ICANN Transcription

EPDP on the Temporary Specification for gTLD Registration Data

Thursday, 25 July 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/iZZIDNbl4-9Lt9llAajPxTM_ZBG-xXI4OMwSX9JfcjtArq5ZlwDSAILNUGvY-U3a

Zoom Recording: https://icann.zoom.us/recording/play/A20jvkgs0R20hDJRA80-BVmNK7lgMak3VWmDZZBtzvdBfcFsInzRg8R6TukYcKdd?startTime=1564063224000

Attendance is on the wiki page: https://community.icann.org/x/l6ajBg

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

TERRI AGNEW: Good morning, good afternoon, and good evening. Welcome to the GNSO EPDP Phase 2 team meeting, taking place on the 25th of July 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 yourself now?

Hearing no one, we have listed apologies from James Bladel, RRSG, and Amr Elsadr, NCSG. They formally assigned Theo

Geurts and Stefan Filipovic as their alternate for this call and any remaining days of absence. Alternate not replacing a member are required to rename their line by adding three “Z”s to the beginning of their names and, at the end, in parentheses, affiliation-alternate, which means that 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 the chat, apart from private chat, or use any other Zoom room functionalities, such as raising hands, agreeing, or disagreeing. As a reminder, the alternate assignment form must be formalized by the way the of the Google assignment link. The link is available in the meeting invite e-mail.

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

Hearing or seeing no one, all documentation and information can be found on the EPDP wiki space. Please remember to state your name before speaking. Recordings will be circulated on the mailing list and posted on the public wiki space shortly after the end of the call.

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

JANIS KARKLINS: Thank you, Terri. Good morning. Hello. Good evening, members of the team. This is our tenth meeting. The agenda was proposed

and has not been objected to so far. May I take that as this is the agenda we would like to follow during this meeting?

I see no objections. We will then proceed accordingly. Item 3: housekeeping issues. Update on the Legal Committee. I know the Legal Committee met on Tuesday. If I may ask Leon to briefly inform on the outcomes of the conversation of the Legal Committee. Leon?

It seems Leon is not on the call. Barry, would you be wiling to brief us on the proceedings of the Legal Committee?

BARRY COBB: Hi, Janis. Just briefly, the call started out reviewing the prior session's question review. There were still a few outstanding action items on that previous set of questions, so we reconfirmed those and they'll hopefully be completed by the end of this week. Then we continued on, I think, starting at Question 6. I think there's a total of about 12 now. We reviewed through the remaining set of the questions. Most of them did require some revisions to further clarify the substance and nail down the scope. Additionally, I think that we'll be evaluating them to ensure that they do align with he needs of the EPDP Phase 2.

Then, certainly, what is on the near-term agenda for the Legal Committee is to try to attempt to understand all of legal requirements that the Legal Committee may need and begin to try to develop a sizing to understand what the overall request [inaudible] might be in preparation for requesting additional resources from the Board.

So I think that's it at a high level. Thank you.

JANIS KARKLINS: Thank you, Barry. Any questions on the work of the Legal Committee? For the moment, there isn't any outcome. Not yet. The next meeting of the committee is scheduled for the 6th of August.

I see no requests for the floor. Let us move to the next sub-item, and that is early input on the review. What's the status? Marika, if I may ask you tell us where we are now with this issue?

MARIKA KONINGS: Yeah. Thanks, Janis. As you all recall, we had a number of groups responding to the request for early input. That input was organized by staff, and an early input review tool was shared with the group a little while back. Based on discussions and on how to deal with that, the group agreed to, on the one hand, factor the input in as the group considers different topics in relation to the SSAD. Staff integrated that input into the worksheet for the SSAD.

In addition, the group agreed to put the early input review tool into a Google Doc form, which would allow the different groups to review that input and add any kind of clarifying questions or comments to that. that would allow for some further discussion or input as needed. The deadline for that is today. I just checked the Google Doc and I think, so far, now input has been provided yet. So no clarifying questions or follow-up comments have been provided by anyone yet.

JANIS KARKLINS: Thank you, Marika. If no clarifying questions will be submitted, then probably the next step would be for the Secretariat to simply try to factor in whatever comments the group has provided in the policy documents that we will be developing at the later stage of our activities. Is that the common understanding?

No objections? Then that is so decided. Our Secretariat will take all the inputs into account as appropriate when we will proceed with our work.

Let us move now to Item 4. That is use case categorization. As you recall, during the last call I asked the Secretariat, together with a group of volunteers, to work and then come to agreement on possible clustering of use cases. I know that the group worked rather intensely in a very constructive spirit. Now you see on the top of the screen the proposal that came out from that group of most interested team members. If I may invite Marika maybe to walk us through the proposal and then the volunteers to [chime] if necessary. Marika, please?

MARIKA KONINGS: Yeah. Thanks, Janis. As you noted, there was a small group of volunteers that agreed to work with staff on a new proposal. Where we started out was basically putting in one document the original staff categorization that the NCSG put forward, as well as the input that was provided by the BC as well as the IPC in response [to] the survey. So that went through a number of iterations and discussions within the small team on how to best

organize it in such a way that it would make most sense to review the use cases. I think it was discussed before. It's not the objective to eliminate any use cases or eliminate any categories in this way. The objective is to identify what percentages [per] category and, in each of those categories, try to identify the most representative case for that category and use that as a starting point.

Once, of course, we've then reviewed the most representative case for each of the categories, the group can then further review whether additional use cases need to be reviewed if they are due to represent a different scenario or result in different responses to the different questions or whether the group is [obligated] to do that and the case that has been reviewed and where the group has agreed on the different responses to the questions in the template, that those also apply to some of the other use cases that we have identified. So, again, that's the determinations that the group at some point will need to make.

Where the small team ended up is where you see here on the screen, divided into five different groups. Below you'll find the legend and the reference to the use cases as they were originally submitted. The first group consists of criminal law enforcement and national or public security use cases. Group 2 would be non-law enforcement investigations and civil claims. Group 3: the need for redacted data for third parties to contact the registrants. Group 4: consumer protection, abuse prevention, digital service provider, and network security use cases. Group 5: registered name holder consent or contract.

I do you want to know that the small team did not discuss whether the order that is represented here is also the order in which the use cases should be considered. I know there were some comments or some suggestions on how that might be best organized, but I just want to make sure that people understand that there's no specific order in that regard.

So I think this is what the small team has shared with the group. Do note that, in this version that you see on the screen, we've made a couple of minor updates. There was, I think, a mis-numbering in the IP use cases. Similarly, for the legends, I think we added a little description to the IP cases to make sure it was clear which one is being referred to.

Basically, those are the updates that we made compared to the version that was shared on Tuesday. I think, with that, I'll hand it back to you, Janis.

JANIS KARKLINS: Thank you, Marika. I would like also to place on record my appreciation to Milton, Margie, Brian, and Chris from the GAC for their very constructive engagement and agreement on this. I'm hoping the group would be in the position to go along with this proposal.

Now the floor is open for any questions if team members would like to raise at this moment.

If not – I do not see them – what would be the next step? My understanding was that the whole exercise of categorization was to help us to select in which order we would examine those cases.

The proposal would be now to do the survey and try to identify in each of the groups the most representative case that we would look at first, and then we would go through the average most representative case from each group. Then we would again start from Group 1, the second most representative case, and then that would be the order of our activities going through those cases. So that is the proposal.

I recognize Marika followed by Alan Greenberg. Marika, please?

MARIKA KONINGS: Thanks, Janis. Just to confirm, at least from a staff perspective, that that was our understanding as well as the next step. I think the one question that we have is, of course, we have already reviewed one case and Group 1. We're still doing that and we'll start discussions today on Group 2. So I think the question is, of course, we can still rank as well from Group 1 and 2 but understanding that, to a certain degree, we have already made a decision of where to start.

I think the other question is – again, I don't know if that's something people want to weight in on: the survey or the feedback that was made on the list. I think the suggestion was that, after Group 2, it would make sense to review the next case from Group 4 instead of going to Group 3 or 5. Again, that may be another question that either ask for input on or people want to weigh in. I think some people already expressed their preference to move from Group 2 to Group 4 as those might be closer related.

One thing I would like to ask the group as well is that I think from a staff side it's a fairly straightforward exercise to put it into a survey mode. Would it be reasonably and acceptable if we asked people to respond to the survey by end-of-day on Monday. That would at least allow staff and leadership them to build the agenda based on the input on the survey and have indeed the next use case basically first reading lined up for Thursday's meeting based on the survey results.

JANIS KARKLINS: Thank you, Marika. Alan Greenberg?

ALAN GREENBERG: Thank you very much. My understanding was somewhat different, that, partly due to the amount of time we have between now and the L.A. meeting, and partly due to the similarity of some of these cases, we were going to do a representative one and then go back and see if there are any issues associated with the other cases that warrant looking at them in particular and, if not, [do we] deem them to have been done because we've already done one that's close enough. So that's somewhat different than what you have been proposed. I can certainly live with either of those, but in terms of the timing, I'm not sure we have the time to do an in-depth review of each of them. Thank you.

JANIS KARKLINS: Thank you, Alan. You're right in the sense that we do not have time to review in-depth all of them. But since we would take the most representative cases and then, for the rest, we would take

maybe only the differences – what we can identify in those, let's say, grouped cases – and discuss only those differences or particularities of each of the cases …

I see no further requests for the floor. Stephanie? Stephanie, please go ahead.

STEPHANIE PERRIN: Thanks very much. I apologize for being tedious because I probably said this before, but as we go through these cases, I wonder if it would be useful if, before we start analyzing them, we map the stages that a compliant organization must go through as it determines whether a request for information is legitimate.

Let me give you an example. The first thing you try to ascertain is who is asking/who am I talking to? In this respect, the accreditation process and certificates that indicate that this is indeed a certified entity that is recognizable, that might have some purpose that could be valid solve that problem, or at least it seeks to solve it.

Then the next questions is, what data do they want/what scope? Then the next question is, under what authority are they asking? Then the next question is, do they have a request that maps? Then there's all the proportionality things.

So, basically, I think, in the absence of mapping the kinds of questions you have to ask when you determine whether to comply with a request for data, we chase our tails. We're running around in circles. People seem to think that accreditation means every

request from a given body is legitimate. Of course, that's not the case. Thanks.

JANIS KARKLINS: Thank you, Stephanie. I think you're talking about what I call building blocks. The left column of the use case, in a sense, is geared towards answering those questions, or at least providing the framework of our discussions. In reality, we're speaking about rather simple systems. We have, from one side, demand by a requester and then, from the other side, we have supply by the registrar or registry. Then we have some kind of interface in between. Then, of course, the demand side and supply side have those building blocks: exactly the questions you raised. We are going through these use cases. We're trying to understand and define of each of the building blocks. So at least that is the attempt from the Secretariat side when they proposed the framework that we're following going through those use cases.

Any other reaction?

I see none. May I take that as we could follow the proposal note that Marika made, that each group would look through and then file the survey, ranking the most representative case in each of the five groups and then we would take it in order of first, second, fourth, third, and fifth group and then we would look into other cases but looking in those specific elements that have not been addressed in the most representative case?

I see no – all the survey would be published today. The request would be to file it by the end of Monday next week. So that is our decision. Thank you very much.

Let us now go through the two cases that we wanted to go through. If I may propose, maybe we take it in the reverse order, that we would finish the final reading of the case/investigation of criminal activity against the victims of jurisdiction of investigating E.U. law enforcement agencies requesting data from a non-local data controller. We got to Point G last time, and there are a few other points to discuss. We would devote maybe 40 or 45 minutes to the final reading of this case. Then we would start the first reading of the next case on phishing attacks. That would be my proposal. It seems that there is no objection.

May I then ask to point the law enforcement case on the screen. So last time we got to Point G. our discussion on Point G was inconclusive. In the meantime, the registrars submitted a number of comments including also on the sub-sections that we have already discussed.

Chris, I would like to ask you whether you have any comments on those points provided by registrars from Point A to Point H, not touching Point G. Chris?

CHRIS LEWIS-EVANS: Thanks, Janis. Sorry for getting this out so late, but I did just send an e-mail to the e-mail group with the comments attached to them. We had a chance to very briefly discuss this yesterday in the GAC small group. I think the first substantial one is in Section C:

whether a registry group felt that only redacted data should be provided and not previously public or currently public data. I think I explained last time that I felt that it gives an increased level of accuracy to the body process [and] the data. Therefore the data [inaudible] of the data subject could then be processed better and with more accuracy.

So I think that's our reasons why. I'd be interested to hear what the Registrars Group's reasons are behind not supplying both the redacted and public data in one request.

They also suggested a change which I agreed with that would be good to update the document with. In Section D, they stated that obviously the requester also needs to indicate legal basis. That's done under E on the template.

Under Section E, they had some questions around whether the requester had authority to request that data and then whether the non-vertical controller was under other obligational [dispensation] to provide that data to a foreign LEA. Really here I think it comes down to this case where we're saying that on the requester it's under 61F because it's a request that's not based off of any legal paperwork or anything. So it's not a 61C. Therefore, there's no compulsion on the disclosing body to release any information. That obviously needs to go through all the appropriate safeguards and obviously whatever process we recommend on this. So I think that was our comments on that.

With F, we agreed with the suggested change. After that, we obviously get to G, which I think we are at the moment.

JANIS KARKLINS: Thank you, Chris. If I may ask you, once you'll be taking into account all the comments that we team members provide, would you then also incorporate the registrars comments also in the very final version?

CHRIS LEWIS-EVANS: Yes, of course.

JANIS KARKLINS: Thank you. Let us now go to G. I open the floor for any comments or questions that team members would like to raise in relation to Point G safeguards.

Alan Woods?

ALAN WOODS: Thank you. I'm going to jump straight in and take a look at what the registrars put in as well and their suggested inclusion. That is that the disclosing should have any additional safeguard: that they must be enabled to verify the legal authority of the LEA to make the request.

I'm going to bit controversial here, and apologies to everybody on this. If we were making a decision under 61F and we have to say an LEA comes to us and says, "I have the legal authority to do this," unless that LEA established what that legal authority is, to me that would be actually a bad thing for a 61F balancing test because it's not up to us. We were not legal authority experts on

this end as controllers. It would really be up to the LEA or somebody in the middle, as we're looking to actually verify that and to confirm that's verification.

So I would change it ever so slightly in what the registrars are saying. I don't think that we must ensure that the LEA establishes the legal authority themselves. It's very important that this comes from LEA and it comes from that aspect and that we are not making a decision on whether or not a particular law is applicable to them in a certain situation because that's just not within our remit. So I would say there needs to be some caution there.

JANIS KARKLINS: Thank you, Alan. I see already the comment from Chris in the last e-mail, that that may be [why] accreditation or authentication methods … Any further comments on Section G?

I see none. Shall we go then to Section H: safeguards applicable to requester in a potentially automated access disclosure system? Any comments?

I see Chris's hand up. Chris?

CHRIS LEWIS-EVANS: This was just to clarify [things] on the comments from the registrar group here. As I remember rightly, we obviously didn't have this in one of the earlier templates. I think it was suggested in an earlier call that we add safeguards under an automatics system because, at some point when we get to discussing whether this is

viable or not, the safeguards under an automatic system may be different.

So I think this was put in here to get the template ready for once we've had that discussion around how an automatic system would work and if it at all it's viable. So really strictly that's why these were here. I think that hopefully answers the registrars' question on that, unless I'm remembering wrong, of course, of why they're in here.

JANIS KARKLINS: Thank you, Chris. The floor is open for discussion of Section H.

No comments? Everyone is in agreement about this proposal's safeguards? It seems to be the case. Then we can go to Section I.

Any requests for the floor? Questions/comments on Section I?

At this speed, we will finalize this case in five minutes. I see no requests. Okay. Then we can go to Section J. I think this will be the first time when we will have a conversation about accreditation. So far we have not discussed that at all.

I recognize Chris. Please go ahead, Chris.

CHRIS LEWIS-EVANS: Thanks. Just again to answer the question already proposed [inaudible], I can see there was a bit of confusion on this. I think this, again, is because it's a bit of a chicken-and-egg situation. As Janis has just said, we've not really discussed accreditation yet. It's very much dependent on a standardized system.

Going from the other comments throughout the response that they've given, I think adding here a jurisdiction and legal basis – what would come under Section E in the template – would be certainly necessarily for an accreditation body maybe to be looking at. So that's certainly what I'd want to add there. Thanks.

JANIS KARKLINS: Thank you, Chris. Any requests for the floor? Now I recognize Hadia. Hadia, please go ahead.

HADIA ELMINIAWI: Hello. I would like to talk about this accreditation part because my understanding is that there's a difference between validation and accreditation. I think that we need first to have validation and then accreditation. Or are we thinking now to include both together? So this is a question. Because, generally speaking, I think that validation could have different forms. It could be automated or non-automated. Then you have the accreditation part, which could actually be fully automated. So this is more of a question. Are we talking about both?

JANIS KARKLINS: Thank you. So we have now a question from Hadia on whether we are talking about validation and accreditation or if we're talking both.

Next is Marc Anderson.

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

JANIS KARKLINS: Yes. Please go ahead.

MARC ANDERSON: There's a lot of interesting things in this particular one that I think are worth spending a little bit of time on. I think the first item there, the first bullet point, talks about the accreditation of user groups seeking access. We talked about this in some of the earlier sections. We touched on this in some of the earlier sessions, and Alan I think had a good intervention on this point: having a mechanism to accredit a user group. In this case we're talking about law enforcement outside of their jurisdiction. Having the ability to accredit the person requesting the access [to confirm] they are in fact who they say they are I think is really important. The use case is pretty [wide], so I think this could be fleshed out a little bit more.

The next [inaudible]. I raised my hand on this one. It says, "Dependent on implementation of the standard system." I just want to say that, even if we don't end up with a centralized standardized system, there would be a lot of value in having the ability to accredit particularly this particular user group but many user groups. How that accreditation occurs may depend a little bit on the system that we ultimately recommend in our policy recommendations. I'm not saying there aren't dependencies, but I just wanted to make the point that this doesn't rely on there being a standardized or centralized system. Even if it's a decentralized

system, there would be a lot of value in having an accreditation system in place.

I think the code of conduct part is interesting. I'm not sure this is the right place for it. [inaudible] having a conversation about code of conduct. Correct me if I'm wrong. I'm not sure that that's part of accreditation. I think that's maybe a different category all together.

The sub-bullet point there on non-disclosure audit information to a data subject whilst part of an active investigation. We've talked about this before. I think this is a very important point. I think this maybe belongs more in the safeguards section. Again, I don't really see what that has to do with accreditation. I think that belongs in the safeguards section where we deal with disclosure or non-disclosure to the data subject.

So a couple points there. I think this is a great conversation for us to have.

JANIS KARKLINS: Thank you, Marc. I think, when we're talking about a standardized system, we can imagine that the same standard may be centralized and the same standard may be applied in a decentralized way. So I personally do not see there may be only a standardized centralized system. Maybe there could be also a standardized decentralized system.

Also, when we are thinking about accreditation, we can think of accreditation by different existing entities, whether existing extraterritorial entities or existing entities in certain jurisdictions.

We can think of creating a special entity for accreditation of one group or accreditation of many groups.

So I think that there are a number of options that we could contemplate. But of course, first we need to see whether we're in broad agreement that accreditation as a principle should be introduced in this standard or not. That's the beginning of our conversation.

I recognize Milton. Milton, please go ahead, followed by Mark Sv.

MILTON MUELLER: Hello. Yes, this section is very important and also very bare and not really filled out, and there are a number of thorny issues. But one thing I think we can [inaudible] up is Hadia's discussion of validation. I think what she means is authentication which is covered in Section K. Once you have established a system of accreditation, then you can determine whether an accredited party is who they say they are, which is what we call authentication and is what I think Hadia means by validation. So we obviously have to deal with accreditation before we deal with authentication, because otherwise you have no basis for authenticating.

I think that the main point I wanted to raise here is a really thorny one. I'd be interested in hearing the opinions of the GAC members on this. It has to do with authoritarian governments and the kind of human rights protections that, for example, we're trying to achieve in the cloud, which involves data sharing among governmental entities.

When we can indeed accredit, let's say, a Turkish law enforcement agency as a legitimate law enforcement agency but at the same time they're national law allows them to investigate and harass people for criticizing the government – I don't want to pick on any particular country here, but you know that there are authoritative countries that have laws like that – how do we handle that? Do we want to simply have a very flat and simple "Yes, you are a state law enforcement agency," or do we want to have additional human rights protections related to who gets accredited? That's the question that I'm raising. Finished.

JANIS KARKLINS: Thank you, Milton. It's an interesting question and probably not a trivial one. The question is whether this is the right place to in general those questions. Of course, that's very much related to the accreditation as a concept.

I have Marcus Sv in line, followed by Alan Greenberg. Mark, please?

MARK SVANCAREK: Thanks. I agree with Milton that what Hadia called validation sounds like authentication, which is Section K, which is blank in this document. But I guess that's okay for now. I agree with Milton that we should discuss accreditation before authentication. I can think of one case where you might be authenticated without being accredited. That would simply be a non-accredited body doing 61F requests who doesn't want to get block listed because of

volumes. But I don't think that that case justifies not doing accreditation first.

I agree with Marc Anderson that I cannot think at this time of any policy implications that would lead to a different scheme of accreditation. I just can't, so I'm not sure that that bullet needs to stay in here. I would welcome feedback from Chris to explain that.

I think that's it from me right now. Thank you.

JANIS KARKLINS: Thank you. Alan Greenberg is next, followed by Alan Woods. Milton, if you could take your hand down.

ALAN GREENBERG: Thank you very much. Just a brief intervention. I really think we need some written definitions of these terms. People are using them in somewhat different ways, and I think we could avoid that by putting something in writing. Particularly for accreditation, there's really two different aspects. One is accrediting a class of people – I won't say a group but a class of requesters – to use the system if it's an automated system or to be identified as a certain class that will be treated perhaps differently in manual requests. Then the second part is accreditation of individuals to be part of that class.

So we might say that trademark attorneys are going to be given certain privileges in general, and then any individual has to demonstrate that they are in fact a trademark attorney and give the certifications that they'll follow the rules and things like that.

So I think we really need to go back and draw up some definitions to make sure we're all talking about the same thing. Thank you.

JANIS KARKLINS: Thank you, Alan. I would like to refer you to the Chair's working definitions. Accreditation was one of the definitions that we agreed at the early stages of the work of our team. Marika has copied the definition in the chat room. Please [inaudible]

ALAN GREENBERG: Then I stand corrected. Thank you.

JANIS KARKLINS: Thank you, Alan. Alan Woods next, followed by Ashley.

ALAN WOODS: Thank you, Janis. When it comes to this accreditation and that we now have the opportunity to have this conversation with regards to accreditation, I think, just going back to something you said about whether or not there may be different accreditation bodies as well, this is a very important point. I think, specifically in regards to the LEA one, we need to be very careful. I think this is possibly a line-in-the-sand moment for us as a working group because I don't think that the accreditation body is something that we necessarily need to define or create or something like that.

Specifically in the LEA, that is up to – again, sorry Chris, but I've had this conversation with them -- law enforcement to come up with some way of ensuring that when they come to us they can

say that we have been accredited, and not only that they have been accredited in some way that is meaningful but also that they've been accredited by something that's been accepted, not only by us. Likely, I would ask them to go to people like the European Data Protection Board and say, "For the purposes of this, is this is something that you would accept as an accreditation that we can bring to, say, the contracted parties or the SSAD?" because, again, we are not capable of defining this accreditation. We are not ever going to be able to determine what the accreditation requirements are here. That should be up to the individuals who wish to be accredited to define what the accreditation for them, for their industry, and for their stakeholder groups would be and then come to us and say, 'Hey, we've got this accreditation. It hasn't been approved in a way that seems to be deemed acceptable by local data protection authorities or indeed the European Data Protection Board." Then we can say, based on that, we're happy to accept that as an accreditation for that.

I will briefly step in and say on the validation part on indeed on the authentication part that I think specifically with regards to law enforcement that is a very important thing that they need to look into as well because the requests that would be allowed via that accreditation or allowed as part of the accreditation for law enforcement would have to take into account some form of verification of the validity and the suitability of that request for a request for data release in that particular instance.

So, as Milton was saying, when the authoritarian regime applies for accreditation, they might get the accreditation, but in order to

prove, this accreditation body should also have possibly a validation saying, “No, this is not a proper request being made because A) it’s not considered to be universally an illegal act that you’re trying to do or it’s absolutely frivolous in the situation such as” – I believe, going back to Thomas Rickert’s points, we don’t want to be releasing data just so that they an enforce a parking ticket.

Things like this are very important, but again, it’s not up to us to define that. it’s up to law enforcement and the coalition of law enforcement people to do that and bring it to us. I think we need to shy away from trying to define every single aspect of this.

JANIS KARKLINS: Thank you, Alan. I think that half of your statement, if we would capture that [verbatim], would represent the policy statement. This is what we are working on. Of course, it is not up to us to define the modalities of accreditation, but it’s up to us to suggest that, as a policy matter, there should be accreditation, and accreditation should ensure certain aspects/points. Then we may want to list those points. Again, it may be too premature, but in principle I think your intervention very much sounded to me like a policy recommendation already.

Ashley, followed by Stephanie.

ASHLEY: Thanks. Can you hear me?

JANIS KARKLINS: Yes. Please go ahead.

ASHLEY: I just wanted to respond, I think, in part to some of the concerns that Milton raised and also wanted to concur with just about everything that Alan Woods just said. I think what Milton is articulating actually is broader than just government and law enforcement. It sounds like more like potential misuse of the information received. I think that a lot of those types of concerns can ultimately be addressed in things like terms of use and enforcement of this terms of use. From a policy perspective, I think, looking back at what we can do, it's just noting that it's important to address these types of issues in the terms of use and ensure that there is strong enforcement of those terms.

I'm not sure that addresses all of Milton's concerns, but I think, from a high-level perspective, this isn't something just specific to law enforcement. It definitely would exist there, but I think there's ways to address it in, I think, very realistic and not-so-complicated ways. Thanks.

JANIS KARKLINS: Thank you, Ashley. Stephanie, followed by Chris.

STEPHANIE PERRIN: Thank you. Once again, I apologize for reiterating the point that I made earlier. I originally raised my hand to respond to something that Alan Greenberg had said. It relates to this whole discussion about how you deal with requests from accredited entities. I would

suggest once again that there are separate processes here. The mere fact that someone is a bona fide law enforcement agency with powers under this or that legislation, which is hopefully part of the accreditation process, or a bona fide trademark lawyer with a likelihood of having legitimate requests under this or that trademark law, or a UDPR provider – I have to say that this is the one that I think comes closest to meriting some elision of the processes here – basically, the mere fact that someone is accredited does not mean they have a valid request.

For those of us who've actually worked in this field, I can assure you that closing the barn door after the horse is gone is no good. You have to interrogate a request from a policy officer to make sure that it's not some rogue guy looking for his ex-wife's address so he can go and kill her – actual case – or a guy who's looking up everybody who's shown up at an abortion clinic so he can counsel them against abortion – actual case. There's a responsibility on the part of the entity releasing the data to interrogate the request. I'm stumped as to how you automate that in any meaningful way. I realize we've accepted that point. But if we've accepted that point, then let's not keep eliding them and trying to do, after the fact, best practices.

So I think, full-stop, somebody is accredited? They're a law enforcement agency. Hopefully the accreditation will say under what authority they can seek data. That you can automate. But the actual request? No. Thanks.

JANIS KARKLINS: Thank you, Stephanie. As I noted, Ashley wrote in the chat that we agreed already that accreditation does not assume automatically access.

I have further requests from Chris, followed by Hadia. Chris, please go ahead.

CHRIS LEWIS-EVANS: Thanks. I just wanted to respond to both remarks and [inaudible] points, which are put in the chat. I agree with lots of those. Really, this is a holder because we've not yet had the discussions at any good level to start coming up with what I felt was needed to go into this template.

I still do feel it is slightly dependent upon implementation of a system. I think, when I wrote that – I'm not even sure at the moment that we've got agreement that there needs to be an accreditation body or if it's a number of bodies or if each registrar and registry needs to accredit every single user it's doing a request from. So I think that's where that line came from: how does that work? Is it that every single contracted party has to act as its own accreditation body? As [inaudible] point earlier, really. I don't see it being feasible for them to accredit a law enforcement agent outside of their jurisdiction or maybe even within. If you look at the number of law enforcement agencies even just in the U.S., it gets a little bit crazy and not really part of their role.

So I think, if we can come to an agreement about – it would have to be a third party and then, [in that case,] would it be a standard

body? Would we do it at a country level? I think that would help with some of the decisions that we're making on how it's done.

Coming back to Milton's point about being able to apply the correct safeguards and whether that's done, both at the accreditation and the authentication level, it's probably that a decision that needs to be made. I'd still like to use Thomas's beer belly question from before because I think that's a good way of phrasing it. Tight controls get in and then there'll be big cases and then smaller cases at the top as well that get [inaudible].

So that was just what I wanted to add. Thank you.

JANIS KARKLINS: Thank you, Chris. The last on the list for the moment is Hadia.

HADIA ELMINIAWI: First I would like to agree with Stephanie that definitely accreditation is something, and the decision-making process is itself is another. When I was actually thinking of validation, I was thinking if it was going to be automated. If we are talking about if we are talking an automated accreditation process, with no human intervention, if you are accrediting organizations – for example, like law enforcement organizations – well, that could be done automatically, I think, easily. But maybe if you're talking about other types of organizations, it might not be that easy to automate the whole process. You might need some sort of validation to the user group in a non-automatic way before you're able to accredit it.

I understand what Milton said and others said, that authentication is the same as validation, but again, I was thinking of a fully automated accreditation process where the organization submits the documents or whatever online, and the decision for accreditation is automated. Well, again, maybe for some organizations, it could be easy to fully automate that. But with other organizations, maybe not. Maybe you need some kind of human intervention along with the automated process.

So there is the accreditation, which involves some kind of validation to he organization that you are accrediting. My understanding is that this is quite different from authentication. And then you have the decision-making process. So you have the accreditation, the authentication, and you have also the decision-making process. Again, you can have an automated accreditation process or a non-automated accreditation process or a mixture of both automated with some kind of human intervention accreditation process. You can have the authentication process and then you have the decision-making process. The decision-making process, I think, in many cases could be really automated. Again, maybe the whole thing would be automated. The whole components of the systems are automated, but some parts of the system could be automated.

Then, of course, there is another issue of no everyone would be accredited, like not all organizations or all user groups would be accredited. Definitely in that case you have the validation or authentication, and then you have access to the information.

So, again, I'm not quite clear. I'm not sure if others said that maybe we don't need to go too much into details, like defining clearly each of the terms. Maybe that's an option, too. Thank you.

JANIS KARKLINS: Thank you, Hadia. Of course, this is the first conversation. There is a lot of uncertainty and points that we need to better understand ourselves before we get to any kind of agreement.

Let me just take very quick interventions from Mark Sv and Alan Greenberg again, and then we will close this conversation on this part of the section for the time being. Mark Sv, please?

MARTK SVANCAREK: Thank you, Hadia, for the opportunity to pedantically debate issues of taxonomy and terminology because that is really in my wheelhouse. So I'm grateful for that.

I think, earlier in Phase 2, we had introduced into the glossary a term called authorization. The accreditor would attach privileges, say, to the accredited body, and they would get credentials somehow for logging in that demonstrates that they are who they say they are and that they are in fact attached to those privileges. Authorization is the decision process, whether automated or otherwise, that allows them to exercise those privileges in the context of that request.

So I think we do have a term for that. It just has been list in the mists of time.

JANIS KARKLINS: Thank you. Alan Greenberg?

Alan Greenberg, please?

ALAN GREENBERG: Sorry. I was muted on Zoom as well as locally. I think the last two interventions that we've had – or maybe more than a few – indicate that the one-sentence definitions and the Chair's definitions are not sufficient. I would strongly suggest that we try to flesh these out with a lot more detail before we have another conversation like this because I don't think it's productive to have people talking on at length when clearly they're using different interpretations of the meaning of some of these words. Thank you.

JANIS KARKLINS: Thank you, Alan. Actually, you took the words out of my mouth. I wanted to suggest the following. So accreditation certainly is an important building block in the standardizes system, and we probably need much more time to discuss it. I understand that, in early inputs, some groups have provided their understanding of accreditation.

If I may ask, for the next case that we will be looking at on the next call or most likely after two weeks, that staff put together a compilation from everything that has been submitted on accreditation, authentication, and related processes. That maybe will help us inform our further conversation on this fundamental

building block. If that would be acceptable also from the staff side, then we could go to Point L.

Marika? Let's hear a positive answer.

MARIKA KONINGS: Thank you. Just to say I think we've already basically done that because, I think – although I think in the charter question it talks about [inaudible] authentication/accreditation. It talks about credentialing. So I think that input is already all grouped together. We've also inserted that as such in the SSAD worksheet. If there's anything we've missed that may have occurred in other sections, we can definitely have another look, but in principle, whether the input is all organized/in line with the charter questions – in fact, there was one of those charter questions specifically addressing the credentialing, which I think fits this category or authentication/accreditation/validation as a more generalized grouping.

JANIS KARKLINS: Thank you. It's even better that it is done already. Maybe, the next time the issue of accreditation will come up, it would be useful to pull out from the worksheet just that particular section and put it on the screen so we have a better grasp of the complexity.

L. Any questions on Section L?

No comments for the moment? Stephanie?

STEPHANIE PERRIN: Sorry to slow us down, Janis. Would you mind popping up the definition of credentialing on the screen? Because I think that this concept of credentials, if we're not really careful, actually performs, through the use of a technical terms and possibly the definition of a technical term, the elision that I had been warning about all morning because we have borrowing that from a technical use of the term "credential." Here we need to think in terms of policy. The token that you get that indicates or provides a "credential" that you are indeed the entity you claim to be and that you have the powers that the system acknowledges those entities do, which are based on law, does not mean that you have a credential to get access to a particular type of data. Thank you.

JANIS KARKLINS: Thank you, Stephanie. Yes, this is the charter question, as Marika said. We most likely were bound to answer those charter questions, but of course, the term credentialing encompasses a few steps. It's just a generic term. If I may suggest that we would come back to that in a more systemic way, a more structured, then we will be looking at the next case, where the sub-section of accreditation will be also present. If you don't mind, Stephanie. This is well-noted, and this is not really a trivial issue.

No comments on L? On M? This is very operational. It seems everyone is in agreement. Seconds or two business days? Alan Woods?

ALAN WOODS: I'm assuming that most people from the CP point of view have thoughts on this one and feelings. If this is part and parcel of the SSAD, this is a system that is being created, and when they create this system and, depending upon what it looks like, they believe this can be processed, depending on what the policy says and two days seems to be something that they can turn around on, then good for them. But if we are still getting down to a more specific individual CP review of this sort of a thing, then it's really up to the LEA to point out where there is an urgency in this particular instance. I think it makes sense that, in certain instances, depending on the individual case, that a specific, quick turnaround might be necessarily in order to prevent a specific crime or harm to anybody in an instance. But saying two days across the board is kind of ridiculous, to be perfectly honest, again because this is the whole problem that we have. I understand where Chris is coming from, and I definitely think from an LEA point of view we can work with that, but I just want us to set this expectation that two days makes sense, that we can just turn around these things in two days in all cases. So I'm just going on the record.

JANIS KARKLINS: Thank you, Alan. Every government, no matter question a citizen would ask, would tell, "You would get your answer, in the best case, in two weeks." So that's the standard speed of any government in answering citizens.

Mark Sv please, followed by Theo.

MARK SVANCAREK: A couple points. I think there's always been a problem with this template between M and O. There's the concept of a response in acknowledgement of the request, and then there's been a response whether or not the data is going to be delivered, and then the actual delivery of the data. So acknowledging that a request has been delivered – we'd like to see that SLA be very compressed.

Second thing. I mentioned in BC1 and BC2 that whatever system we come up with does need to accommodate the idea that some requests have higher priority and that some requests require different levels of confidentiality. So just keep that in mind as we develop our policy: whatever mechanisms we set up have to accommodate those concepts.

Lastly, to Volker's comment, I do recognize that, if you have a lot of requests, it's hard to process them all in time. But I would also like to put forward the controversial position that, if you have a lot of requests, you're going to need to staff up. So it's not just a one-sided thing. Thank you.

JANIS KARKLINS: If I may ask the Secretariat and also Chris – for me all are identical – just check whether there is a mistake on the left column or if this simply is a mistake of copy-paste in general.

I have Theo next. Theo, please?

THEO GEURTS: Thanks, Janis. Just a housekeeping point. Like my registrar colleague, [Matt], pointed out, we will be replying on several points made earlier. He put it out in the chat. Just in general about a lot of these points here, we are not commenting. This is going pretty fast, so we'll get back to it on the list, I guess. There's a lot to process here. So do not take silence as complete agreement. Thanks.

JANIS KARKLINS: Noted. Thank you very much. Now Chris, Chris, please.

CHRIS LEWIS-EVANS: Thanks, Janis, and thanks to Alan before. Realistically, let me explain a little bit why went down this way. Obviously, as Alan says and maybe what [Jess] has said, I think maybe M and O should be different – expected timing of acceptance and expected time of substantive response as the second. But realistically, going to the level of requests, this is just for LEAs. As most of you have commented, that level of request is generally lower than across other user cases. So we feel that two business days plus some time with a response on top – we could talking about four business days there. That's more than reasonable. If we come to you with a silly response or a silly request that you turn around and say, "We can't possibly do that in X number of days," at, then that's something that we'd always listen to.

I did separate them out, so I don't think two businesses days would be an SLA, but I think certainly [inaudible] that we would

want to achieve because, effectively, in this user case, we're talking about a crime in action.

So that's our initial thoughts around why that timing on this. But we'd certainly be prepared to see what your responses are once you've had time to consider. Thank you.

JANIS KARKLINS: Thank you, Chris, for this clarification. It's obvious that, in other cases, most likely we may except different suggestions in the right-hand column on the question of what's the expected response time.

I have a new hand of Mark Sv. Please go ahead.

MARK SVACAREK: Thanks. Volker makes a comment that we can't apply GoDaddy standards to all of us and that different entities are staffed differently because they're different sizes of business. That's very, very true.

My analysis of the names that Microsoft looks at is that this is a very long tail data set. By "long tail," what I mean is that, with people like GoDaddy, we look at names associated with them many, many times a day, but we'll looking at tens of hundreds of thousands of names, and many registrars are going to have one request – one request per day, one request per week. I think that is in line with the size of their businesses. So it's not as thought very small businesses will be subject to thousands and thousands of requests per unit time. That seems, at least on the face of it,

unlikely. So I think there's a natural balancing that occurs. If you're very small and you don't manage a lot of names, you're not going to have a lot of data request, unless, of course, you are a bad actor who is encouraging the bad activity on your name. Those are very, very few. There are not so many of those. Thank you.

JANIS KARKLINS: Thank you, Mark, for this comment. Look, I think we got a rather good sense of these questions as well. As I mentioned, most likely the answers will be different in different cases.

Let us know for the moment put this aside and continue with N: Is automation of a substantive response possible or desirable? In this particular case, the answer is yes.

Any comments or disagreement?

I see none. Let us now move to Point P: How long can the requester retain data disclosed, and what are the requirements for destruction following the end of the retention period?

The floor is open for any comments or questions on this particular point.

Alan Greenberg, please?

ALAN GREENBERG: Thank you. I'd actually like to go back to N. I was a little bit slow on the draw here. I guess I'm hearing two different things from different people. By saying yes here, we're saying automation is possible, which means the decision is going to be automated. Yet

we're hearing substantial people in this group saying it's never going to be possible to automate the decision.

I'm happy to defer the discussion, and I'll note I have posed a question to the Legal Committee that focuses just on that: Is it ever going to be possible to have an automated decision? So I'm happy to defer it, but I just wanted to note that there is a discrepancy by saying the decision can never be automated and yet we can have an automated response here. Thank you.

JANIS KARKLINS: Thank you, Alan. Noted. Kristina?

KRISTINA ROSETTE: Thanks. A similar point to Alan's. I'm a little confused as to how the determination was just made that there was no disagreement when the registrars had submitted comments indicating that they did not agree with that response. Chris, in his response, said, yes, it's worth discussion.

So I think we're moving a little too quickly here and not taking into account all of the information and input that's been provided. I think we need, particularly on this point, to step on the breaks for a minute and just make sure that we're taking into account all of the information that's been received. Thanks.

JANIS KARKLINS: Thank you. Stephanie?

STEPHANIE PERRIN: Thank you. I think that, not to go further on Alan's point about expanding our definition, it depends on what you mean by "automate." As somebody who has processes these requests, not specifically the WHOIS requests but requests where you have quite a few actions to perform – who is it, how do I know that's who it is, what powers do they have, how do I know that, who certifies that they have those powers, what's the track record, what's the star rating of these guys? – let's not trivialize how much work automation can do. It can all of things up to analysis of the precise request.

There may be instances, which I'm busy racking my brains for to comment on the Technical Study Group's excellent paper, where some data fields could be released safely to bona fide parties, not necessarily the very sensitive data such as address and phone number. But pattern analysis, for instance, could be managed in this way.

But the thing is, people seem to think that automated means all the way to the finish. Automated may just take 80% of the workload out. It would still be useful as long as it's affordable. Thank you.

JANIS KARKLINS: Thank you, Stephanie, also for bringing your hands-on experience. I think that this is also very important to know from a practitioner: how long that may take, what is possible, and what is not. Thank you for that?

Alex Deacon, followed by Alan Greenberg.

ALEX DEACON: Thanks. Hi, everyone. I just wanted, on this topic of automation, to, I think, echo something that maybe Marc Anderson mentioned earlier, which is that all of the details that we're discussing in these use cases and in the template I think are relevant and can be used and are important, whether automation is important or not or whether automation is possible or not or whether we decide to automate or not and how we decide to automate in the future.

So I guess I caution us not to get too deep into the weeds on this topic now. It is important, but I think we should focus on the job currently at hand, which is walking through these use cases, answering these questions as best as we can. I think, as we do that, we could set up a time in the schedule to further discuss automation and then, of course, things we discussed earlier – accreditation and the like – which are all important. I just want to make sure we don't get too distracted for this and we continue to make the good progress that we've been making. Thanks.

JANIS KARKLINS: Thank you, Alex. I think that you're absolutely right. This automation, if I'm not mistaken, is also one of the charter questions, and certainly it is one of the building blocks that we need to discuss and develop. Here's exactly the same thing. If I may ask the Secretariat to pull together whatever has been submitted on the issue of automation and put that on the screen when we look to the next case next week or a week after. Then we could have a more substantive discussion on issues relating to automation, keeping in mind also this particular case. If that is

okay, then I would ask Stephanie and Alex to take their hands off and Alan Greenberg to speak.

JANIS KARKLINS: Thank you very much. I'll just note that N says automation of substantive response, which I take to mean that the actual data that is being asked for is given. The only data that is redacted are names of the organization or entity and contact information. So there is nothing that we deem to be non-sensitive information that is redacted.

So, yes, of course, some parts of this process are going to be automated no matter what we do. No respondent is going to know the names of everyone in the world and their rights. We're going to have some level of automated systems and lookups to identify who is accredited, who is not, and if you're really Janis Karklins or not. But that's not what we're asking here. thank you.

JANIS KARKLINS: I am. I can testify to that. Sorry, I'm trying to joke.

ALAN GREENBERG: But how do you prove it?

JANIS KARKLINS: Look, now I will give the floor to Chris and then I understand that no one wants to speak on Point P. Chris, please go ahead.

CHRIS LEWIS-EVANS: Thank, Janis. Just listening to Alex there, maybe a suggestion for the template is to remove the word "possible" and leave "desirable" because that will stop us getting drawn into automated discussions on every single user case. We can push that to another separate discussion. Thanks.

JANIS KARKLINS: Thank you, Chris. Actually, that is also in your hands because I would like to ask you, based on previous conversations, registrar submission, and what you hear today to maybe try to fine-tune the case for the record because we can imagine those cases will in one way or another attached in an annex or annexed to whatever policy document we will come up with as supporting information.

So on Point P …

No comments on this particular case? Marc Anderson?

MARC ANDERSON: Thanks, Janis. I'll just comment on this real quick. I think, in the protections section, we provided a little bit more information as far as how long retention could last, particularly around the requester. I think it was a little bit more clear there for me in early sections. The language in P is maybe less clear. I guess maybe this is just feedback for Chris. I would suggest you use the same language you used in the previous section around retention. I think it's clear from this use case that there's no blanket answer. You can't say with certainty at all that it'd be two years, two weeks, or two months. It's going to vary depending on the particular case. I think

you did a much better job explaining that in earlier sections. So just a little bit of feedback for you there.

JANIS KARKLINS: Thank you, Marc. In absence of further requests for the floor, I suggest that Chris would continue based on inputs fine-tuning the case and produce an updated version. We would then post the updated version on a Google Doc or the website. Sorry, I'm not sure exactly where. Marika may say where. Then we could probably suggest that the last reading is by e-mail exchange while we're working on other cases.

Marika?

MARIKA KONINGS: Thanks, Janis. I think the question is, before now, we've been posting all the use cases on the wiki page, as they're more static documents for the different groups to review. I think the questions is, once Chris produces a final version, do you want to use a Google Doc for any kind of final comments, or do you prefer to do it in a similar way as I think we've done with the registrars, for example, sending their comments and identifying which section they had their comments on? So it's really up to you and the group to determine how you would like to deal with that final version.

JANIS KARKLINS: Thank you, Marika. Let me suggest that, for the moment, the updated version would be posted on the wiki page that everyone

can read. Then, once we will have a few cases, we will decide whether and how we would finalize those cases for the record.

With this, in case of absence of any further requests for the floor or objections – I see none – we can then move to the first reading of the next case, which is investigation of criminal activity where domain names are used. A specific example is phishing attacks.

If I may suggest that we would stick to the proposal that has not been objected to so far. That is, in the first reading, everyone can indicate the difficulties that they have specifically with the particular case and then present in writing those specific comments that will be introduced for the reading next week. In order to introduce and then post the case for next week, ideally those comments in writing should come in by tomorrow night (by Friday night) but equally can go until Monday morning. If that would be acceptable, then I would use that method to go through the initial reading very quickly and then go section by section during the second reading.

I recognize Greg's hand. Please, Greg, go ahead.

GREG: Thank you, Janis. I wrote this use case, so I'll be presenting it and am probably best prepared to answer questions that come out of it. We do have a practical problem, which is that I will be on vacation next week. My question is – I'm happy to prefer it (the presentation) until the next meeting, which would be August 8th – how to handle that given the practical problem.

JANIS KARKLINS: Okay. Thank you for lurking. Why don't we then do the following? You walk us through the case now, and we will see if there is any violent reaction. Then we'll decide how to proceed after hearing initial comments.

GREG: Okay. Let's see how far we can get then. This is in some ways a set of tasks and purposes that occur in many cybercrime cases. We can talk about phishing as a specific example. There are the reasons why people request the data and how they use it during the course of one of these investigations. These are also done by both investigators in the private realm – for example, companies who are being attacked by phishers. Some of these steps are also done by law enforcement because they're trying to achieve the same goal. So that's the background. Our purpose here is to help explain how some of these things work practically. We'll see what issues surface.

We start by quoting Recital 49, which gives us some very practical advice in these cases. The recital talks about how the processing of the data is a legitimate purpose for the controller in these kinds of situations, and obviously the people who wrote the GDPR were aware of some of these things work on the Internet and how people are defending themselves and their customers and their users.

As we go through, we'll talk about compromised versus malicious registrations. I'll get to that in a moment. Let's move on to A. In this use case, we're defining things generally, which would be parties responsible for dealing with these kinds of problems. In 49,

it talks about network operators, providers of online services, commercial security service providers – that kind of thing. As I mentioned this involved corporate/academic investigators and law enforcement. They also rely on these parties in addition to using some of these techniques themselves.

B. Why is non-public registration data necessary? Here's some of the reasons why the data is requested and how it's used. One common need is to determine whether the domain name is compromised or maliciously registered. "Maliciously registered" means registered by someone who is a bad actor, who is using the domain name to commit a crime. A compromised domain name is an innocent registrant but the domain name is being used probably without their knowledge for a criminal or abusive purpose – someone gets their hosting broken into, for example. These kinds of things happen every day.

It's important to determine in a lot of cases the difference between these two cases because it will then determine what good options you have to deal with the problem. If a domain name is maliciously registered, suspending the domain name is an option. That can be done by a registrar or the registry operator. You shut off all functionality of the domain name. The only person that's going to hurt is the criminal.

However, you don't want to do that probably with a compromised domain because, again, that will shut off all the services associated with the domain name. That may shut down the legitimate sections of the person's website and may shut off their e-mail and so forth. That tells us what mitigation steps might be appropriate. This is a very responsible kind of evaluation to do

because you're taking into account the collateral damage that could occur if you do the wrong thing. So this is a very measured step and you're trying not to make things worse and you're trying to come up with an appropriate solution to the problem.

Also to note, reputation providers, such as block list providers, don't generally block list compromised domains, or they may put them on a special list. Again, you don't want to filter out traffic to a legitimately used and registered domain name. Block list providers – some of them – list specific URLs, but some just list domain names. When they list a domain name, they're writing it off. They're saying, "Don't have anything to do with it." That's what they're recommending to their customers. Again, the difference is important there.

If we can continue to scroll down. Okay, so that's the end of that particular bit. We can continue to see Task 2. Thanks. Okay. Another reason why you're looking at the data is to determine what additional domains may be related to the one that's a problem. This is especially true when, again, you're dealing with maliciously registered domains. It's very often the case that a criminal or malefactor will register a set of domain names and they will work their way through them. We see this in malware and phishing cases all the time.

The issue here is dealing with ongoing harm. We also want to find the criminal and abusive infrastructure. Typical case: an investigator finds that there's a problem associated with a domain, and then I might go look at the IP address that domain name is supported on – so the DNS information – and then I can determine what other domain names are also on that particular IP

address. But that won't necessarily tell me if those domain names are being operated by the same bad actor or not. Sometimes it may tell me some clues, but it may not help me make a determination about which ones might be a problem and which ones I should look into and maybe which ones I might want to block list, etc. In this case, you may need to cull which domain names on that IP address belong to one party versus the other and then concentrate on the ones that have a known problem associated with them.

Task 3, or Purpose. I want to assess the accuracy or truthfulness of the contact data. If the contact data is bogus – if it is fake, if it is purposefully inaccurate – then that certainly is a sign of bad faith, and that goes into my decision-making process. It also, of course, constitutes fraud, and it's a violation of ICANN policy. An accuracy check of the data may involve validation and verification and checking it against other data sources, etc. You'd be surprised, by the way, how poorly sometimes criminals do the job of faking their data. So assessing accuracy is important.

The next on is #4. You want to document the case, including the evidence and the rationale for the action that you might take. If you're the data controller – say you're registry or a registrar – you might want to preserve the reason why you have made the decision to suspend a domain name. If I'm reporting a problem to someone, I want to be able to substantiate why the domain name is a problem. If I make a request to someone saying, "There's a problem on this domain name. I request that you do something about it," I need to give some information about why that is the case. Again, this is being responsible. It's also giving a decision

maker information that they need in order to make a determination.

Task 5. [Farzaneh], we will talk later about automation. Task 5: Attribution of crime and abuse to a specific actor. Obviously, law enforcement does this when they're investigating a case. Private parties also want to be able to do it so they can potentially report that information to law enforcement, for example. They may also want to do it so that they avoid other assets associated with that party.

Task 6. Again, reporting to law enforcement.

Now, of these tasks, a lot of them do involve automation. One of the practical problems we have on the Internet that things are moving at Internet speeds. There are literally thousands to millions of these kinds of incidents happening each day. Systems that protect people are not effective unless there is automation. Some of these tasks are being done on a minute-to-minute, second-to-second basis.

For example, the block lists that protect all of us and are used in our browsers and in our e-mail are literally updated second to second. Some of these tasks, like determining associated domain names are done using algorithms. Some of the larger block lists that are used to protect us have hundreds of thousands of domain names on them at any time, and those needs to be maintained and groomed. You don't generally want domain names to stay on them if they do not need to be listed for an extended period of time. You need to bring new ones on. You need to figure out in some cases how to prevent harm as quickly as possible.

So it's important for us to understand that the systems that protect people do involve a high degree of automation. The WHOS data, or the registration data, is an important part of that, along with DNS information and a lot of other systems that are used as components of decision-making.

I see some notes in the chat. I'll turn it back to you, Janis.

JANIS KARKLINS: Thank you very much. I think, Greg, the question is – you will be on vacation next week – will you have a substitute?

GREG: Yes, but my own personal substitute is not versed in these issues like I am.

JANIS KARKLINS: Okay. Then I would suggest, taking into account that we are about ten minutes before the end of this call, the following: that we would, for the next meeting, devote part of the time of the meeting to get the initial reactions of the team on this case, which means that no inputs in writing should be done by tomorrow or Monday morning. So please prepare yourself to provide general comments during the next call on Thursday. The rest of the time of the call we would devote to thematic discussion on accreditation based on the paper that the Secretariat will pull together from all submissions that have been done so far on the topic.

I see there are three hands up, as far I see. Alan Woods, Milton, and Stephanie. Alan, please go ahead.

ALAN WOODS: Thank you, Janis. Noting what he just said there, I don't want to belabor the point. But I do feel I want to give just an initial reaction to this to maybe frame the way I'm thinking about this.

At the outset, I want to say that I'm exceptionally sympathetic to this particular use case, purely because I feel that this is one of those use cases that the law has failed, not necessarily ICANN in this particular instance. But that does lead me and segues into this: that, unfortunately, this is a problem and an issue with the law – the law is we would have to apply it – and not necessarily an issue that something that we in this group can fix.

As said, I'm exceptionally sympathetic to this, but looking at even the list of the legal bases and the lawful bases that are being quoted on this, realistically, when you look at this, you're saying that the LEA do rely on this research. That's all very well and good, but the problem is that these researchers, as you said yourself, are private. They are not the LEA, and they cannot rely on the vast majority of them.

So this does unfortunately still come down to a 61F review. That's the crux of this: that we need to look at this as a 61F review. There is not legal basis for this, and, to be perfectly honest, this is something that the industry of security researchers needs to take up with those who created the law because we still have to apply the law and we have to apply it as best as possible. I don't think

ICANN and this group can make any efforts to change that. We have to apply it the way it is. We will try and figure out a way of doing it as best as possible, but I just want to set expectations here that the law is the law, and we need to make sure that we are sticking within the boundaries when we come up ultimately with our policy decisions on this.

GREG: Just to respond, I think our entire work in this group is figuring out how we deal with the situations within the bounds of the law.

JANIS KARKLINS: Thank you, Greg. Milton, please?

MILTON MUELLER: Can everybody hear me okay?

JANIS KARKLINS: Yes. Please?

MILTON MUELLER: All right. Greg, I think that what you've done with this use case is that you've conflated a couple of things that actually could be separated. I don't actually agree with Alan that this is a problem with the law. I think that you have gotten used to having open WHOIS data, and you made a lot of assumptions that actually are not warranted.

It strikes me that the fundamental use case here is the need to defend or stop an attack operationally. It is not to identify and prosecute the guilty party. In many such cases, it doesn't matter a whole lot who registered or who is using the domain. You just need to stop the harmful activity. Once you've identified the harmful domains, we will at some point have to turn that information over to LEAs to actually do something about it other than, for example, blocking or suspending domains.

I know a bit about how these kinds of activities happen and how these forms of cybersecurity defense work. For example, you don't need redacted data to substantiate why you have suspended a domain. You say, for example, it's part of a DDoS attack and you have to block it or sinkhole it somehow in order to protect your network or your customer from the attack. There's a whole lot of information that will not be redacted that is highly relevant here. We will be able to send requests to the registrars' abuse contact. You will be able to send a message to an anonymized e-mail address. You will have the main country and state or province of a domain. You will have the data registration. All of that I think will be not redacted.

So I totally support efforts by private actors to sift through this information and identify what they need to do to stop attacks, but I think that you're taking it a step further and assuming that you need to open up the data that you may not need to do in many cases.

GREG: I'll respond. I could give you some practical walkthroughs on some cases where the information is absolutely important to have. You made several statements during the last couple of minutes that we would need to unpack, one of which is that all these cases get reported to law enforcement. The practical issue is that the vast majority of these cases do not involve law enforcement at all and is not reported because it is neither practical nor necessary.

MILTON MUELLER: That's right. You just stop the attack, right? That's exactly what I'm saying.

GREG: Well, not necessarily. Reporting to law enforcement is what I'm talking about at the moment. There are thousands of these happening right now. Most of the way that things are dealt with on the Internet is not through law enforcement. They don't have the resources. Instead, it's dealt with between private parties. Basically, our Internet is a network of networks, and you talk with the party who's responsible for the resources that are at issue. A lot of what's done is reliant on contracts, which govern the behavior of the users and so forth. What I'm saying is a lot of this stuff is done by the private parties talking to each other, working with each other. Law enforcement is not involved in any way, and it's not going to be because it's not practical.

Over the years, I've made a lot of requests to parties saying, "Well, here's the problem." Sometimes that works and sometimes that doesn't. There are parties out there who don't care. You can

say, “Yes, report it to the hosting provider,” but they’re not the only ones who might be able to do something about a particular problem.. Some of them are complicit in the bad activity. So some of these things we went through are actually very practically important, and the data is enormously useful and, in some cases, key to making the right decision and avoiding harm to all the parties who are being victimized. Thanks.

MILTON MUELLER: Again, I’m not sure that he’s really answered my question. Tell me how you need to know the phone number behind a domain name registration to stop a botnet attack. Just to use one—

GREG: That’s really an irrelevant use case. Tell you what. During the next—

JANIS KARKLINS: Gentlemen, sorry. I think we have run slightly beyond the purpose of the first reading/initial reactions. This conversation should be in detail once we will get to a very specific discussion on each of the tasks during the second reading. But your concern, Milton, is noted. I think we will have the possibility to discuss it further during the second reading.

We have two minutes remaining. Let me see if Stephanie is back on the call.

GREG: Janis, what would you like to do in our proceedings on this particular case? What will happen on the list, and what will happen in next week's call, if anything?

JANIS KARKLINS: Look, let me maybe stop here since we have less than two minutes before the end of the call. My proposal is that, next week, we will devote some time to collect further initial reactions to this case. You will have your substitute present but also you have a chance to listen to the recording, Greg, and be well-prepared for the detailed discussion the week after.

So the second part of next Thursday's meeting we would devote to thematic discussion on accreditation. For that, leadership will send a document which will be basically an extract from sources or inputs that have been submitted by groups on this topic so far. We will simply have a free-floating discussion on accreditation, starting with the definitions and then also policy questions and maybe practicalities that we may want to discuss.

So that is my proposal. Then, in the second week from now, we would come back to this use case for the second reading and see how far we can get and whether we will be able to introduce a third case for the first reading. So, again, it depends on how quickly we will plow through this case. I suspect that we may need to spend some time beyond one hour or one-hour-and-a-half. So that's my feeling.

Stephanie, would that be okay?

STEPHANIE PERRIN: That's fine with me. I was going to recommend that we leave it for two weeks until Greg can be back. There's a lot of meat to chew on here, and if people would do their research, that would be very productive.

JANIS KARKLINS: Again, I think that we can collect the initial reactions. Greg will be perfectly fine listening to them on audio and be prepared in two weeks to respond once we will get through all the elements of the case.

With this, of course we didn't get to the end of the agenda. Sorry for that. It's the third time in a row, but it seems that we are spending time discussing substantive issues. I consider that extremely important. The action items will be published to the mailing list because we have a lack of time in listing them now. That reminds me to thank all of you for active participation. We will meet again in one week's time for now. Thank you very much. This meeting stands adjourned.

[END OF TRANSCRIPTION]