understanding of 61c that that was the legal basis at all, so I'd like to just hear more from Brian about why he believes there may be situations where there might be legal obligations on contracted parties to disclose data to third parties. There's just, I don't want us to get into a discussion disputing the legal basis of this point but I'd just like to get a better understanding of why he believes this legal basis is applicable, and maybe an example or two. That would also be helpful. Thank you.

JANIS KARKLINS: So thank you, Amr. I see Farzaneh's comment and I would like to call on Farzaneh to raise her issue. Farzaneh, please.

FARZANEH BADII: Yeah. Thank you, Janis. I'm sorry. I was not ready to take the mic. But so basically, what I have seen – this is like a general comment and not necessarily only with this case – but whenever the use cases are up and we comment and I see that Milton's comments have been posted on 15th of August so it wasn't that late. And then the drafters of the use case just disagree with the points and decide not to make any changes, not to come to any compromise and I think that we are not going to get anywhere if this continues if we disagree and then they say, "No, we are right," and the text doesn't change. I think the time that we are putting in, also they are putting in, is kind of wasted. Thank you.

JANIS KARKLINS: Thank you, Farzaneh. I think this conversation is exactly to address those points where is remaining points of disagreement after exchange of comments on Google Doc.

So if you have a specific comment or issue with the current case, please don't hesitate to raise your issue here or in any other case. And now, Brian, to you.

BRIAN KING: Sure. Thanks, Janis. So I think the outstanding question for me is from Amr and I'm happy to explain our line of thinking there.

So the concept behind 61c is that UDRP and URS opinions can be appealed. And often, if that appeal happens in court, like it might in the U.S. or other jurisdictions, then processing the data might be necessary to comply with the legal obligation to comply with that court or participate in that court proceeding. So that's one example that we're thinking of where there would be a more typical legal obligation instead of just the contractual 61b obligation.

JANIS KARKLINS: Thank you. Thank you, Brian. Alan Woods. Is next.

ALAN WOODS: Thank you. Thank you, Brian.

So just to echo what Milton was saying and I think you both said it in the group chat as well. I think 61f not being here would be an issue and I think just to probably say what Farzaneh was saying there, it's important for us to actually go through this and do the actual review of this to "This is what we would do. This is why we're using the use cases." We're saying, "Okay, they say that there's legal basis. Is this the correct legal basis and would we go back to the math for clarification?" That's what the process is. We're just doing it in a full kind of plenary fashion here.

When you get to 61f, or sorry, 61b, the contract, ironically, we just talked about the legal [question] going to Bird & Bird about their memo on 61b and I think reading 61b, especially where they're talking about the second half of that particular memo and they're talking about the necessity and whether or not it's strictly

necessary for the performance of that contract and they enjoy a parallel between abuse management of a registrar and say even in their reckoning that that's not actually a 61b because it's not strictly necessary for the registration of the domain itself, and however, they do believe that it would be a 61f.

And I think it's probably short-sighted of the IBC to not put 61f in here and I would urge them to reconsider that specifically as well. And again, looking at the legal advice that we do have, and again, if we're going back to the, so be it. But at the moment, that's the advice that we do have.

JANIS KARKLINS: Okay, thank you very much. There are some comments in the chat room how to resolve these differences in opinion. And I would like to encourage team members, think sort of for the future, we will have some policy recommendations including related to lawful basis and how we would reflect these policy recommendations or these difficulties that we encounter, basically looking through every use case, what legal basis we could use to request information or disclose information.

And then how these difficulties will be reflected or differences of opinion will be reflected in policy recommendations and how we will be able to formulate those policy recommendations. So I think this will be the tricky part when it comes to disagreement on each of the use cases. For me, it is simply an indication that this probably will be one of the difficult issues in our discussions working on policy recommendations. Whether we need to come to agreement on each specific case, which article would be

applicable, again, I'm not sure. But in general, please think forward how we will reflect these issues in the policy recommendations.

So any other comments on legal [inaudible]? Any reaction, what Brian said, responded? I see Milton. Milton, please go ahead.

MILTON MUELLER: Yeah. It's okay, I think, at this stage for Brian to say we disagree that it's all 61f, but it's unacceptable for him not to amend this to include 61f as one of the legal bases. That's just not acceptable. It has to go in and it has to go in now.

We have somebody from his own stakeholder group, Thomas Rickert, saying that it should be in there. We have the registrars. We have the registries. We have the non-commercial, so I just don't see how you can stonewall on this. Let's get that done.

JANIS KARKLINS: Thank you, Milton. Alan, you are still on the line or this is the old hand? Thank you. So Brian, you heard insistence and so please consider that request.

Let me now go further. The case, Sub-Section F. I think the Safeguard section is also very important for our future work. Any difficulties with the Sub-Section F? I see none.

Sub-Section G? Any questions? I see none.

Sub-Section H? I see no requests.

I? No requests.

Accreditation, J? Any thoughts? Any questions? Amr.

AMR ELSADR: Thanks, Janis. Just flagging another comment I posted on Section J, just that I'm not sure I agree with "or" being used in these accreditation criteria and appreciate that we still haven't agreed on what accreditation actually is. But in general, I think if there is going to be processing of gTLD registration data, I would assume that a combination of these criteria needs to exist. It shouldn't be one or the other, or the other, or the other because there are four of them.

So for example, if an actual trademark holder is filing a complaint, they would need to provide evidence of ownership of the trademark. They would need to provide evidence that a dispute has been filed and they would need evidence. They would need a combination of these things. In the case of an agent doing this on behalf of the trademark holder, I would assume that at least three or possibly all four of the criteria should be submitted together. But the way they're written now, it seems that whether it's the trademark holder or the agent, all they need to do is submit one of these criteria, whichever one they choose, I suppose, and that would be fine. But I don't see how that should be the case. So I just wanted to flag that now.

Again, I'm not asking Brian or anyone else to respond to this now. I appreciate that I only submitted these comments a short while ago. So I just thought I'd voice the concern. Thank you.

JANIS KARKLINS: Yeah, thank you. I think in practical terms, that accreditation, if we would decide that as a policy recommendation to sort of seek to establish such accreditation mechanism, then that would be much more complicated and should be addressed to organizations with a specific knowledge and experience in these fields. So that, I think, is another step in our conversation. But thank you for raising this issue.

So I see two hands up. Michael. Sorry, Milton and then Marc Anderson. Milton, please go ahead.

MILTON MUELLER: I just have a question about number four. I've been beating my head against the screen trying to figure out what it means.

So why would an entity-seeking accreditation or disclosure, actually, have to be affiliated with a dispute resolution service provider and what does it mean to be affiliated with? Are we talking about the actual dispute resolution provider requesting the disclosure or is it a third party? I thought it was a third party we were talking about. I just don't understand that number four, so hopefully somebody can fill me in what's meant.

JANIS KARKLINS: Okay, thank you. Brian, this will be after Marc for you to answer. Marc, please.

MARC ANDERSON: Thanks, Janis. Can you hear me okay?

JANIS KARKLINS: Yes.

MARC ANDERSON: Excellent. My question is a little bit similar to Milton's and so I guess I'll piggyback on what he said. This is a question for Brian. I guess you're losing me a little bit in accreditation. I'm wondering if you can sort of explain how, what your visioning here when you wrote the accreditation section. Who is the accreditation for as you envisioned this use case? Are you accrediting URS UDRP providers? Is the accreditation for the entities that would be seeking to file a UDRP or URS claim or both? I guess I'm just, I got to this section and you just kind of lost me a little bit here so I'm wondering if you can provide a little more detail, what is it you have in mind, what's your vision for this particular section in the use case.

JANIS KARKLINS: Thank you very much, Marc. Brian?

BRIAN KING: Yeah. Thanks, and great questions from Milton and from Marc. And I think part of the confusion might be that we were trying to stick to the template and maybe that didn't allow us the best opportunity to be clear here or we missed that opportunity anyway. So I think there's two things that we're thinking about

here and one general overarching thing that we've been reluctant to talk about accreditation all along because I think it means different things to different folks, and also that we think that we shouldn't talk about accreditation until we've identified a problem that accreditation will solve for us. And we may have finally found such a problem here.

So there are two things happening in this box and one, I think, to [Omar's] point is that these were kind of drafted as "or" because if you look at number one, number one says you're a person who can demonstrate that you have an IP right. Number two is if you're not that person, that you work for that person. And number three is that you show that something has been filed. So it could be one or two and three is kind of the way that this goes to get you accreditation and then we can talk more about what accreditation means.

Number four, I think is the real problem that accreditation can help to fix. And that is if you are WIPO or – what do they call themselves now? – FORUM, a UDRP provider or a panelist, so someone to capture the affiliated with dispute resolution service provider, maybe you should be accredited to just pull in or pull out the data about a domain name when you've received a complaint. And that accreditation doesn't come without safeguards, obviously, audit trails and that kind of thing.

But the fact that those groups will always need to access the full non-public data could be just the type of problem that accreditation helps to fulfill and I don't think that situation extends to the IP owner or their employee, agent, or service provider, whoever is filing the UDRP. I think we try to make our concept fit

in this box and we probably didn't do it as well as we could, but that's what we're looking at there. Thanks.

JANIS KARKLINS: So thank you, Brian. I think that this box is self-evident, at least from a common sense point of view. If we are looking to the title, it's accreditation of the user group and if we accept that the structure of the standardized system is, there is building blocks on demand side, and building blocks on supply side, then accreditation would fit as one of the potential building blocks on demand side which would indicate to data possessors that entity requesting information is not just a random entity but somebody who is working in the area and potentially could be trusted because of the nature of their professional activity. So that is, of course, not a guarantee that the request is legitimate, but that is an element that would indicate to supplier of information on disclosure of information that this is not just a random person from the street, but somebody who may be trusted.

And so in case of IP, intellectual property, of course that's reasonably straight-forward if we think that intellectual property protection system in the world is well-organized and there are authority organizations that could, if they are wishing and accepting to provide that accreditation service should that be decided. I see Milton's hand up. Milton, please go ahead.

MILTON MUELLER: Yeah. Janis, you said that you thought it was obvious that these things kind of fit but I think what we may be dealing with here is a

case of conflation which should be eliminated from the use case. So it's apparent from what Brian said that in some sense, the user of this use case is the dispute resolution provider and in other cases, it's the trademark holder seeking to protect their rights. And I don't think those things can be combined in a single use case. I think there are different legal bases. I think there are different use cases and I think that might be accounting for a lot of our disagreement here that this is not the same user group.

So there's the people who want to disclose information in order to decide whether they want to file a UDRP case or a URS case, and then there's people who are the dispute resolution providers and they're very different. I think I would see the legal basis for the two of them being very different.

So I'm reading the comment here, "We can't de-conflate complainer and dispute providers since they work together on the filing." Well, of course you can. They are different use cases. I would have no problem with a use case that says that a dispute resolution provider has a 61b contractual basis for disclosure, no problem with that at all. If you're telling me that any trademark holder in the world can disclose, then clearly to me, that's a 61f. It's a very different case. And I think it's easy to de-conflate them. I think it solves all kinds of problems in terms of defining this use case. So I'll be quiet now.

JANIS KARKLINS: Thank you, Milton, for your comments. I think that simply indicates that we need maybe to use the cases in order to understand broader issues because if we are thinking of writing policy

recommendations, we will not be able to write a policy recommendation for every possible use case or real life situation. So we need to still think slightly wider and then, of course, implementation will be different. That will be the next step in the process. So Brian?

BRIAN KING: Yeah, thanks. I think Milton's really on to something there and I don't think we agree with absolutely everything that he said, which should be no surprise, I think to anyone. But we do, we are talking about a couple different folks here that are going to have a need to process this data. And I think that we could do two use cases. We're trying to be sensitive here to the folks in the groups that thought we had too many use cases and we had to try to keep the concept in tact here. This probably goes to [Omar's] question or point about 61c also is that the same kind of world is implicated when these things are appealed in court, so if we had a separate use case for every kind of discrete thing, then we might have less confusion or fighting about those. So maybe we're damned if we do, damned if we don't.

But I think it's worth noting that we think the 61b processing basis still applies even to the complainant because the GDPR 61b, processing is necessary for the performance of a contract to which the data subject is party. The GDPR doesn't require that the process or the new controller for their own purpose is a party to that contract. It's that the data is necessary for a contract that the data subject is entered into. And that's 61b basis and that logic extends to whoever is involved in the UDRP or URS, be it the legal entity of WIPO or FORUM, or panelist or the complainant.

Right? Because it's still the contract that the data subject entered into. So the 61b processing legal basis should carry through regardless. So that sounds like it might be where we have some disagreement, [inaudible] understand if that's the case or if I'm missing it. Thanks.

JANIS KARKLINS: So thank you, Brian.

In absence of further requests, let me now move to the next sub-section, L. Any comments on L or disagreements? I see no requests except old hands.

M?

N?

O? No requests, so seems to me that we have, on this case, still remaining disagreement in the section of legal basis, and Brian, if I may ask you to consider every concern that has been expressed during this conversation and amend the case properly even if you disagree, then the method would be to simply indicate that there is a disagreement on that and probably to the rest of the team, simply an invitation to think more about accreditation issues that also seems to be a bit complex issue.

BRIAN KING: Janis?

JANIS KARKLINS: Yes, please.

BRIAN KING: Thank you. If I could respond before we close, I think we're on the cusp of something here with the legal basis question and I'd like to have more conversations about 61f. I'm all ears and my colleagues here have really implored us here to consider 61f as a legal basis here and I'd love to understand that perspective a bit better. It sounds like we haven't properly sold the concept of 61b to everyone and we're pretty convinced that that's the way the law works, so if there's remaining disagreements about that, we can just note those in the document and move on. That didn't seem to be a popular approach maybe because we hadn't noted those in the document yet. But I think that we're not quite finished with that conversation and I'd love to take it on later or now or whenever you think is appropriate. Thanks.

JANIS KARKLINS: Yeah, I'm happy to entertain another ten minutes of this conversation if you wish so and if team members are ready to talk about legal basis in this particular case.

BRIAN KING: Thanks, Janis. And if I could, I'd like to maybe start with the point that Milton just made in the chat that there's a 61b for dispute resolution providers and maybe that's a thread we can pull on to get where we need to be. So why do we think that the dispute resolution provider is a party to the registration agreement in which the data subject has a contractual tie to the UDRP? I didn't

think that the dispute resolution provider signed every registration agreement. Sorry to be a bit pedantic there, but why would it apply to the DRP but not to anyone else involved in the process? Thanks.

JANIS KARKLINS: Any reaction? Milton? May I call on Milton?

MILTON MUELLER: Yeah, okay. So I just put a comment in the chat, but I mean it just seems obvious. The answer to the question seems obvious to me that the registrant has signed a contract that commits them to bring their disputes to a dispute resolution provider and so that's in the registrant contract. You must respond to a DRP and have your case arbitrated by them, and then complainant is not a party to that contract. They are an unaffiliated third party with a legitimate interest, and again, I want everybody to understand on every side of this debate that I totally support the legitimacy of the interest of a trademark owner seeking disclosure of a registration record that looks like they have a reasonable suspicion that it is an infringing or a domain that abuses their intellectual property. I'm totally in favor of that and I just think it's pretty clear that the legal basis for the trademark holder is very different from that of the dispute resolution provider who has a contract both with ICANN and is invoked in the registrant contract. But maybe the contracted party should write these contracts and deal with them should we talk in here.

JANIS KARKLINS: So thank you, Milton, for your explanation. Anyone else?

BRIAN KING: Yeah, Janis, if I could respond. So I can appreciate where Milton's coming from. I think it's not even a logical baby step then to consider that if the registrant has submitted to the jurisdiction of the UDRP or URS which require the complainant to prove that the registrant doesn't have rights in the name, that the registrant acted in bad faith, that knowing who the registrant is, is imperative and necessary to prove that their personal data, if the registrant is even an actual person, would be processed by that complainant. It just seems to be common sense.

JANIS KARKLINS: So thank you, Brian. There was Thomas's hand up but then it disappeared.

[THOMAS]: Thanks, Janis. I was too quick in lowering my hand. The way I see it, I think that to look at the contractual relationship with the registrant, the contracted parties involved as well as the complainant may obtain data based on 61b, because deploying the UDRP procedure is something that is part of the contract with the registrant. But if you then have third parties such as the dispute resolution provider who obtain that data, the contract between ICANN and them would likely create a 61f because there is a legitimate interest in using that third party as an independent arbitrator or dispute resolution provider. So why don't we leave those two legal bases in? And I think we're good.

JANIS KARKLINS: So thank you, Thomas. Brian, your hand is up still or that's an old one.

BRIAN KING: Sorry, Janis. It's just still up.

JANIS KARKLINS: So anyone else? If not, then I would, again, like to encourage Brian to consider putting those comments in the case and noted that there might be some difference of opinion and then post that updated case on our Google Doc again.

And with this, I would like to move to next agenda item and see whether we can close the SSAC case. Can we get that on the screen?

Case investigating criminal activity where domain names are used, a specific example, phishing attack. So there, we had several rounds of discussion of this case and there were a number of disagreements and I would like to see, maybe invite Greg to indicate whether comments of Farzaneh, mostly, have been addressed in a constructive way. So now would be the case to say that.

GREG SHATAN: Okay. Hi. So we did make a number of edits based on comments received. There were only two working party members who made mark-ups on this document. One was Alex Deacon, and that's just

a couple of comments. Mainly, objections and comments came from NCSG.

Now we made some edits based on those, and in other cases, we responded to the comments by explaining why we said what we did and why believe it is correct. So these are cases where we've responded. We can talk about them some more, although I do want to be respectful of the group's time.

A question for you Janis, is my understanding is that these are not consensus documents, that we do have this issue of people want edits but sometimes there's disagreement about them, so what happens? And so that's my question to you. If we have a disagreement, how should that be reflected?

JANIS KARKLINS: Yeah. No, thank you. I think we may have minor differences of opinion and we're not seeking for complete consensus. But if there is, let's say, violent or conceptual disagreement, then either we need to bridge it and then reflect back this middle ground in the document, or as in the previous case, we would need to indicate that a specific issue had opposite views or very divergent views. So that would be my proposal.

GREG SHATAN: Okay, so how would you like to proceed? I mean, there are quite a few comments here.

JANIS KARKLINS: Yeah. Let me ask Farzaneh since Farzaneh was actively involved in commenting of issues. Would you like to raise those issues for the record? Farzaneh, please go ahead.

FARZANEH BADII: Thank you, Janis. So basically, some of these comments, most of the comments are from NCSG. We worked on a document and then imported those comments to the Google Doc here, and wherever is my own personal opinion, I have mentioned it is my personal opinion.

However, there is, in some instances, the SSAC use case invokes a [recital] that we disagree they are applicable to this use case. And it seems like Greg does not agree with us and I think this is like a disagreement on whether there is title applied for or not is kind of like a legal issue that I don't know how we can resolve it. But as Marika said, we could get the penholder to note in the use cases that different opinions were expressed about this and it kind of puts our argument why the [recital] that Greg has invoked do not apply to this case, why we think that the other clauses, 61b, other than 61f do not apply to this use case.

And also, I think that my comment about the safeguards for that applicable to the entity disclosing the nonpublic registration data still stands because as I said, as I argued last week – I don't know when – the safeguard requirements are applicable to the entity for actually protecting the data subject. It's not about facilitation the requesters access to data. And I think that they still do not believe that I am right. So for example, they still say that a requester should be able to request and receive both the public data and the

requested nonpublic [inaudible]. No. I'm not saying that I disagree with this. Sure. I mean, we can discuss this later. But these requirements do not belong to column G, specifically, because there are actually safeguards for the data subject and not for facilitating the requester access to data. So a lot of the comments that we have made have not been fully addressed, and as Greg said, this is not a consensus document. And if it's not a consensus document and if we are not actually extracting policy recommendation based on them, I don't know what we are going to do with these documents. My concern is that we keep saying these are not consensus documents. They don't have to be changed when you oppose the text, and then later on, we actually extract policy recommendations from them. So I am unclear about how we can go about this, but as Marika said, maybe we can just add, maybe the staff can add the disagreements to the text. That's about it. Thank you.

JANIS KARKLINS: Yeah, thank you, Farzaneh. I think that the value of this exercise is to building our understanding of the issues that allows us to formulate policy recommendations afterwards. These documents, as I personally see, might be attached to the report for information that would demonstrate the way how we got to those policy decisions, which informed our discussions and again, as I already tried to indicate that policy recommendations most likely will not be able to address every single real world possible case but rather, will be more sort of higher level and policy level and then implementation that address more practical further steps in operationalization of those policy recommendations. But I have

now many hands up starting with James followed by Milton, Marc, and Thomas in that order. James, please go ahead.

JAMES BLADEL: Thank you, Janis, and in recognition of the length of the queue, I will be brief and just note that I believe that contracted parties have noted their discomfort with the combination of criminal activity and abusive activity in outlining this use case. I don't know if it was captured here or in this document or if it may be in a previous version, but we do believe that there is significant overlap between this as written and the previous use case that was established, I believe by the GAC, one of the first ones we looked at.

So if we can tease that out or separate them into two, I think that's worth considering because I think that the law enforcement, I think everyone recognizes, has a much more robust legal basis for disclosure and they have authorities and capabilities that transcend this policy and this potential framework that we're developing so I just want to reiterate that concern, that including criminal activity as part of this use case is probably not appropriate and it belongs somewhere else but it should probably be teased out of here. Thanks.

JANIS KARKLINS: So thank you, James. Milton, please.

MILTON MUELLER: Yes. So it's me again and I think what we have to be clear about here is what we're doing with these use cases in terms of how they fit in to our final report and how they fit in to our process. I think we all understand what Janis has said, that these kind of exercises allow us to confront issues which then sharpen our understanding of. The problem comes when we talk about including these use cases in our final report in some way.

So if documents are part of the report, ideally, they have to be consensus documents in the sense that we are all comfortable with the representation of the use case in question.

At the very least, they need to acknowledge all major differences of opinion. That is, we cannot allow whoever happens to be the penholder to be an advocate for a particular use case and the use case becomes a wish list. And in the case of this particular case, the SSAC case, it is a wish list. It's saying, "We want any and all data. We want it automatically. We want to claim any and every legal basis that can be thought of, and we want to conflate private actors with state actors." And our whole task as policymakers here is to not do that, to tell ICANN what is likely to be legal and what is likely to be illegal under the GDPR and other privacy laws in this SSAD.

So we can't allow the use case, the penholder to simply arbitrarily decide that they don't agree with something and they can unilaterally determine what the appropriate legal basis is. We have to work that out as a group, or if we don't do that, then we cannot include these use cases as part of our report. Thank you.

JANIS KARKLINS: Thank you, Milton. I acknowledge your point. I said this is my personal opinion and then certainly this is up to the group to decide how to, what to do with the use cases at the end of the process. But I think we are now getting a very clear understanding that if we cannot agree on certain issues, then these disagreements need to be reflected in the use case and I will make sure that this is done, if not be a penholder, then by the staff. Marc. Marc Anderson, please.

MARC ANDERSON: Thanks, Janis. I want to agree with Milton and James. First, on the point of including the use cases in the final report, when we first went down this use case path, I understood that the reason why we would be looking at use cases is that we would use them as a tool to help inform our deliberations on developing policy for access to nonpublic registration data. If our purpose for developing use cases was to produce documents that would go into the final report, that's a very different purpose and reason for developing these use case documents and I certainly would be looking at them differently and commenting differently.

So I agree with Milton's points. I don't think that we're on a path that I, at least, would support including them in the final report and if that's the intent, that will cause me to go back and revisit them.

On James's point though, I want to circle back to that. I think James made a very good point and I want to expand on that a little bit in that there are many important things in this SSAC use case but the inclusion of both abuse and criminal in the same use case is making it difficult for me and I think my contract party

colleagues as well, to look at the entire case on the whole. I think there are things in there that are best left to an abuse use case and there are things in there that are best left to a criminal use case. And the fact that this use case as written covers both, sort of conflates aspects that should apply just to a criminal use case are also being applied to an abuse and things that are best left to an abuse case are also being included in the crime abuse case. So what we're seeing is there's overlap between two use cases that's really making it difficult for us to take sort of a fair and holistic look at the use case as it's written. So that's, I think, causing some of the difficulties we have in evaluating this use case.

JANIS KARKLINS: Thank you, Marc, and let me withdraw my idea of attaching the use case to the report. So please forget about it. I mis-stepped. I take it back and if there will be need to discuss what to do with use cases, we will the engage in proper discussion. Next is Thomas on my list followed by Alan and then Greg will conclude this conversation. Thomas, please.

[THOMAS]: Thanks very much, Janis. I'd like to make two points. One is on the use case itself. Maybe this has been discussed earlier, so please bear with me if I [see] your time. But for me, the biggest question on this use case is how to identify eligible requestors. In the legal team, we've been discussing SSAC 101 which offers a definition of a security researcher and that definition, to me, is overly broad so that everybody who is, let's say, interested in studying Internet use would fall under that definition. Also, if you,

let's say, only run your own main server, if you're interested in delivering e-mail property, that would make you qualify under this definition.

So my question to Greg would be has there been any thought given to ensuring that not each and everybody who can come up with certain ideas that have to do with security can be an eligible requestor and get access to this system which would likely open the floodgates for [gaming] the system.

The second point that I'd like to make is on the policy versus use case side. And I think what we've seen in classical lawmaking is that laws should be abstract and general and apply to a multitude of use cases, but the more explicit legal provisions are, the easier it is for the reader to digest and understand what they mean. And I think on an issue as important as this with all the liability risks potentially involved for the parties where [valid wise] to include as much detail as possible in the policy in order to make sure that there is no [inaudible] afterwards and the policy might be construed in the broader way that causes liability risks for all the parties involved. Thank you.

JANIS KARKLINS: Thank you, Thomas. Indeed, in the case, in Sub-Section J, there is very little information about accreditation and Greg, maybe you can think while Alan is talking and you are listening to him, what would be your thoughts about how the accreditation system would look like if that is decided to be established. Alan Greenberg, please.

ALAN GREENBERG: Thank you very much. Your withdrawal of the use case in this final report takes away half of my comment, so I'll be very short. I don't see this use case as conflating crime and abuse because they are, in fact, two aspects of the same thing. The fact that someone is abusing domain names does not make it not a crime. So when you're looking at things like phishing which may use multiple domain names to affect the phishing activity, it is implicitly both domain name abuse and a criminal action which ultimately may well go to law enforcement for criminal enforcement. But they're not necessarily [inaudible] to each other to be treated differently because they're two aspects, two faces of the same type of thing that is being investigated. Thank you

JANIS KARKLINS: Thank you, Alan. Greg, now back to you.

GREG SHATAN: Okay, so I'll try to round up the comments. First, let me go with Alan's comment. That was basically what I was going to say. Crime and abuse are not disambiguated because they can't be. I mean, if you have a Venn diagram, there's a big overlap between the two. And of course, something like phishing is a crime.

Now what can make a difference is which party is dealing with it when. As we've said, law enforcement has different bases than a private party. However, as SSAC has said, private parties are dealing with things that are criminal like that and would be making requests because they're dealing with that kind of behavior and

that's why we reference 49 at the top of this document, which explains why that's an important consideration. So trying to jam these two together, you still have to keep legal bases part.

Regarding safeguards, as a group, I think we have a chicken or egg situation which is safeguards might be pretty much the same no matter what kind of a party is making requests, especially under 6f. It doesn't matter whether it's a network operator dealing with cyber crime or maybe an intellectual property requests. Safeguards are all going to be similar, and as a group, we haven't said, "Okay, let's talk about safeguards." Right now, it seems more like we're collecting ideas for what safeguards might be relevant. And so we put down some things that are important, but we also assumed as we stated in the comments, the group is going to have to get to safeguards and talk about them kind of a little more holistically and as a separate subject.

So in relation to what Thomas said, accreditation comes out of safeguards. We'll have to figure out what safeguards are important for any party to have in place and then you get to the issue of accreditation which is partially an issue of trust and it's partially an issue of having some sort of expertise, perhaps, and the ability to properly handle data.

So again, we didn't try to get into accreditation criteria in much depth because we'll probably have to do that at some other point. SSAC has said, "Look, here's a broad definition of what people do when they're dealing with security issues and here are some of the people who do it." That doesn't necessarily mean that we think that all of those people should have access and should be automatically accredited, by no means. It's our assumption that

people who get into some sort of accreditation program will have to meet some sort of bars. So I don't think we're really far off on those issues at all.

I wasn't sure what to make of Milton's comments. He ascribed some motives to people and I'm going to look at the transcript. I may comment further on the list after I can quote the transcript. But in some ways, I felt like Milton was saying, "Yes, everybody does have a veto on anything said in this doc and it is, therefore, a consensus document." So I'm going to have to go back and look at the comments there.

I am with Janis in that these documents are, right now, the only place we have to capture points and ideas. The parts of an initial and final report that are consensus-based is not every single thing in the document, perhaps, but the recommendations which are going to be more specific. So it would make sense to note places where there are disagreements.

And there two things that Farzaneh said. One was about safeguards, which I've talked about. The other one is about legal bases. The SSAC team started looking at the bases from the comments. Now, what we said is, "Look, 6f is going to represent most of our requests here." I think we all agree on that. However, after looking at it, we do think that it would be inadvisable to rule other bases out because there are some demonstrable cases where those are certainly possible. In the document, we put some comments about that and more examples of where some of these other bases could come in.

So we think it's inadvisable to rule all except 6f out and we've explained some of the thinking there. I'm not sure what the danger would be in keeping them in with some additional commentary.

JANIS KARKLINS: Okay, thank you, Greg. I see Marc Anderson is asking for the floor. Please, Marc.

MARC ANDERSON: Thanks, Janis. You know, listening to what Greg just said, I just had a thought. I appreciate the points he's making and I want to just make a suggestion. This is a little bit off the cuff, but you're talking about the legal bases there at the end and I really think you're getting to the heart of the problem and I think the legal basis discussion is really causing us to stumble on this use case a little bit, and there are a number of very good and important things in this use case that we should be talking about and instead we're getting wrapped around the axle on the legal basis.

So maybe Greg, just a suggestion listening to your points, what would you think of separating the use case based on the legal basis? So we could have a conversation on this use case if it's a 61f and we could have a conversation about this use case if it's any other legal basis besides 61f. Again, just a thought because I'm feeling a tad frustrated that we're not getting to the important parts of the discussion on this use case and rather, sort of hung up on the points of disagreement and if that might be a way to break through that and getting us to having a more productive conversation, maybe that'll help.

GREG SHATAN: I see what you're suggesting. The use cases were supposed to flow from a particular use or a particular problem that was trying to be solved. Right? So in this case, we said, "Okay, let's talk about cyber crime, phishing as an example." The bases, now flowing from that, it depends on sometimes who is making the request and who is dealing with it right? And so we have to have these bases under this use case.

I don't know if it would be useful to have five different use cases that are all cyber crime, each one having a different basis. That might be duplicative and maybe even more confusing. I think what we have done here is we've said, "Look, this case is primarily dealing with private actors." PSWG and the GAC people have presented one for law enforcement and it deals with a different basis. I thought that was a good division.

JANIS KARKLINS: Yeah. Thank you, Greg. I think this is one, also important aspect that we need to think further, specifically thinking about recommendations. Most likely, that will be discussions about user groups or user categories but the philosophical question or systemic question is, of course, how much access the private actors will have according to policy to private registration data, nonpublic registration data. So I think that is something that we are learning from this case where from one side, there is legitimate interest and a wish to have as much access as possible. From the other side, the argument is that it will not be as it was. There is a new situation and we need, really, to find that

balance and reflect that in the policy recommendation. And this case, in my view, is very illustrative in that respect.

So I see no further requests for the floor. Let me then conclude and invite Greg or any other penholder to reflect conversation that we had in the case. For the moment, I would suggest that we would park this case after amendments and see whether we need to revisit it at one point when we're going through the zero document. That would be my suggestion.

In absence of opposition, then I would like to move to the next agenda item and that is another SSAC case. When a network is undergoing an attack involving a domain name and the operator, that network needs to contact the domain owner to remediate security issue. So who will be introducing that case? Greg, that's you? Or Ben? Ben, please go ahead.

BEN FULLER: Yeah, thanks. I'll take this one as I have quite a bit of experience doing this exactly and was the initial penholder on the use case. I'm hopeful that this is one that is simple enough that we can avoid some of the wrap around the actual issues. Essentially, domain names are often used, either maliciously or via compromise in DNS-based attacks, DDOS being the most common. This presents itself in scale when a botnet is used.

There's examples. I included in here things like the Mirai botnet. I think a lot of us are all familiar with that sort of situation. And realistically, the use case is about a network operator who is under attack and they need to get a hold of the holder of a domain

name that is the command and control infrastructure for the botnet that is initiating the attack. In order to do that, realistically, we're talking about contact so [inaudible] data isn't really going to work. E-mail could certainly be addressed via the e-mail form that can be put in WHOIS. But most of the time, this is a situation that needs kind of immediate contact, so we're stating in C, that the registrant, admin, and if it's provided, technical contact name, e-mail and phone is the personal data elements that would be required here.

In Section D, we are again saying and acknowledging 61f is going to be the basis in almost every case. But we did include 61d because as was the case with Mirai, sometimes critical infrastructure like hospitals and power grids and law enforcement and that sort of thing can be brought down by these attacks. So if it is the case that the network that's being attacked or is suffering damage belongs to critical infrastructure, we think 61d might apply and that would be, of course, disclosed in the disclosure request to the controller.

At risk of blowing past this, I'd kind of like to know if there is any initial violent disagreement to the inclusion of 61d in the case of critical infrastructure.

JANIS KARKLINS: No, Ben. Please go through the case and then we will have a conversation because this is initial conversation. More substantive and in-depth will be next week.

BEN FULLER: Okay. So then in Section E, we again are citing [Recital] 49 because this is exactly what [Recital] 49 is describing is the need for certs and C-certs and network operators to be able to defend against attack, essentially. We've all read it. Hopefully that is something that we can see that this [Recital] does apply in this case. Obviously, any comments on that would also be welcome.

Can we scroll down to Section F?

So we've had quite a bit of discussing refining safeguards since this was initially written, so please forgive if some of this is some edits that we just need to make in bulk. But we are definitely proposing that the requester would have to comply with all GDPR aspects. Let's see here.

As far as disclosing the data, same standard safeguards in place. Only supply in compliance with GDPR as we've discussed before. As far as the safeguards, I think this is all fairly standard.

When we get to the accreditation aspect, again, we don't have a specific recommendation as far as accreditation. It may or may not even be possible. I have thought a little bit about whether there could be an element of accreditation tied to the owner of the network information via the IP address providers, but that's something that we would need to think through a little bit more just as a way of demonstrating that the person requesting the data is actually the owner of the network in question. Or as was kind of mentioned in the intellectual property case, sometimes the owner of the network subcontracts the maintenance and defense of the network out to a third party provider. Some of them are Dell

SecureWorks and those sorts of companies do so on scale for a lot of companies.

Go ahead and scroll down.

Something that may need to be considered as far as whether the controller is going to produce or dispose of the data, they may need to ask for the logs to show that the attack is happening and thus, tied to the domain name in question so that they can have reasonable certainty that the disclosure may need to take place.

So what we're saying in [ill], the basic information that needs to be provided is, what is the domain name, what is the purpose, acceptance of the user agreement, and if accreditation can be developed, then whether or not this is an accredited user or authorized on their behalf.

As far as the timing, if automation is possible, the hope would be that this could be within a few seconds but if a manual review, as is likely to be the case in some of these 61f, same day response would be desirable and as much as we can refine that just because of the possibility that a network is down and thus, collateral damage is happening so time is of the essence.

The only other thing that I wanted to bring up was in Section P, the length of time that the data would be maintained. Usually, whenever there is a network-based attack, there is an after-action report that needs to be completed, a deeper dive. This is almost always happening after the attack is over, and usually, could be done within 30 days. Some of the really large attacks might be a

little bit longer but hopefully that level of data retention is not something that causes too much consternation. And that's it.

JANIS KARKLINS: Okay, thank you, Ben. So now it's time to raise questions, issues with the current use case. And I see a few hands already up. Let me start by Alan. Alan Woods followed by James.

ALAN WOODS: Thank you very much. And thank you, Ben, very much for that. I actually am one of the people who I appreciate this use case very much so. I think I don't get into the details because, again, as Janis said, that is for next week. I think there is some consternation with B in the sense of I think you're looking at it from the wrong point of view in the sense that you're looking at it from what the point of view as a requester as opposed to the actual processor, or the controller – sorry – who would have to look at that. It's a lot easier of a balance for us, probably, in the instances that you were describing to work through 61f in that [inaudible] and the very, very straight-forward 61f where it's harder for us to prove the necessity of a 61e on that one.

What I want to say – sorry, that was an aside – very much so about the policy, specifically the policies that we can pull out in looking at this use case and going back to things that the [inaudible] are trying to look for as well in our letter. And in particular would be, I think James just said this in the message, is about the urgency. Just because something is under a 61f, it doesn't mean that it has to be slow. And I think one of the

important aspects that we need to put into something like this is that the urgency of the request is something which should dictate the response as well, and the speed of the response. So there could be different buckets of urgency, which this sort of a thing, whether there's an imminent threat to the infrastructure of the Internet itself, such as the SSAC is set up specifically for, should be put into an urgent bucket and should be looked at [inaudible] other ones which are maybe less urgent [inaudible]. So I think that's a very, very important [inaudible] policy point that [inaudible] taken, but one of the separating elements that has been pointed out by this very good use case is that of urgency. So thank you.

JANIS KARKLINS: Thank you, Alan, for your comments. Noted. Next is James. James Bladel, please.

JAMES BLADEL: Thanks, Janis, and I think Alan covered quite a bit of what I wanted to say. I just wanted to say kudos to SSAC for this particular use case. I think, folks, this is the closest thing we have to an easy homework assignment because this is the original purpose of collecting and displaying WHOIS data in the first place, back in 19-whatever.

But yeah, just also noting and echoing Alan that 61d makes me a little uneasy. 61f, I think is a slam dunk and just because something is subject to a use case doesn't mean it can't be expedited, particularly if it has a low volume incidence like the

types of attacks we're talking about when compared to other types of disputes. So thanks and I'll drop my hand.

JANIS KARKLINS: Thank you, James. Next is Brian. Brian King followed by Chris.

BRIAN KING: Sure. Thanks. I think this is a great use case and I appreciate SSAC walking through it. I think they did a nice job with this one. I might note that in particular for the cases, that we have noted here critical infrastructure, hospitals, those all sound like public interest things to me so 61e may be applicable as well. So just noting that. Thanks.

JANIS KARKLINS: Thank you, Brian. Chris Lewis-Evans.

CHRIS LEWIS-EVANS: Thank you, Janis. Yeah, just repeating what Brian said there. So I have slight issues with D. I think I'm [inaudible] on the other SSAC case as well. That legal basis is very limited in scope where someone's life or death is in imminent danger, and obviously, when you see cases like this, firstly looking at network then taking down straightaway when you're reacting. So a more applicable use case such as a public task may fit better at that point. So yeah, I mean as Brian said, that might need to be considered to be put in there. So that's just my first initial point. Thank you.

JANIS KARKLINS: Thank you very much. Any other comments at this moment? I see none. Can that be?

Let me ask or make a question or comment from my side. So listening to you and the previous case, so most likely, the network operator will be a private company and acting in public interest, preserving network or preserving network from being down. So the accreditation or let's say providing information that this is really a network operator and not somebody from the street who is asking the question, so if you could think further on this accreditation or a system which would provide comfort to data possessors, disclose the information very quickly, that they do not need to make a search on who is the requester and why a requester is making this request. There are simply more systemic issues that need to be talked through, also thinking about the previous case.

So with this, Ben, I am turning to you.

BEN FULLER: Thanks. It's a point well taken. We'll spend some time thinking about how accreditation might be possible [even if it] is and thanks everybody, for the comments. I just wanted to reiterate that it would be extremely helpful for anyone who has comments or who made comments in the queue to please edit the Google Doc and put the comments in there so that we can make sure to catch all points and hopefully address them to everyone's satisfaction.

JANIS KARKLINS: So thank you, Ben. So it seems that we are at the end of today's meeting agenda. So let me raise one issue under any other business, and that is in preparation for the Los Angeles meeting, I suggested that we would invite CO to discuss issues of mutual interest and in this respect, I received a very positive feedback and it seems that there is a general interest in talking to Göran during our presence in Los Angeles.

So in order to structure the discussion and maybe better prepare that discussion, it would be useful to draft whatever questions we would like to raise. That does not exclude that any other questions could be raised during the conversation with Göran and we would schedule sufficient time for that conversation. So in that respect, I asked staff to put up a Google Doc with a few initial questions that stand out from the notice and I would like to ask everyone to contribute to that Google Doc with whatever questions you would like to put to Göran.

So with this, I see Brian's hand is still up. Brian?

With this, I would like to draw a conclusion to this meeting. Please send comments on the SSAC 1 use case by tomorrow end of the day, that they could be incorporated in the document prior to the next reading next week.

So next week, we have three meetings, two scheduled, one extraordinary. On Tuesday, Legal Committee will meet and continue examining legal questions, hopefully presenting them for consideration of the team on Thursday during the regular meeting.

So regular meeting will take place on Tuesday at 2:00 P.M. and agenda will be circulated on Monday. We will go through use cases. I think we still have a few of them to cover and then on Thursday at 8:00 P.M. UTC, we would have extraordinary meeting, hopefully not [inaudible] long in order to collect reactions on the zero draft which we would intend to publish on Tuesday, 27th of August.

So with this, I am looking once again if there is anyone from the team wishing to take the floor at this stage. If not, then thank you all for active participating in the meeting and this meeting stands adjourned.

ANDREA GLANDON: Thank you. This concludes today's conference. Please remember to disconnect all lines and have a wonderful rest of your day.

[END OF TRANSCRIPTION]