ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2
Thursday, 14 November 2019 at 14:00 UTC

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

TERRI AGNEW: Good morning, good afternoon, and good evening and welcome to the GNSO EPDP Phase 2 Team Meeting taking place on the 14th of November 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're only on the telephone, could you please identify yourselves now. Hearing no one, we have listed apologies from Georgios Tselentis of GAC, Matt Serlin of RrSG, and Amr Elsadr of NSCG. They have formally assigned Olga Cavalli and Sarah Wyld as their alternates for this call and any remaining days of absence.

Alternates not replacing a member are required to rename their lines by adding three z's to the beginning of their names and at the end in parentheses their affiliation dash alternate, which means you are automatically pushed to the end of the que. To rename in Zoom, hover over your name and click rename. Alternates are not allowed to engage the chat apart from private chats or use any other Zoom Room functionality such as raising hands, agreeing, or disagreeing. As a reminder, the Alternate Assignment Form must be formalized by the way of the Google link. The link is available in all meeting invites towards the bottom.

Statements of Interest must be kept up to date. If anyone has any updates to share, please raise your hand or speak up now. Seeing or hearing no one, if you do need assistance updating your Statement of Interest, please email the GNSO Secretariat. All documentation and information can be found on the EPDP Wiki Space. Please remember to state your name before speaking. Recordings will be circulated on the Mailing List and posted on the public Wiki Space shortly after the end of the call. Thank you. With this, I'll turn it back over to your Chair, Janis Karklins. Please begin.

JANIS KARKLINS: Thank you, Terri. And good morning, hello and good evening team members. I hope you had a nice and eventless flight back home from Montreal. So, welcome to the 29th online meeting of the team. We have Agenda now on the screen. Agenda went out a few days ago, no comments have been received so far. My question is can we confirm proposed Agenda? So, I see no objections, so we'll proceed accordingly.

So, let me once again thank all team members for their very active and constructive participation in ICANN66, where we had four meetings and I think we made very good progress. Of course, always we want to progress faster, but we closed an important topic, accreditation. We started discussing also new building blocks on logging auditing, and we'll continue that today.

So, we also had a conversation about how to proceed and I understand that receiving word is that we would continue with the rhythm as it was before ICANN66 until early December, and then we will take stock and see whether we push out the Initial Report or we postpone until face-to-face meeting. And if that will be the case, then we'll pick up a few Priority 2 Items, which are pending for the moment. So, this is my takeaway from Montreal, and so I don't know if anyone wants to take the floor at this stage. I see no request for the floor.

So, let me then raise another issue about the time of the call. So, now we are on winter time and as a result, we have calls one hour earlier than during summertime, so that coincides with the very early start for those who are on Pacific Coast, and very late for those who are in Japan. And I don't know. So, the proposal is that we would maybe maintain the same hours as we used all the time. And so, the question is whether that is something that everyone would agree with. Margie?

MARGIE MILAM: Hi, it's Margie. I am not a morning person. It's very, very hard to do a 6 a.m. call. Is there a possibility of, because I understand there's also the Japan time zone which makes it difficult for Rafik, maybe alternating so that at least we don't always have to have it this early in the morning? But it's really difficult for several of us on the Pacific time zone.

JANIS KARKLINS: So, what about starting Legal Committee calls an hour later? Would that be some kind of a compromise that we could look at?

MARGIE MILAM: Yeah, that would be helpful. Anything that brings it up an hour would be helpful.

JANIS KARKLINS: I know what does it mean, one hour of sleep in the morning. Okay, so then maybe we can agree that we would keep team meetings as is, 2 p.m. UTC, and the Legal Committee would meet then at 3 p.m. UTC, which would then allow those on the West Coast to have one more hour of sleep. So, I don't see body language, but it seems that might be acceptable. So, thank you very much. So, I am not sure whether… Marika, are you on the call already? Can you share the screen on the status of the building blocks?

MARIKA KONINGS: Yes, I managed to get my Zoom to cooperate.

JANIS KARKLINS: Okay, good.

MARIKA KONINGS: As soon as I find my screen. Here we go. Janis, you want me to run through it?

JANIS KARKLINS: Yes, please.

MARIKA KONINGS: I do hear a bit of an echo.

JANIS KARKLINS: Me too, actually.

MARIKA KONINGS: So, someone may need to mute their microphone. Okay, better already. So, this is the latest status of the building blocks. Staff has gone ahead and updated it with the dates we discussed during our meeting at ICANN66. So, you should have, hopefully, clarity on when that line for comments are and the expected review dates. We've also marked, for a couple of the building blocks, where we have started, review has started discussions so that only the ones you see in white are really the ones where we haven't really paid a lot of attention to but again, those have been slotted for further consideration.

We've also noted that there a couple of building blocks where most of the line which has been finalized, there's just a couple of items where either the group hopes to obtain further legal guidance that may clarify whether the two items or have a further decision on the entity that disclosing the data and needing to review them in that particular section. So, this is current state of work. Just want to flag as well, and I think we've noted it before, that we have added the updated language on the balancing test framework that was circulated by Matthew, so you'll find that here on the bottom. Again, it's also already lined up for conversation, but people can already go ahead and review that.

And if I may take the opportunity as well to maybe remind everyone, and I think some of you have been very enthusiastically editing and providing input on the building blocks that we'll be discussing today, but we've noted that quite a few have done that in the form of edits instead of comments, which of course makes it a bit more challenging for the group to review and consider potential changes.

So, if we can just encourage everyone as you go ahead and review these building blocks, please us the comment function, even if you have specific language, put it in the form of a comment because that makes it easier for the group to first consider that language and have a conversation around whether it's broadly agreed or not before we actually incorporate it. So, that's where we are. I hope that was helpful and I'll hand it back to you, Janis.

JANIS KARKLINS: Yeah, thank you, Marika. It's very helpful. So, as you see there is progress since last time we saw the screen, this table. Still, a few blanks and that said, we have a few meetings to go. So, any comments in relation to the building block table? I see no requests for the floor. So, then we'll move to the next sub-item, and that is travel requirements for ICANN67. Terri?

TERRI AGNEW: Thank you everyone. If I could just please remind you to complete the Alternate Form if you're not traveling. Well, actually I'm going to start with the January meeting. We have about 14 folks who still need to book for the January EPDP Face to Face Meeting Travel. If you could please get that done as soon as possible. And then if you did need travel requirements for ICANN67, that did expire last week, if you needed to alert us, but if something has fallen through please alert us right away. Back to you, Janis.

JANIS KARKLINS: Thank you. Milton, your hand is up.

MILTON MUELLER: Yes. Sorry for not being up on this, but what exactly were the dates of the January meeting? The invitation I got said it was one day, is that right? January 27th?

JANIS KARKLINS: No, it's not, Milton. We're looking… Let me pull up a calendar. We're looking January 27th, 28th, 29th.

MILTON MUELLER: Yeah, okay. Then I can't go so that's why I haven't responded. I assumed it was a week or most of the week and that just won't be possible at that time for me. So, I'll appoint an alternate for NCSG.

JANIS KARKLINS: Okay, thank you, Milton. So, any other comments at this stage? So, in absence, then let us go to the next Agenda Item and that is logging building block. So, if I may ask to bring that building block on the screen. So, we had initial conversation of the logging building block in Montreal. And we set up a small group on Monday night who in parallel with the Committee, Legal Committee, reviewed the language of the logging building block, and what we are now seeing on the screen is the result of that initial reading of the building block on logging. So, I would suggest that we go and look at text paragraph, but before that Marika is asking for the floor. Marika go ahead.

MARIKA KONINGS: Yeah, thanks Janis. Sorry. Challenge is getting off mute here. This is Marika. I just wanted to make sure that people understand what they're currently looking at. The added steps are made by me that are marked 4th of November, or I think all those edits that are marked 4th of November, were made as a result of the Small Team Meeting that took place in parallel to the Legal Committee Meeting on the Monday at ICANN66.

There are, I think, some other edits that have been suggested and some comments that have been made in the document that have a different date associated with them. So, again, I think it's important for the group to kind of factor that in that there's currently a mix of edits, and again this goes to the point that I made previously, it may be helpful for future editing exercises that people make their changes, unless they're kind of specific changes that were agreed, in kind of comment form because it makes it a little bit easier for the group to review what has changed and the rationale for the change that's being proposed. But that is basically what you see currently on the screen.

JANIS KARKLINS: Okay, thank you Marika. Marc Anderson?

MARC ANDERSON: Yes, Marc Anderson. As one of the people on the small team responsible for all the red ink on this page, I thought I'd raise my hand and give a little more context on this. Our last meeting, I gave a quick update on what we tried to do here with the logging, which is essentially take it up a level and not be too prescriptive on exactly what logging is required. But we wanted to look at what the activity of the SSAD System is and what we thought the key events were that needed to be logged.

And you see that towards the bottom there's three bullet points, logging related to identity provider, logging related to the entity that receives the requests, and logging related to the entity authorizing the requests. So, we thought sort of at a high level, the activity related around the sort of agreeing or approving the identity of a requester, authorizing requests, and the actual processing of those requests, were the key activities. And so, we focused on those three things. And again, trying to take it up a level and draft this in sort of general principle type language rather than prescriptive about what actually has to go into the logs.

So, hopefully that's context that helps if you're reviewing and looking at this. Maybe one other thing I'll just add, is we may need to revisit logging after audit because we have the audit requirement, we need to make sure all the information necessary for the audit is being logged, so maybe a little bit of a chicken and the egg type thing. But just sort of noting that they maybe can't be treated in a vacuum. Otherwise, hopefully that's helpful context for everybody reviewing this.

JANIS KARKLINS: Yeah, thank you, Marc, and also I want to note that at the top, there are lists of what information should be logged and what are the main principles and then there is also Implementation Guidance that describes exactly these things in details, of what needs to be logged. So, please, scroll down the text and the link has been sent to the chat. So, my proposal is to go with this section by section, and take it, discuss them, and see whether we can agree. Would that be okay? Okay, no requests.

Then, the [inaudible], "EPDP Team expects that appropriate logging procedures are put in place to facilitate the auditing procedure outlined in the recommendations. These logging requirements will cover the following; accreditation authority, identity provider, activity of accredited users such as login attempts, queries, and what queries and disclosures are made, disclosure decisions are made." Are we in agreement? I see no comments. So, let me go then to the first section. "EPDP recommends that activity of all SSAD entities will be logged." And then description of what has been logged in the Implementation Guidance. Chris Lewis-Evans?

CHRIS LEWIS-EVANS: Thanks Janis. Sorry, I had my hand raised for the last one. I put a comment in the text that we further wrap around the Point 3 and Point 4. So, both those seem to try and cover queries. So, realistically that logging should only happen in one place. So, I think separating those out, either by removing queries from the third item, would be a lot clearer in my mind. Thanks.

JANIS KARKLINS: Okay. For the moment we do not know whether reception of query and decision on the disclosure will be made in the same point. So, that justifies why they're separate. The moment we will do the accuracy reading, so if that appears will be the same entity then we can merge them without changing the meaning. Would that be okay, Chris?

CHRIS LEWIS-EVANS: Yes.

JANIS KARKLINS: Okay, thanks. So, are we in agreement that activity of all SSAD entities should be logged? Seems to be the case. Kind of logical thing. So, Point B, "Logs will include the record of all queries and all items necessary to audit any decision made in the context of SSAD." That's a statement of principle. Daniel?

DANIEL HALLORAN: Thank you, Janis. Yeah, I agree this is a statement of principle and I just want get, from an implementation point of view, my understanding is that this would be, that principle would be worked out in implementation because someone's going to have to come up with a list of the exact data elements that have to be retained. I see this really as a start of a data retention specification.

And one thing I raised in Montreal was that there's also going to be data protection implications of this data retention, there's going to be personal data in it of the requesters and possibly of the data subjects, so that's another consideration we'll have to look at at some point, I guess, in implementation. Thank you.

JANIS KARKLINS: Okay, thank you. Look, if you scroll down the text, you have Implementation Guidance that provides you a full list of information that is suggested to be logged. So, we will get to that in a second. Marc Anderson?

MARC ANDERSON: Thanks Janis. Marc Anderson. I do want to agree with what Dan said. I think where we kind of hit a wall when we were reviewing this building block was particularly around how long the logs would need to be retained. And we didn't have a chance to sort of get into who would have access to the logs, under what circumstances, and how long they would need to be kept for. In part because that may be a conversation that we have to have after we talk about [inaudible]. But I think Dan's right, that conversation, it's something we have to account for.

JANIS KARKLINS: Okay, thank you. Certainly, we will. And when it comes to the period of retaining of data, that's the Subpoint C which in the current version suggests that logs must be retained for a period sufficient for auditing and complaint resolution purposes in a machine-readable format. So, in the comments I spotted that Thomas said to put down three years. In initial version, there was a proposal of two years. But in this current version it is more generic and not prescriptive, and that will be left for decision during the implementation. So, any comments? Any preferences apart from ones I outlined? So, I take silence as a certain level of comfort with what is on the screen now. Marc Anderson?

MARC ANDERSON: Thanks Janis. I guess I'm raising my hand on the three year period. I guess as Dan's pointed out, there will likely be personal information in these logs. So, if three years is the period we're retaining it for, I think we need to say why it's three years. I think I made the same comment when we had the meeting in the small group, is I'm not advocating for or against three years, I just think we need to be able to say why we are… It can't just be a random period of time. We have to have a reason why it's three years. And we may have good reasons why it's three years, it's just not articulated here.

JANIS KARKLINS: Okay, thank you. Thomas, could you explain reason of three years?

THOMAS RICKERT: Sure. Thanks very much, Janis, and hi everybody. The reason for the three years was that in case data is being reviewed by a contracted party owning non-public WHOIS data, and somebody then complains, let's say that is on the last day before the two year retention period before the contracted party starts, then upon expiry of the two years, none of the parties would have data available to evidence to whom what data has been revealed and potentially [inaudible].

That was the rationale why I had suggested to have a longer retention period for the logging than we would have for contracted parties to retain the data, but I'm okay with generic language that you suggested and bracketed language at the moment. I would only recommend the reframing of that to make it more specific and more defensible, if I may, which I hope you find amicable or friendly. We could say that retention period should be determined during implementation and it should be a period sufficient to cover the period in time until third party claims against the controller are barred by statute. You know?

This is basically the reason why I picked three years, but it may depend on the jurisdiction that the entity doing the logging may reside in. So, I think if we attach it to a statutory pension requirement or statutory limits, then we would be on the safe side. And I should also note that is a period, a retention period, that is typically acceptable because you must be in a position to defend against claims by the other subjects. Thanks.

JANIS KARKLINS: Okay, thank you. If you could put your suggestion in the chatroom, Thomas, that would be appreciated. Mark SV please?

MARK SVANCAREK: Mark SV for the transcript. I think we should not assume that there will be any personal data stored in these logs. I think it should be pretty straightforward to design them in such a way that there isn't. So, while we need to keep that concept in the back of our heads, in the Implementation Guide we should be very clear that to the extent possible, there will be no personal data included in the logs. And if we are able to that, which I think is likely, that will remove some of these concerns about retention and other things, as well. Thank you.

JANIS KARKLINS: Thank you, Mark. Ayden?

AYDEN FERDELINE: Thanks. This is Ayden. I agree that we should provide a rationale for a retention period, and I agree with the arguments that Thomas has put forward, they make sense to me. I hope I'm not jumping too far ahead here, but in C I wanted to suggest a revision to the words in a machine-readable format, just for the avoidance of doubt. I would suggest changing this to a commonly used structure machine-readable format accompanied by an intelligible description of all variables. Just so that we… Whether this is Implementation Guidance instead or should be within this building block, I'm not sure, but I think that would be useful. Thanks.

JANIS KARKLINS: Thank you for the suggestion. If you could put these aforementioned in the chat, also that would be appreciated. So, anyone feels uncomfortable with what Thomas proposed and what Ayden proposed? I see that there was some positive reactions in the chat. So, I think that we would then retain formulation proposed by Thomas and we will add also the precision that Ayden suggested in calling the new structured machinery to the format to be more precise. Good, thank you. May I take that as we're done with C?

And let us move to D. "The logged data will remain confidential and must be disclosed in the follow circumstances; in the event of a claim of misuse, they may be requested for examination by an accreditation authority or dispute resolution provider. Logs should be further available to data protection authorities, ICANN, and the auditing body, and when mandated as a result of due legal process and when it's the result of the due legal process." So, three things. Any issues? Thomas, it's your old hand [inaudible] or you want to speak on D? Alan Woods?

ALAN WOODS: Thank you. Alan Woods for the record. Yeah, so you see my comment there, I just put that in this morning and apologies that I only got into this today but [inaudible] like most people. Could you… Sorry, just one second there. So, thank you. Sorry about that. So, my point is that if we're planning the legal advice, again, from our EDBP or the European Data Protection Board, I just want to keep us mindful of what's there in the future as well, that if the liability is still retained by the contracted parties in this, then we just need to keep in mind that there is a potential that we might need to release those logs to the contracted party as well. This is again something far in the future, but I think if we're putting it into the building blocks, should probably just have a concept of that, that again, depending on what we get back from the Strawberry Team's efforts, it could have an effect on that. So, apology about the delay there. Thank you.

JANIS KARKLINS: Okay, thank you. I understand that you then suggested to add somewhere, in which subpoint, small i,, ii, or iii?

ALAN WOODS: To be honest, I'd say at this particular moment it's more of a footnote because what's in there could be very well for what it is, depending on the advice but I just want to make sure that we have it in mind for when it comes through, that there may very well be a change needed once we get the advices back.

JANIS KARKLINS: Okay, so then I ask Marika to start to take a note and put it somewhere that there is a check needed during the proofreading. Brian?

BRIAN KING: Thanks Janis, this is Brian. As a constructive point to Alan's point, perhaps we'd put a pin in this and say the controller(s) and see how that shakes out. And to the point I raised my hand for, is that I think including DPAs explicitly in 2 is inappropriate because it's probably captured under due legal process and it seems that DPAs there wouldn't necessarily have a special privileges to investigate these logs. But anyone that has the legal process to do that should be able to do it. So, I would strike DPAs from romanette 2 and then just consider that to be included as intended under romanette 3. Thanks.

JANIS KARKLINS: Okay, thank you. Marc Anderson?

MARC ANDERSON: Thanks Janis. Marc Anderson. Generally, I think I'm good with what's in D. We spent a fair amount of time on that in the small group and the end result is pretty positive. One item that we talked about though that doesn't seem captured here is sort of use of the logs by the technical operator of the system. There may be need for sort of troubleshooting and general technical op, to use the logs for general technical operation of this system, and we didn't want this language to be construed to prevent that. And I'd be happy to suggest something offline, but I think we wanted to have that use case accounted for here as well.

JANIS KARKLINS: Okay, thank you Marc. So, any issues with the suggestions to strike data protection authorities with understanding that they would fall under small roman 3 on due legal process? Ayden?

AYDEN FERDELINE: Thanks, this is Ayden. Brian raises a really interesting point. I just put something in the chat. I was wondering if we change data protection authorities to relevant supervisory authorities, would that be a way of keeping that language there or is it still unnecessary? Thanks.

JANIS KARKLINS: Thank you. Brian, your reaction?

BRIAN KING: Yeah, thanks Janis and thanks Ayden. I see where your getting at there. If I remember correctly in the legal memos that we got from Phase 1, the SSAD might not necessarily be under EU jurisdiction, and so I wouldn't assume here that there would be necessarily a relevance to supervisory authority for the SSAD. So, if there is one, they would certainly have due process under romanette 3 to get to these logs, and we should certainly allow them to do that. I just think it's captured already under 3 and including DPAs under 2 is inappropriate because what happens if a Brazilian DPA wants to log something. It just seems odd to have it explicitly there. Thanks.

JANIS KARKLINS: Okay, thank you. Would, for instance, asterisks at the due legal process, and then which would in a footnote mention such as data protection authorities, law enforcement agencies, would that be something we could think of? Okay. So, then we will try then to put what is now in the chat. On Marc's point, can we include a small roman 4 by use of technical operator of the system in case of necessity probably? Any opposition to that? No hands. I take it then we can include to put the small roman 4. Chris?

CHRIS LEWIS-EVANS: Yeah, thanks Janis. Chris Lewis-Evans for the record. I totally agree with that, the technical thing, but I would say to enable the system to operate correctly, just to limit why they're having access to the logs. I think it's to ensure proper running, not to have a look in the logs at their will. So, just to put that stipulation on it would be good.

JANIS KARKLINS: Yeah, thank you Chris. I think that's a very good suggestion. So, we will retain then Chris's suggestion as an explanation why technical operator needs to get access. So, okay. Thank you. Let us now then go further, and further we have Implementation Guidance.

In Implementation Guidance, we have three points. One, logging related to the identity provider with the four subpoints and let me take first four. For identity provider, "details of incoming requests for accreditation, results of processing requests for accreditation including insurance issue and such identity credentials or reasons for denial, details of revocation requests, and indication when identity credentials and authorization credentials have been validated." So, any issue with this list? Marika?

MARIKA KONINGS: Thanks Janis. This is Marika. No issue with the list but I just wanted to flag that some changes were made to the introductory sentence that original read, or the small team had suggested there that it would read, "at a minimum, the following events must be logged." And that suggested change has been made here so it would read, "All activity must be logged which should enable authorized auditors to determine." So, just wanted to flag that

that's a change that has been applied and making sure that everyone is happy with that.

JANIS KARKLINS: Okay, thank you Marika. So, any issue with the suggested change of the shuffle of the sentence? Daniel?

DANIEL HALLORAN: Thank you, Janis. I actually had a question that were in the text. I can wait.

JANIS KARKLINS: Okay. Chris?

CHRIS LEWIS-EVANS: I think I might like, Mark actually explained the 'at a minimum' first in the small group really well. So, I think he's probably got a set of things to say, so I'll let Marc go. Thank you.

JANIS KARKLINS: Okay, Marc, go ahead.

MARC ANDERSON: Thanks Janis. Marc Anderson. I think Chris is right, I think I like the original language better. As I said in the intro to this, we tried to keep it high level and not be too prescriptive. 'All activity must be logged', you know, I think when that language gets to implementation that would have a very broad interpretation and so I like the original language better.

JANIS KARKLINS: Of course, that's yours. Right? I'm just joking. Milton?

MARC ANDERSON: I think it was Alex Deacon's.

JANIS KARKLINS: No, I'm joking. Milton, please.

MILTON MUELLER: Very picky minor point, but the, "All activity must be logged which should enable authorized auditors to determine;" so the word determine doesn't work with logging. I think you would mean… You would have to change the first word to logs, I think. I mean, just the grammar is kind of something. It's not a big deal.

JANIS KARKLINS: Yeah, thank you. But first let's see… I have a difficulty identifying who suggested the change to, "All activities must be logged."

MILTON MUELLER: By the way, I agree with Marc about that statement being a bit excessive.

JANIS KARKLINS: Okay, let me then put the question to the team. Would anyone object the retention of original language suggested by small group which would read, "At the minimum the following events must be logged." And then we would have a list of what logs. Which would mean that the one who proposed, "All activities must be logged.", would recall the suggestion. So, no hands up. So, I think then we retain the original version. And so, thank you for flexibility. And then let us go with the first bullet related to identity provider and foreseeable issues with that. Daniel?

DANIEL HALLORAN: Thank you, Janis. On the last sub-bullet there it says, "Indication when the credentials have been validated.", which sounds like it would be a timestamp. So, this entry would be a date, the timestamp when the credential was validated, which I think means when the identity provider issued the credential. Then it says, "That is when they log in.", which sounds different.

It would be every single time that user logs in, which I'm not even sure the identity provider would see when the user logs into the system, if that's different, if the gateway is different than the identity provider, or if this means every time the user logs into the identity provider. That part I highlighted didn't make sense to me. Thank you.

JANIS KARKLINS: Okay, thank you for question Daniel. Anyone can answer from the small group? Marc Anderson?

MARC ANDERSON: Thanks, Janis. Marc Anderson. I'll give it a shot. I think our attempt was to capture both events. So, if you look at the second bullet point there it says, "Results of processing requests for accreditation, e.g. the issuing of the identity credential or reason for denial." So, I think that's intended to be one event, when the identity provider confirms that person's identity.

But then also when a person logs into the system itself, that… I guess it depends a little bit on how the system's implemented but when the person that has a validated identity logs into the system, we wanted that event to be logged as well. And so, I [inaudible] that might not necessarily be performed by the identity provider itself, I guess you could implement the system both ways. But my recollection is the intent was to capture both events, the issuing of the credential and the log in event of a validated entity. If that helps, hopefully I did a good job explaining.

JANIS KARKLINS: Okay, thank you, Marc. Daniel?

DANIEL HALLORAN: Thanks Marc. So, it sounds like you're saying the part that says, "i.e. when they log in.", that means that is when the accredited user logs in to the gateway or it logs into whatever the system is, not when they log in to the identity provider. Because this is under log in related to identity provider and not log in related to the gateway or the system. So, we would just need to move that bullet. Thanks.

MARC ANDERSON: Yeah, I see your point. That can probably be clarified. I believe the intent is to capture both events. So, yeah, I think maybe separating them out would be helpful.

JANIS KARKLINS: Okay, thank you. Then we will separate them, and we'll retain the validation with identity provider and logging in the second bullet point. Brian?

BRIAN KING: Thanks Janis. This is Brian. So, just to clarify then, that parenthetical should just be picked up and moved down to the authorizing the request, right?

JANIS KARKLINS: The logging probably would be when sending requests, logging entity receiving requests, that would fall probably under second bullet.

BRIAN KING: I see, okay.

JANIS KARKLINS: Rather than authorizing the request.

BRIAN KING: Sure, okay. Thanks Janis. Fair enough. I think that makes more sense. So, then I guess my follow up question, if I could, is what's the point of logging log ins if there's no data requested. Because we're already logging the request, right?

JANIS KARKLINS: Right.

BRIAN KING: Sorry to integrate you. I'll go on mute. Thanks.

JANIS KARKLINS: Okay.

BRIAN KING: I think that's the point I'm making.

JANIS KARKLINS: No, no. Okay, thanks. That's useful. Marc?

MARC ANDERSON: Thanks Janis. Marc Anderson again. I do think this language came from Alex. We're at a loss not having him on the call here to be able to explain his thinking so I'm trying to channel my inner Alex here. But if you recall the diagram he provided to us in L.A., he had a process flow where you would access the SSAD System, but [inaudible] would actually be validated by the identity provider itself. So, I think he was drafting this with his process flow diagram in mind. It was a nice one-pager he presented for us in

L.A. in which case it would be appropriate for the identity provider to log the requests.

To Brian's question, we thought just generally, remember there's all kinds of things happening on the SSAD System and we thought it would be appropriate to log any log in type events that occur separately from the request for data itself. Because there's not necessarily a one-to-one correlation between the two events.

JANIS KARKLINS: Okay, thank you for explanation. Daniel?

DANIEL HALLORAN: Thanks. I'm sorry to keep beating this up. I think it sounds like we're just a little bit too far into the weeds on implementation here. I understand now. Thanks for clarifying. It sounds like it would be kind of a single sign on thing is what Alex had in mind and maybe the gateway wouldn't know all the details that would be authenticated by the identity provider as a single sign on or off situation, that makes more sense.

I don't think we should assume though there will be such a thing as a log in. Maybe throw in that this might be implemented through something like RDAP with Windows certificates or credentials or something. So, anyway I think we're down in implementation weeds and as long as this is guidance and we understand it, we'll have some flexibility once we know how the system works to actually go back and build this, every word of this will be biding, it's guidance. So, I think I'm going to stop commenting on this. Thank you again.

JANIS KARKLINS: Yeah. No, thank you, Daniel, for raising this issue. My suggestion would be to ask Marika or Kate and Berry, go back to Alex and discuss it with him and then maybe fine tune slightly, as a result of this conversation, fourth bullet point and see whether there is a need of splitting it in two and bringing the logging of log to the second bullet point. So, I think that would be the best way forward and then that will be reflected in the next version of the building block that we will review online.

So, with that understanding, I would like to move to the second bullet point, “Logging related to entity that receives request.” So, “Information related to content of the query itself, results of processing the query including changes of state, received, pending, in-process, denied, approved, approved with changes.” So, any comments on this? I see none. So, the third bullet point, “Logging related to authorizing the request.”, and that would be, “Request response details, e.g. the reason for denial, notice of approval, and data elements released.” Any issue with this? I see no.

So, then what we will do now. The changes that we agreed will be reflected immediately. Staff will consult with Alex and maybe fine tune the fourth sub-bullet of the first bullet point in Implementation Guidance and will then indicate when the changes are made to the team. And hopefully team members will be able to agree on proposed changes by silence procedure. And if there will be variance and disagreement, then we will come back to it. Otherwise, I consider that this building block is turned from yellow to green. And of course, we will revisit once we will do the proofreading of the whole set of recommendations if there is any inconsistencies.

And with that I would like to suggest that we move to auditing building block. So, auditing building block is in… So, let me see. Not to make the same mistake as before, is there something, Marika, you would like to say? Yes, you want. Please, go ahead.

MARIKA KONINGS: Yeah, thanks Janis. Just to note that we have a little bit of a similar situation here as with the previous one. I think you can see, well at least on my screen as you see on the screen, I think the green edits, those were all made in response or as a result of the small team conversation. Edits, I believe, that are visible in different colors have been made by others following that meeting. So, I just want to make sure that people are aware of those changes. And just flagging as well that a number of comments have then been added to some of the items. So, again, the green color, the small team provided, then you see those with my name and the date of the 4th of November. Some of the other colors are suggestions that have been made by team members.

JANIS KARKLINS: Okay, thank you very much. With this understanding, let us move paragraph by paragraph starting with the first one. “EPDP Team expects that the proper auditing process and procedures are put in place to ensure proper monitoring and compliance with the requirements outlined in these recommendations more specifically.” And then comes text that is suggested by Steve

DelBianco and it says, “As a part of any audit the auditor must be subject to reasonable confidentiality obligations with respect to proprietary processes and personal information disclosed during the audit.” So, any comments or issues with these two paragraphs, or two sentences rather? So, no hands up. Okay. So, then I see that there is no issue with this, so let me go further down.

Audits of accrediting authority. The accrediting authority must be audited periodically by an independent auditor. So, here comes suggested changes, “To ensure compliance with policy requirements as defined in accreditation building block. Should the accreditation authority be found in breach of accreditation policy and requirements to be given an opportunity to cure the breach but in case of repeated noncompliance or audit failure, a new accreditation authority must be identified or created.” So, that is proposal. There was a question of Alex. I understand the two questions whether we haven’t agreed that ICANN would be accreditation authority and would remain but let me take a few comments here. Marc Anderson and Eleeza afterwards. Marc, please.

MARC ANDERSON: Yes, Marc Anderson. I’m seeing, looking at this now, that I think we might have some terminology differences. So, I think in logging we talk about logging related to the identity provider, and then in auditing we’re talking about the accreditation authority must be audited, and I think we’re talking about the same thing. I think in logging, we’re referring to an identity provider and under audits we’re talking about accreditation authority.

JANIS KARKLINS: No, Marc, we are talking about both. We are talking about accreditation authority and we're talking about the auditing of identity providers as well, because there will be procedures how accrediting authorities selects and tasks identity providers to do the job. So, that should be audited. And then the performance of identity providers also should be audited. So, if you scroll down the text, the next chapter of this or subject of this is audits of identity providers.

MARC ANDERSON: Okay, thanks for clarification. That being the case, then the hole is with logging where we don't have any logging requirements for the accreditation authority then.

JANIS KARKLINS: Okay. So, I think I will keep that in mind. Let me go to Eleeza and then Alan Greenberg.

ELEEZA AGOPIAN: Hi, thank you, Janis. This is Eleeza. So, we put in a question or comment on the heading of this section, audits of the accrediting authority. I had just wanted to speak to it a bit just in case anything we put in here wasn't clear. Basically, I think some of this is difficult to determine how it could be implemented without knowing a bit more about the system, but because there are 70 different audits and audits can be, as we know, burdensome and expensive, we're trying to determine what the standards are for those audits, if there could be any more Implementation Guidance added to that effect, and then as well I think the point that Marc just made, if the accrediting authority as we understand it to be ICANN, then perhaps it would be more clear to make that explicit here. And then I had a couple of other comments in the comment bubble.

JANIS KARKLINS: Yeah, okay. Thank you. Alan Greenberg? While Alan is unmuting, may I take Brian?

BRIAN KING: Sure, Janis. It's Brian.

JANIS KARKLINS: Okay, Alan, go ahead.

BRIAN KING: Go ahead, Alan.

ALAN GREENBERG: Yeah, sorry. I forgot that I was muted on Zoom. I'm having… Maybe I missed something, but I'm having trouble understanding how if ICANN is the accrediting authority, who is it that's going to sanction ICANN and create a new accrediting authority? Who is it above ICANN that can do this?

JANIS KARKLINS: Community, probably.

ALAN GREENBERG: But what mechanism would be used for that? Who is the Community? Are we talking about the ICANN Empowered Community? I would've thought if ICANN is failing this badly, this is perhaps a new thing we have to put in the Empowered Community to force ICANN to fix it or something, but I can't see a mechanism in the world as we have it today where ICANN can de-accredit itself and create a new authority. [inaudible] how it could work.

JANIS KARKLINS: Okay. No, thank you for raising this.

ALAN GREENBERG: Thank you.

JANIS KARKLINS: Brian?

BRIAN KING: Thanks Janis, and unfortunately I don't have the answer to Alan's question. I see Dan here, I'm sure he'll be helpful. I wanted to kind of support the concept that Eleeza made in the comments there, and I think if ICANN outsources the accreditation authority responsibility to someone then, yeah, ICANN doing its own contractual compliance with that body makes the most sense. It's probably the least expensive and would have ICANN be in a position to audit its contracted parties just like it does for the rest of its contracted parties.

And I think we would only want the independent auditor scenario if it was necessary for a concept that Alan G. is talking about where ICANN is itself the entity that's doing the accrediting, in which case it would be appropriate for ICANN to pay for an independent audit of itself, as is the case which financial audits and things like that but I think that will be a limited outcome only in that scenario where ICANN's doing the accrediting itself. I hope that's helpful. Thanks.

JANIS KARKLINS: Yeah, thank you, Brian. Daniel?

DANIEL HALLORAN: Thank you, Brian and Alan and Janis. I think these are the exact issues that are raised in Eleeza's comment, that it just seemed a little strange to us from an implementation point of view that you would have… If ICANN is the accrediting authority which means the entity that is recognizing identity providers I guess, this seems to me it's sort of parallel to ICANN and the UDRP, which is our first Consensus Policy. We recognize dispute resolution service providers, we recognized WIPO as a dispute resolution service provider, and they're approved and as long as they follow the policy they maintain that approval. If they're not following the policy and the rules then we would theoretically revoke their recognition as an approved provider.

But ICANN doesn't and WIPO doesn't pay an auditor to come in and do independent audits. We would have the ability to ask them questions, like Brian said, do contractual compliance basically. There wouldn't be a contract in that particular case. So, we could do vendor management, as we talked about earlier, but not necessarily forcing ICANN or the accredited entity to burden an expense of an independent audit which can be very expensive. And it didn't seem to make sense for us.

And as to Alan's question about what to do if ICANN isn't following the policy, I think that would be just like, what if ICANN isn't following the Transfer Policy, what if ICANN isn't following the Registrar Accreditation Policy? We don't have independent audits of every other, or as far as we know, any other policy. We have other ICANN accountability mechanisms, we can have reports, you can come and ask questions at the public forum, you can file a complaint, you can go to the ombudsman, you could file a reconsideration request, independent reviews. So, there's lots of ways that the Community and contracted parties and others can hold ICANN accountable.

And we haven't used this particular tool of an independent audit which, as Eleeza pointed out, we just had to have understand like what would be the budget for this, I don't know if it might be hundreds of thousands or a lot of money to pay for an independent auditor, to train them on what they need to audit against, what standard they're going to be auditing against, and reports, and then we have ICANN Staff engaged and responding to those audits, and we need to know what a periodic basis is, is that monthly, quarterly, yearly. So, Eleeza just has all of these questions in her comment. Thank you.

JANIS KARKLINS: Okay. Thank you, Daniel. Alan Greenberg?

ALAN GREENBERG: Thank you very much. Yeah, if ICANN has identified and has a contract with someone to be the accreditation authority, then there's no problem taking it away from them and giving it to someone else. But we have specified somewhere else that ICANN is or will be the accreditation authority, so these need to be consistent. In terms of audits or verifying, clearly if ICANN is operating the SSAD and we're using the accreditation authority, whether it's us or we outsource it, then this is subject to all the normal rules associated with GDPR or whatever the privacy legislation in other jurisdiction is, and if we're not accrediting properly, then clearly we're violating the appropriate privacy legislation and that we're subject to use sanctions.

So, we have a financial reason if nothing else to make sure this is operating properly, whether ICANN chooses to use audits to ensure that or some other mechanism, I'm not sure we really need to be concerned at that level. So, I'm not sure we need audits at all as Dan just said, but I think we need to be consisted. Either it's ICANN operating or being the accreditation authority and we can't de-accredit ourselves, or it's outsourced like the UDRP ones are and then of course we can change providers if the first one isn't doing their job properly. Thank you.

JANIS KARKLINS: Okay, thank you. I'll take note and then I will make a suggestion. Milton, please?

MILTON MUELLER: Yes, I agree we have to be consistent about this. If we are talking about ICANN being the accreditation authority, and I was not entirely one hundred percent sure that we had actually decided that, it sounds like we had still contemplated them outsourcing it, so if we could decide one or the other then we can make… I think the key issue with respect to keeping the accreditation authority, if it's ICANN, accountable, certainly will not be things like the ombudsman or things like that. It's completely outer space inappropriate recommendation.

I think we would have to put something into the policy here about access to the data that would be used to determine whether ICANN was doing an acceptable or unacceptable job. And maybe the audit thing could be something that was triggered under special circumstances and not something periodic and regular, which I agree with Dan could be expensive and burdensome if there's no problem. So, that's something to think about. But is there any way procedurally to defer this issue until we have nailed down exactly who the accreditation authority is?

JANIS KARKLINS: Okay. Can we… Marika, could you pull up on the screen or put in the chat appropriate apart from accreditation building block where we, as far as I recall, agreed that ICANN would be… You have it already. Milton, you can read in the chat that from the agreed or stabilized accreditation building block, we say that accreditation policy defines a single accreditation authority run and managed by ICANN Org with a footnote that states that ICANN Org may outsource this function to a qualified third party. However, the details of this are outside the scope of the document. Thank you, Marika.

So, I think with that in mind, we need to rectify the text here and take out the de-accreditation or the new accreditation authority must be identified. Here we're talking about accrediting authority and if the accrediting authority via ICANN Org are found to be in breach of the accreditation policy and requirements, it will be given an opportunity to cure the breach. And so maybe adding something along the lines of like following the ICANN appropriate policies or the submerging policies existed or accountability policies existing in ICANN, or in line with accountability policies existing in ICANN so that would be my suggestion. And then we would see the audit of identity providers, if we can agree with that. Thomas?

THOMAS RICKERT: Thanks very much, Janis. Maybe we have it somewhere, and please let me know if we do, but I think that if actually an audit shows that ICANN, being responsible for the accreditation, made mistakes or that there is an accountability issue with ICANN, then I think the mechanics should be that if it's a minor breach, ICANN needs to be given notice to cure the breach, but if it's a material breach, then all parties involved are entitled to stop sharing data without having to be afraid to be sanctioned contractually by ICANN.

I think what Alan G. mentioned is not really an option to replace ICANN in this, or at least that would require significantly more thought. I think we are all set to make this work with ICANN and if there's an issue then the operations of the SSAD need to be paused until such time when the problem is fixed without the contracted parties and others involved being sanctioned.

And also to Milton's point, I think that we've come back to this point a couple of times saying that we haven't yet made a decision as to who does what, and I think that maybe for our group the easiest way to deal with it is just plow forward based on the assumptions that we saw on the Strawberry Teams paper, and that would actually be ICANN operating the central gateway and taking the relating responsibilities in the operational roles. So, I think that unless we otherwise our group should just move forward based on that assumption. Thank you.

JANIS KARKLINS: Thank you, Thomas. Look, I think we can still operate without leaning a hundred percent to Strawberry Team proposed mechanics because the accreditation is part of the whole system, how system functions, and we said that system could be used exclusively by accredited entities or individuals, and whether that is centralized or decentralized system accreditation will be working anyway.

An example where ICANN could be in breach of a policy is, if now my memory does not fail me, we said that there would be a limited of number of identity providers. And we may see a situation where ICANN has started to giving out accreditation providing authority to hundreds and thousands of different entities. So, that would be in breach of the policy, just an example. It's theoretical possibility, most likely in practice it won't be like that because it's not really a profitable business to do entity checking but it is first to comes to mind.

So, look, I think we should start… We'll reword this particular text based on our conversation today with assumption that ICANN Org is accreditation authority and that ICANN Org can decide to outsource function of accreditation authority and verify compliance of the entity which gets this function, or ICANN Org performs it itself.

And I would suggest that we move to the next paragraph, is audit of identity providers and see whether we are in agreement with this suggested text. And as you will see, the text is more or less the same in every chapter of this building block. So, let me now ask if there are any comments on audits of identity providers.

And I will read it out. "Identity providers must be audited periodically by an independent auditor to ensure compliance with policy requirements as defined in the accreditation building block. Should the identity provider be found in breach of a protection policy and requirements, it will be given an opportunity to cure the breach, and in case of repeated noncompliance failure the new identity provider must be identified. And in any audits that the provider shall be tailored for the purpose of assessing compliance and independent auditor must give reasonable advance notice of any such audits, which notice shall specify in reasonable detail the categories of documents, data, and other information requested. And as part of such audit identity providers shall provide to the auditor in a timely manner all responsive document, data, and other information necessary to demonstrate its compliance with accreditation policy." So, that's the suggested language. Brian, or are we in agreement with that?

BRIAN KING: Thanks Janis. It's Brian. I don't think so just for one point that I see Eleeza may also be making, and that's the independent auditor point there. It seems that this is even more of a no-brainer for the audit of the identity provider to be done by ICANN, just like it does for the rest of its audits. So, that may be Eleeza's point or not but that's mine. Thanks.

JANIS KARKLINS: Okay, thank you for suggesting taking out independent auditor. Eleeza?

ELEEZA AGOPIAN: Hi, thanks Janis and thanks Brian. Yeah, I mean that's sort of what I was getting at, basically. Again, as with the comment above, it's sort of difficult to envision how this would work without knowing more about who the providers are. So, I put in the comment here what if the identity providers were Interpol or WIPO, would we have to hire an independent auditor to cover that? So, a similar comment as the point made earlier.

JANIS KARKLINS: Okay, thank you. Thank you. So, would then team be in agreement to replace an independent auditor with the by identity accreditation authority? Instead of independent audit, the audits of identity providers would be conducted by accrediting authority. Milton?

MILTON MUELLER: Yeah, I'm not sure that I do support that change. I think there are good reasons to have this done independently of ICANN. If there is a problem in ICANN's incentives I think would not be to create any trouble for anyone. I don't understand why ICANN could be trusted to fulfill this function on its own. I think it would need to be an independent auditor. Open-minded, could be convinced otherwise, but just looking at this on its face, I don't favor that change.

JANIS KARKLINS: Okay, thank you. Marc Anderson?

MARC ANDERSON: Thanks Janis. I may be trying to split the difference here, but it maybe just auditor and we don't need to be prescriptive here, whether it's an independent auditor or whether ICANN's performing the function, or some other third party. I think maybe we can just not be prescriptive on this point here.

JANIS KARKLINS: Okay, thank you. So, your suggestion is not replace 'an independent auditor' with 'ICANN Org', but simply just strike independent and then the text would read, "Identity providers must be audited periodically by an auditor."?

MARC ANDERSON: Yes.

JANIS KARKLINS: Okay, thank you. Milton, would you feel comfortable with that suggestion?

MILTON MUELLER: First of all, grammatically all you would have to say is "It must be audited periodically.", to do what Marc is trying to do. You wouldn't need to say, "by an auditor." I mean, presumably audits are done by auditors. But I'm not sure how that gets us out of the dilemma, really. Do we trust ICANN to audit its own identity providers or do we not? I think that's the question. I'd like to hear opinions on either side.

JANIS KARKLINS: Okay. Let me give it first shot, I do. But let me ask whether Alan does. Alan Greenberg?

ALAN GREENBERG: Yeah, thank you I was going to suggest deleting the 'by an auditor', and whether ICANN chooses to do the audit with its own

Staff or hire an outside auditor is equivalent to how it handles Registrars under the RAA, and it may use its own compliance department to do various verifications, or it may hire an auditor to do it. So, I don't think we need to specify. I think the essential part is it needs to take some action periodically to make sure things are being done properly.

JANIS KARKLINS: Okay, thank you. Brian?

BRIAN KING: Thanks Janis. It's Brian. I agree with everything Alan G. just said and I think that this is the way that ICANN works and that the DNS works, is that ICANN audits its contracted parties, and this would be someone, these identity providers will be parties that have a contract with ICANN, and same thing as a contracted party that we all know and love. But the same concept, and this is what ICANN does. It's in alignment with their role to coordinate the global DNS, they make sure that they've audited everybody that they've contracted to do something is doing what they say and introducing the concept of an independent auditor for this seems odd and its different. It's much more expensive than having ICANN do it themselves.

So, if we are going to introduce that concept, I'd like to be sold or convinced or I'd like to hear a good justification for that, perhaps above and beyond Milton might not trust ICANN to do it well. So, if there's anything else that could kind of back up the need for that independent auditor and the cost that comes with it, I haven't been convinced of it yet, but I'd like to leave the door open for that, but otherwise I'd just scratch that clause there by an independent auditor. Thanks.

JANIS KARKLINS: Okay, thank you. Let me suggest that we put 'by an independent auditor' in score brackets, and then we strike it out, which means that if there will be convincing arguments at one point during the proofreading of the text, then we may remove brackets and then maintain concept of independent auditor, otherwise it would be deleted. It's simply like a placeholder and the text would stay as is except that 'by an independent auditor' would be stricken out but put in brackets, which means an option we could revisit and put it back if needed. So, that would be maybe my suggestion going forward. So, no objections so far.

Let me now then take "Audit of accredited entities." Now, "Accredited entities or individuals must be audited periodically." And I think that here we will use exactly the same formulation throughout the text, "by an independent auditor", or just, "must be audited periodically for compliance with policy requirements as defined in the accreditation building block. Should the accredited entity or individual be found in breach of accreditation policy requirements, it will be given an opportunity to cure the breach, but in case of repeated noncompliance or audit failure, the matter should be referred back to accreditation authority for action. And any audit of accredited entities or individuals should be tailored for…", and then the same thing as in the previous text that you already felt comfortable. Eleeza, your hand is up.

ELEEZA AGOPIAN: Hi, thanks Janis. Sorry, thought I was on mute. Similar comment here, which I think Marc best addressed by suggesting the brackets in that first sentence, whether or not every single entity and individual must be audited or if they are subject to audit, I think that helped clarify the text. But also, in the comment I noted does this require single use requesters as well, how often would the periodicity is, and so forth. Just looks like it's missing some detail that would be helpful for implementation. Thank you.

JANIS KARKLINS: Okay, thank you. Any suggestions in answering Eleeza's concerns on the frequency and auditing of individual one time requestors? So, in absence of hands, I will say look, probably that is a little bit implementational issue. Common sense should guide implementation of this policy in any circumstances and probably it does not make much sense to audit every second individual requester. That said, maybe simply going through and auditing one individual requester, one time requester, simply to see what the policy is appropriate and whether that should be continued that way, or something should be fine tuned as a result of the functioning of the system, and experience gathered during the system. So, that may be reason for or outcome of periodical auditing also one time applicants. So, that would be my thoughts about what you said. Alan?

ALAN GREENBERG: Thank you very much. I don’t know how one would audit individual requesters. I’m not sure how one would audit the accredited requesters, but I’m even less sure how one would audit an individual requester. You’re going to go to their home and inspect all the papers and all of their phone calls to make sure they didn’t release the data, or that they erased it? I just don’t understand the mechanism, and I think it might be almost as difficult to do it with some of the accredited ones. So, I would’ve assumed this is going to work more on a complaint basis than on an auditing basis. Thank you.

JANIS KARKLINS: Okay, thank you. Any other comments, any other thoughts? Brian?

BRIAN KING: Sure, Janis. This is Brian. So, the thought that I’ve had and the thing that’s given me some difficulty on this is that I think it makes total sense to audit the requesters. But it seems, and I was just talking about this with our group last night, it seems that what the audit might want to do is to prove a negative. And so, the audit, if it’s to be effective, should audit to show that you didn’t do anything with the data that you said that you weren’t going to do, sorry for all the negatives in that sentence.

But, I don’t know how you audit for that, I don't know how you can account for everything that someone did with the data and then by process of elimination or some other wizardry show that they did or didn’t do something that they said they wouldn’t do. So, sorry to ramble on that but I wonder if there's some specific way, something that we could search for, right? Could we do ongoing representations, right? Registries, Registrars have to represent every year that they continue to comply with their RRA or their RA, you know? Is that an appropriate course of action for accredited entities and individuals or is there… Just maybe somebody could help me understand how an audit could be carried out that might cover what we want it to cover here, thanks.

JANIS KARKLINS: Okay, thank you for your questions. Volker?

VOLKER GREIMANN: I don't really see the problem here. I mean, ultimately the audit would just work like contracted parties audit works right now. Compliance, ask a couple questions, ask them to show proof. If they do not show proof, it's a failed audit. If they show proof and that proof confirms to other information that compliance may have available to them, hooray, that is passed audit. But if the proof that they show or the comments that they make in response to that do not match information that they have available, for example if y tells them, "Hey, x used that data to do zed.", and they contradict that, then you ask them to explain that contradiction.

It's as simple as that. Of course, you cannot go to their homes as Alan suggested and go through their cupboards, it's documentary evidence that has to be weighed on its merits and if you make a complaint against a party for misusing the data, then you should also provide the auditors with that evidence that you have that they misused that data, and that evidence can then be used against that party that is subject to the audit. And if they cannot diffuse that bomb that is burning, then they failed that audit. Simple as that.

JANIS KARKLINS: Yeah, thank you, Volker. That's actually… For me, this conversation is revealing and where I see that the, not difficulty but missing point… So, this text that is in front of us speaks about audits of accreditation practices of accredited entities, but it does not address issue of an audit of accredited entities, how they treat the information that has been disclosed to them.

And now looking to this text on the screen, I think we need to add that aspect as well since we do audits of documents which accredited entity has provided to identity providers and see whether those documents are sufficient to be issued credentials, that's one part of audit. And then the second audit should be also, or second part of the audit, should be see how accredited entities deal with disclosed information and whether they deal with disclosed information according to policies in place here. So, this is where I see we have a little bit of work to do. I have Alan Greenberg before Alex. Alan G. please.

ALAN GREENBERG: Yeah, thank you very much. I completely agree with what Volker said at the end, that if you have a complaint, then you go to the party and ask them to explain it. Now, I don't know how one can prove that I erased an email messaged that released some information to me or I tore up the piece of paper and shredded it. You can't prove that unless you videotaped your action of doing it.

But asking them to explain it when someone else has claimed that there has been a violation, that's fine. Whether there's an appeal process to that or whatever, I don't know, that's a detail. But that's different than going out explicitly and saying, "We're going to audit you." A reaction to a complaint is a very different thing than an audit triggered by, "Because you're one of the ten, one in ten people that we're going to audit every week." So, I think we just have to be careful on the wording. Thank you.

JANIS KARKLINS: Okay, thanks. Alex?

ALEX DEACON: Yeah, thanks Janis. This is Alex. Yeah, I think…

JANIS KARKLINS: Alex, just a second. May I ask Alan to mute yourself, otherwise there is echo. Alex, please go ahead.

ALEX DEACON: Yeah, hi. That sounds better. Yeah, I just wanted to follow-up on what Alan said. I think really what we need to decide here is kind of when this audit happens, is it based on a complaint, which I think makes sense. Do we specify a random audit for some statistically sufficient subset of requesters? What we currently have is that it's mandatory, it's a must, for every requester on some periodic basis, yearly, and I think that's something that just doesn't seem achievable to me. So, I think if we focus on audits that are complaint-based or even random, I think we'd be in a better spot. Thanks.

JANIS KARKLINS: Okay, thank you Alex. Alan Woods?

ALAN WOODS: Thank you, it's Alan Woods for the record. I mean, an immediate reaction to what Alex just said there, I genuinely think that complaint-based audits is looking at a very, very, very small percentage of people who would actually bother to make that complaint. And that would be looked very badly upon by the DPS because there's not a meaningful review of the system that we have in place. It is a reactive review of the system that we have in place. So, I can't really agree with that. I think what Thomas just said there in the chat is perfect. We should be looking at a mix of different actions, complaints, random audits, and some… I mean, in order to make the robust, we are saying there are safeguards in place. We need to be able to test those safeguards and not just in a reaction to a complaint.

JANIS KARKLINS: Thank you. I think that auditing is already well established. So, there are principles, and professional auditors, even those who may work for ICANN, know all those principles and we should not be rewriting or redeveloping the wheel that already exists and is widely used in business practices around the world. Volker?

VOLKER GREIMANN: Yes, I actually agree with Alex that a yearly or a regular audit of all the requesters is probably not feasible. I am envisioning more an audit system that's similar to the current audits that ICANN carries out with Registries and Registrars where every contracted parties can be expected to be audited once every say three or four years. And probably will also be audited but not every single year. They have cycles where they pick some out, and there will be audits based on complaints, and there will be general audits which will be on a different scale. So, that would work, and I think that has been shown to work in the previous ICANN framework already. So, if we just rely on the existing frameworks, I think we should be good.

JANIS KARKLINS: So, thank you. Look, I think I will ask Staff maybe to amend this part of the text based on our conversation and present it for the next iteration that we will have on this particular building block. And I would like to go further and see, to get down to the bottom of the text until the end of the call. So, with your permission, I will go to audits of contracting parties and I would like to receive reactions to this proposal. "In the audits of contracting parties, as a part of this policy shall be tailored for the purpose of assessing compliance and independent auditor", again, we'll strike it out, "must be given reasonable advanced notice of such audit", and blah, blah. And the same text as in the previous chapters. Sarah?

SARAH WYLD: Thank you, Janis. Hi, this is Sarah. Just wanted to speak to the CPH comment, and apologies for the typo in there, but we noted that as we were going through together the auditing block with the logging building block, that there does seem to be a discrepancy and the contracted parties do not have role in the accreditation block and very limited in the logging block. So, it's a little bit confusing to see them called out so clearly here in the auditing block.

I do definitely agree that the party disclosing the data should keep logs and should be audited on the work that is being done. I just think we don't quite have enough information set out to properly document that here. One thing that might be helpful would be to compare together the logging, auditing, and accreditation blocks to make sure that each group of actor, each actor in that system, has obligations in all three places. Thank you.

JANIS KARKLINS: Yeah. Thank you, Sarah. Indeed, there should be full consistency and the contracting parties do not have anything to do with the accreditation but would be acting according to policies outline in SSAD. And that is the subject of audit, the compliance with the functions that contracting parties are supposed to do. So, that should be reflected here, not accreditation, that's for sure. And this should be also very much linked and consistent with the logging building block on requirements for logging. Yes, Sarah. Please.

SARAH WYLD: Thank you. Yes, I did want to just point out again or clarify, I went through all of the building blocks and I didn't really find references to contracted party obligations. So, we might need to change it. Yeah, as Alex is suggesting, I think what we're referring to here is actually auditing of the disclosing party, which might be the contracted party, but we haven't defined that. Thank you.

JANIS KARKLINS: Yes, not yet. Okay, then my suggestion is let's put all this subchapter in square brackets and we will come back at the moment, we have a functional model or decision on how model will function and what will be the role of contracting parties in that model. Okay, let's see, auditing of logs. So, what type of comments we will get here? So, Marika, you have an explanation on where this text comes from, where your suggestion comes from.

MARIKA KONINGS: I actually don't. Just on the previous, Alex had suggested in the chat as well that for the previous section, emails have been worked already, update the heading so it would read, "Audits of the authorizing entity", a.k.a. the discloser. And then we can maybe then add a footnote to this that section may need to be further reviewed once the group has taken a decision or made a determination on who that entity is to see indeed if the requirements there are sufficient or whether something else is needed, depending on who the discloser is going to be. And of course, we'll move the red brackets but changing the heading may make also further clear what the target of this specific section is.

JANIS KARKLINS: Look, let me… I'm just thinking out loud. We may have a situation where disclosure is made at the central gateway and the request is sent to contracting parties, and contracting parties act on the decision made at the gateway. So, that's one scenario. Then the action in this scenario, action of contracting party also could be audited in principle. So, another scenario is that the disclosure model is made at the contracting party level. So, and in that scenario also actions of contracting parties could be audited for compliance to the policy. Again, that's why I think contracting parties may not necessarily disappear from the heading. Margie, your hand is up.

MARGIE MILAM: Yeah, hi. Margie. Yeah, I think the audits you just touched on is what I was going to say. Which is that there is a role for contracted parties even if ICANN is the discloser in the delivery of the data to the discloser. So, I think all I'm saying is we need to address it later once we know what the role of ICANN will be.

JANIS KARKLINS: And now listening to you, maybe we need to add a chapter or subchapter in this auditing, the auditing of disclosing entity, and describe what the auditing of disclosure decision could look like. Just a thought.

MARGIE MILAM: Yeah, I think so, but as Sarah notes let's wait until we know what the model will be and then that way we can be more specific.

JANIS KARKLINS: Okay. Thank you, Margie. Hadia?

HADIA ELMINIAWI: Just to add, I just wanted to point out that under all possible scenarios, contracted parties will certainly have a role in disclosing the data, whether they disclose it directly or make the decision or not, or indirectly through a gateway, but they will also have a role in there. To your point, we will need also to have some kind of audits to the authorization entity or maybe the gateway, but again we don't know yet the model that we're dealing with. So, maybe we could hang on on the other details and point that, but under all scenarios contracted parties will have a role certainly. Thank you.

JANIS KARKLINS: Yeah. Okay, thank you Hadia. So, let me now look into the auditing of logs. First of all, I think the text should be aligned with the previous text on who does auditing, a third party firm should randomly audit, probably auditor should randomly audit. It's more sample of query logs for compliance with terms and conditions. "Query logs should cite purpose of access, which must be tied to legitimate and legal use of feature of accredited users use case. Audits will be conducted by a third party funded company and logs are to be delivered with the identity of the log origin tokenized or otherwise so that auditing organization cannot see and thus risk identifying methods of an accredited party." So, this is very much different text from what we have had before. So, I see Eleeza's hand is up. Eleeza?

ELEEZA AGOPIAN: Thank you, Janis. This is Eleeza. So, I had inserted a comment from us on, I think, the small sample of query text. Basically, the question is how is this different from the audits that are described above? It seems to be somewhat baked into the audits you had conducted, particularly of the authorizing party or authorizing provider. It just seems like it could potentially be redundant. And then who's logs are being referred to here? In the logging building block, we refer to all kinds of different logs. Is this all of the logs that are described in that building block or is it a set of those? Those are the questions we had.

JANIS KARKLINS: Yeah, thank you, Eleeza. Alex?

ALEX DEACON: Yeah, thanks Janis. Yeah, I think I agree. When I went through this auditing of logs section, and I think it was Sarah's comment or contracted party comment, I think that logic kind of indicates that we should just delete this whole section. I agree with Eleeza, it is duplicative, and it's already covered by the text above so I think we wouldn't lose anything by deleting this and I think less is more in this case. Thanks.

JANIS KARKLINS: Okay, thank you. So, there is suggestion to delete this audit of logs. So, if there is any reaction. There's one in the chat. So, let's for the moment delete that and see whether in the proofreading, we discover that something is missing. It is not deleted forever but it is deleted temporarily. And if I may now ask… So, the conclusion of this reading is that based on this conversation, I will ask Marika, Kate, and Berry to review and to propose edits in line with what we discussed and suggested. And this will be posted for review of the team and we will revisit this building block once again. I am not closing it, we will revisit this building block once again for the final reading as soon as we will be ready.

And with this, I would like to ask Staff to put response requirements building block on the screen. So, now we have about ten minutes remaining, therefore probably we cannot go paragraph by paragraph. My question is, is there anyone on the team who has extreme difficulty with any of the paragraphs in this provided building block? Volker.

VOLKER GREIMANN: Yes, I'm not quite sure because this seems to be all changed recently with edits in various places, so I'm not quite sure if I have read the most current version or not. So, I'm not comfortable with confirming this at this stage.

JANIS KARKLINS: Okay. Alex?

ALEX DEACON: Yeah, thanks. So, this is Alex. Why don't I give an overview of the changes I made based on the action I took in Montreal? I think most of this text was updated, I think, by the deadline I was given but I'm happy to explain this so people can digest it and think about it. The first thing I did was kind of clarify the difference between checking that a request is syntactically correct and also that a request is complete per policy, per our building block. And for each of those I've tried to get more specific in terms of what the response is. Remember, this is the response requirement. So, in the case where a request is not syntactically correct, I kind of created this new term called… That in that case, I'll just highlight it here, an error response detailing the errors that have been detected is returned.

In B, I talked about completeness and in that case I suggest that when a request is found to be incomplete per policy, that an incomplete request response is returned. And then we talk about the response for the acknowledgment receipt, which is in C, which basically says, "Thanks, your request meets the requirements and it has been received." And then in D it talks about response requirements for what I've called disclosure responses, this is the response for when data is returned or denied based on the decisions.

And what I tried to do there is, we've talked about in the automation section, I've tried to capture that some of these responses can be automated and responded to, and some will require manual intervention and I wanted to try to capture that nuance here in D, which suggests timeframes for a disclosure response. The issue is, as with many of our discussions, is that I think D especially really depends on who the disclosure is, whether it's centralized or distributed. So, assuming it's centralized and I've put some square bracketed text that I think makes sense.

And I think those are the main changes that I made here. Again, to pop up even one level higher, my action was to change this text, which we borrowed from the reasonable access section in Phase 1, to be more in line with a system in SSAD, which will use RDAP and some technologies for authentication and authorization. So, hopefully that helps. Thanks.

JANIS KARKLINS: Yeah, thank you, Alex, for this clarification and also putting the pen on the paper as a response to our conversation in Montreal. So, thank you. Marika?

MARIKA KONINGS: Yeah, thanks Janis. This is Marika. When Staff read through this, one suggestion or one sense we had is that a lot of the detail that Alex has added sounds more like Implementation Guidance than policy recommendation. So, we're just wondering if it would make sense to kind of separate this out a little bit like we've done in the logging building block where kind of the general policy recommendations are put up front and then a kind of more detailed how this is expected or could look in implementation is then described either through the language. Or I think James had already suggested as well, a diagram may be helpful. So, we're wondering if that makes sense here to kind of separate it out, the real detailed how does this look like in implementation from the this is the policy that should drive the implementation of this building block.

JANIS KARKLINS: Okay, thank you, Marika? Any reaction to Marika's suggestion? Brian.

BRIAN KING: Yeah, thanks Janis. I think a diagram might be helpful as I've seen suggested in the chat. I think if you break these down, I think everybody sees a lot of words here and that can be scary. I think if you break these down, these all are like two sentences and it's like if in this scenario, then this should happen, and those are policy principles, right? If a request looks like this, then this should be the response. So, I think if I could suggest that we kind of look at these bullets in that sense, it looks a lot less like a long complex story and a lot easier to digest. So, let me make that suggestion and then if anybody wants to do a chart, then that'd be cool, too. Thanks.

JANIS KARKLINS: Yeah, thank you. So, why don't we then we ask Marika and Staff to try implementation what she suggested and then put it out tomorrow that everyone has ample time to look it through and we would take up the final reading of this building block first thing during Thursday call, since we have come to the closure of today's call. And so, I see Alex is also willing to continue writing. So, please feel free, Alex and together with Marika, to continue fine tuning this building block. And on Thursday we will start with this building block, hoping to conclude.

So, we have in principle finalized logging building block, we will rewrite and at appropriate time we will revisit auditing building block, so we will continue working on response building block next time, response requirement next Thursday. On Tuesday we have a Legal Committee Meeting as we agreed on this will be 3 p.m. UTC. And all that remains to me is to thank all of you for active participation, very constructive participation, and wishing all of you a good rest of the day wherever you are. So, thank you very much. This meeting is now adjourned.

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

[END OF TRANSCRIPTION]