ICANN
Transcription
Next-Gen RDS PDP Working Group
Tuesday, 09 May 2017 at 16:00 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. The audio is also available at: https://audio.icann.org/gnso/gnso-nextgen-rds-pdp-09may17-en.mp3
Adobe Connect recording: https://participate.icann.org/p7cfnzbdipw/

Attendance of the call is posted on agenda wiki page: https://community.icann.org/x/EsPRAw

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

Michelle DeSmyter: Well good morning, good afternoon and good evening to all. Welcome to the GNSO Next Gen RDS PDP Working Group call on the 9th of May, 2017 at 1600 UTC. In the interest of time there will be no roll call. Attendance will be taken via the Adobe Connect room so if you're only on the audio bridge today would you please let yourself be known now?

Hearing no names, I would like to remind all participants to please state your name before speaking for transcription purposes and please keep your phones and microphones on mute when not speaking to avoid any background noise. With this I will turn this over to Chuck Gomes.

Chuck Gomes: Thanks, Michelle, and welcome, everyone. Let me start by asking if anyone has an update to your statement of interest? Not seeing any hands I will assume not, so let's jump right into the agenda.

And agenda Item 2 is continuing our deliberation that we started last week, or actually probably the week before, on charter question and a sub Question

5.1, showed gTLD registration thin data be entirely public or shared access be controlled?

Now we discussed that question and kind of did some rewording and so forth of a conclusion, did a poll, so let's take a look at the poll results. Note that you have them in front of you in Adobe. And you have scrolling capability so you can scroll down in it. You can see that we had 38 people participate in the poll. And the results then follow the 38 people including the comments.

Now there were a lot of comments in the poll, which is great; I'm not complaining, okay. But because there are so many we are not going to go through them item by item but I encourage you to glance through them. If you scroll down to the results for Question 2, you will see there that we had 84% agree and just under 16% disagree. In case you are interested, take a look at the comment numbers that are highlighted in yellow. So four out of the six people that disagreed submitted comments.

((Crosstalk))

Chuck Gomes: So you may want to – is that Daniel? Hello?

((Crosstalk))

Chuck Gomes: Argue one audio only, Daniel?

Man: Am I what?

Chuck Gomes: Are you on audio only?

Man: Yes.

Chuck Gomes: Okay thank you. Okay so you know how to handle that, I don't need to explain that to you. So speak up if you want to say something. So comment –

comment numbers 1, 2 and 10 and 11 were by people who disagreed, okay, the other two people did not comment. So if you would like to look at why they disagreed, that might be helpful and we are going to discuss the results. There is pretty strong support for this statement, 84% certainly is enough to assume rough consensus at this stage even though we are not voting at this point.

So what I'm going to do now is open it up for any questions or comments. If anyone who submitted a comment would like to comment further in this meeting, it now is the time to do that, just raise your hand or speak up in the case of Daniel. And if anybody have a question of a comment that's in there, now is a good time for that. Michael, go ahead.

Michael Hammer: Thank you. Michael Hammer for the record. I just wanted to make a comment that where we have, what appears to be a fairly strong consensus, Not saying vote now but voting sooner rather than later so we can start nailing down some of the things where there does appear to be consensus so that we can move on, because a lot of this stuff is interrelated so things we can nail down will help us as we consider other things.

Chuck Gomes: So first of all, we don't resort to voting according to the GNSO PDP procedures, okay? We will at the end assess, the leadership team will assess the amount of agreement. But as we committed at the beginning this process we are going through now we are keeping it relatively informal. Once we get to actually doing a formal consensus call at the end that has to be handled according to the procedures in the working group procedures.

And we will get there, and even that is not a vote in a traditional sense of a vote but at that time we will need to give everybody a chance to consult with their respective stakeholder groups or…

Michael Hammer: Okay.

Chuck Gomes: …or things. And so I appreciate your sentiment. I would like to close things up now as well but we can't do that at this point. Go ahead Michael.

Michael Hammer: Allow me to rephrase. Documenting those items where it appears that there is a strong consensus in listing and referencing for example the poll in question where it occurred.

Chuck Gomes: So we are doing that.

Michael Hammer: Okay.

Chuck Gomes: Yes, and in fact our action item for this particular issue is to conclude that we have at least rough consensus on this point, and that will be entered into our rolling documents that we've been entering those things into so far.

Now what we will do with a lot of those rough consensus conclusions is we will shortly try to turn those into requirement statements where applicable as well. So I think we are going to accomplish what you want but maybe not to the same extent that you said at first. So thanks for the suggestion.

Jim, go ahead.

Jim Galvin: Thank you, Chuck. Jim Gavin for the record. I just want to clarify maybe one thing about the question, just to go on record saying this I suppose, because I actually like Comments 1 and 2 that were there. And I want to say that I agree with both of them. Although I would agree with the statement in principle, that thin data elements should generally be accessible without identifying yourself, I note and the question we put thin data in quotes. And I, you know, just want to say that I'm interpreting that to suggest that we have some rough consensus on what those thin data elements are.

But just as the one comment makes attributed to Marc Anderson here, even I raised the question of dates at one point in time, and he adds domain status to it. I'm hopeful that we are still going to have a more definite discussion about exactly what is thin data at some point in the future. And I guess that kind of speaks to the issue that Michael Hammer was raising. So we're in a place of rough consensus here, but there might be a detail yet to be determined. Would that be fair? Thanks.

Chuck Gomes: Absolutely, Jim. This is Chuck. That's fair. And keep in mind, we're going to look at data elements individually as well so – including the data elements in thin data. We are assuming a specific definition of thin data right now that we've been using for quite a few weeks. But we ultimately need to agree that we at least reach rough consensus that we want to include all of those.

Now if you look at Marc's comment, I just looked at that yesterday, I hadn't seen it before, and the way I understand it is really looking at the – from a registrant perspective, which some of you do too. And he is wondering whether registrant would want all of those things displayed or would at least like to be able to make the decision whether they are displayed. So certainly we can talk about that further. But we will, when we get back to data elements specifically look at them individually. And if we decide to define thin data differently, we can do that.

Any other comments or questions? So what we are going to do then is add this conclusion, rough consensus, temporary conclusions – I'll put those qualifiers in front of it because we won't finalize any of this until we've made a lot more progress, because as Michael Hammer said too, there is so much interdependency, we could come back and revisit any of these as we make other conclusions. Any other questions or comments, let me take a quick look at the chat. You know I'm not very good at that when I'm running a meeting. No, what Lisa says that our working document is updated every time we have one of these conclusions so.

Okay, so I think – I don't think we need to spend any more time on that. You may want to scroll down and to question number 3, which is on Page 5 of the document that is in Adobe there and that was sent out a couple days ago. We were trying to reach any conclusions on this but basically lay the groundwork for following – continuing discussion on this issue of access to thin data. And you will recall, for those that were on the call last week, that we had quite a lot of discussion about anonymity and things like that last week in our discussion, and even the week before.

So we are going to take a look at these three options that you were given in last week's call individually and talk about them. You can see that we had pretty strong support for Option A which was basically anonymity of access. But there were also, you know, a significant number of people that didn't support that. So we are going to talk about that now and see if we can at least on this call reach reasonable agreement with minimal opposition in terms of whether access for thin data elements should be completely anonymous or not.

And as one of the comments pointed out, you may never have total anonymity in the sense that an IP address will be connected through your access and so forth. So let's start discussing just the first one, anonymity, although it kind of is connected to the second one as well but we will get to authentication later.

Greg Aaron, it's your turn.

Greg Aaron: Thank you, Chuck. This is Greg. To set the scene, A and B are options that are kind of the opposite of each other. One is anonymous, one is unauthenticated. So in A you are anonymous. And it says, "as is allowed by Whois." B requires identification. So I wouldn't call that unauthenticated. I don't know if that's the right word. C is about something that is actually related but also completely different from A and B.

Rate limiting and captcha mean – those are two different things. Rate limiting is usually accomplished by IP address but IP addresses often will not be able to be connected with a person who is making an inquiry especially if you are using some sort of a network or VPNs. So I don't want people to think that these are mutually exclusive and there is a lot implied in the choices.

And again, we have to be careful about what definitions people are talking about because for instance in B, I think on authenticated is not the right term to describe what we are trying to talk about in B. So let's define terms and just be mindful of that as we start our discussions. Thank you.

Chuck Gomes: Thanks, Greg. And let's keep C kind of separate from A and B, not that they are not all involved in the same process of accessing data, but I think we put that in there because the issue came up the last few weeks. And there seems to be very little opposition to those kind of things happening for operational reasons and management by the registrar or the registry to make things – to avoid excessive querying and so forth. But let's keep that one kind of separate.

The other two, yes, are very closely related. I don't think they are opposite but kind of in part maybe. And the reason we said on it, what we are saying in B is that the user requesting the data may have to give us an email address or something that we are not going to validate that or authenticate it, and maybe authenticate is not the best word.

That's all we're trying to say in B is yes, we may require some identification but it will be checked. It's mainly to do auditing or something like that whereas in A we've got, you know, we're saying as anonymous as possible. You may just look at a screen, you may not have to query it. Again we haven't talked about methods of access but that's what we are getting out there.

And Lisa, please add more clarity.

Lisa Phifer: Thanks, Chuck. Lisa Phifer for the record. I just wanted to ask whether you'd like to now move on to the handout to begin deliberations because I think our big take away from the answers to Question 3 was really that there was interest in further deliberating on all three of these concepts, three or four…

((Crosstalk))

Chuck Gomes: I think so, Lisa, but let me ask because people have access to the comments left allow a little bit of time if people want to look at the comments if you haven't already. So let's just pause a little bit and before we move the document on the screen and go on does anybody have any questions or comments regarding the results and any of the comments that you want to call attention to on this? And I'll pause for a minute or two while people can look through them if they haven't already.

And feel free if you don't have time to get through enough of these in our meeting today because we are not going to wait too long to go back and look at those and add any comments to our list discussion in the coming days and we will do that. I'll just wait maybe another minute and let people see what's on the screen.

And of course, if you want to made a comment and want to comment on it you are welcome to do that too. Keeping in mind that our purpose of polling in Question 3 was kind of just to get the thinking going on these issues that have come up in the last few weeks and not to reach any conclusions on the poll.

Okay, Lisa, go ahead. Let's switch over. And everybody should have access to the results so you can do those – look at those further on your own. Let's switch over to the materials that were prepared for our deliberation on these three items.

You can see that the first slide is just one we've looked at a lot, kind of shows where we are at, we are looking at gated access right now and pretty much the conclusion – rough consensus conclusion that we just made was in other words do not have gated access for the thin data elements understanding that we will look at some specific elements later in more detail.

Go to Question 2, there is our definition of thin data and examples of it. And you can see the agreement on Page 2 that we reached based on the poll results and that will be added to our running document, okay, gTLD registration thin data should be accessible without requiring inquirers to identify themselves or state their purpose.

If you go to Slide 3, the question is, what steps should be taken to control in data access? And we, staff in particular and the leader – the chair and cochairs, put what you see on the screen there as a starting point. We haven't reached any conclusions, we just thought it would be helpful to facilitate our discussion to start with these. And so you can see Number 1, when querying gTLD been data elements, requester identification should be, and then there are three options, disallowed; allowed but not required; or required.

So what are your thoughts on that? Let's just throw it open for discussion. Go ahead Jim.

Jim Galvin: Thanks Chuck. Jim Galvin for the record. I'm wondering if the purpose of this discussion, you know, we could separate the first two from the second two. I think that, you know, Items 3 and 4 are more of an operational concern and separate from a policy concern about the data itself. And I just would like to put that out there as a suggestion for our discussions the way we go about it before I jump in on talking about one or the other. Thanks.

Chuck Gomes: Jim, I think you know – this is Chuck – I support that because that's essentially what I said in response to your other intervention, then I think that those are. And I look at those as operational; some people don't like that word but that to me that's what they are is operational things done to make sure that there's not abuse of the registry or registrar system so or even the

RDS system if it wasn't related to registries and registrars directly. So I think separating them make sense. So let's do that. Okay?

So any comments? Now what I'll do with a little bit is probably do a little live meeting poll on some of these just to get a sense of where people are. But I think it would be helpful if some people want to talk about Number 1. And if it's helpful to talk about 1 and 2 at the same time that's okay, okay? Otherwise we'll start with 1. So Rod, you're up.

Rod Rasmussen: Yes, I typed a comment in the comment box on the third item. While that has a technical sound to it that truly driven by policy. And I remember this being an area we talked about extensively in the EWG around these kinds of – the kind of access you may be able to provide, whether it's completely anonymous, whether it is some sort of, not necessarily anonymous but the weight of getting at data that has multiple – I'm getting a bad echo here so, losing the train of thought.

But anyways, the idea was you would have – you could have multiple levels of access. And it's not necessarily a technical question as much as rules of the game kind of questions. Yes, I think there's a general aspect to talk to that can be separated but that still is a policy question I think. Thanks.

Chuck Gomes: Thanks, Rod. This is Chuck. Help me understand why we limiting if they – you think it's driven by policy.

Rod Rasmussen: I'm looking at charter Question 5, the third item, how many levels of access. That's what I was speaking to.

Chuck Gomes: Oh I thought – I misunderstood. Okay so bear with me a second. I need to scroll back up. I must have missed…

((Crosstalk))

Rod Rasmussen: I'm sorry, I'm looking at what was on the screen. Sorry.

Chuck Gomes: Okay, so the ones on the – rate limiting is Number 3, right, the third item? Or are you looking at – so when you say third item, I looked at rate limiting that's on…

((Crosstalk))

Rod Rasmussen: Okay, yes, we're talking apples and howitzers here. Yes, I was on the first page which is the gated access question so…

((Crosstalk))

Chuck Gomes: Oh okay, that's why – that's why we're not connecting, okay, all right fine. Then you can ignore my question, okay? So let's go to Scott.

Scott Hollenbeck: Thanks, Chuck. Scott Hollenbeck here. So I'm reading these questions and I'm having a fundamental problem with the way they are structured because generally one does not query and data elements, one submits a query for a domain name. And what you get back may well be described as thin data. So like I said, I'm having a fundamental problem in understanding where we are going with this. It might be better structured as when one submits a query for a domain name what determines what you get back, and that they be measured by whether or not you have provided identification information or no identification information or factors along those lines.

Anyway so I guess what I'm getting at is I think we're going to be talking about this for a while but I just don't know that I see were going to end up in a good place. Thank you.

Chuck Gomes: Thanks, Scott. And your point is well taken that you are really querying a domain name. But if we are going to give access for thin data elements the point is should we allow access and it probably could be worded a lot better without any requester identification for any elements, understanding that they are really querying a domain name. When you are querying the domain name ICANN.org, should you be allowed access without any identification of who you are when you're doing that. So that’s really what we're asking I think. Jim, go ahead.

Jim Galvin: So thanks, Chuck. Jim Gavin for the record. I guess to Scott’s point, you know, I mean, Scott’s right but I think, you know, multiple people have said this, you know, before, some of these things are little awkwardly worded sometimes. And, you know, the wording puts comments and questions in a context for us and so they can be tough to answer.

For me when I read this, this page here of 1, 2, 3 and 4, this enumerated list I’m thinking about it in the context of the poll that we just took. And so the idea is I’m making a query and the expected response is then data elements. And so we are asking these questions in the context of that and so that is the way in which I am going to answer here now.

I’ll respond directly to your question about what we think about these four things. As far as the first two are concerned, it seems to me that given the results of the poll and the general consensus that, you know, then data elements should in general be available broadly, that the best answer in both of those cases is B, allowed but not required I think. You know, I mean, unless we want to go down the path of, you know, absolute anonymity even to the extent that we all know from a technical point of view it’s not absolute but at least conceptually let think about it that way, you know, the best answer for 1 and 2 is to choose B.

With respect to the rate limiting and captcha, and going back to something that Rod said, I think that there are two dimensions to rate limiting. I think that when some people see rate limiting they automatically get concerned about bulk access to data. And my answer to that is I see 3 and 4 as strictly operational issues. They should be allowed but not required, and there should not be any policy about them except to say something like that; they are operational concerns. And, you know, any sort of provider that has to deal with protecting their own infrastructure, you know, they are going to do whatever they need to to protect their infrastructure. And they need to be allowed to do that.

And I don't think that you can create a policy that suggests that they can't do that. And so my reaction to the concerns about bulk access is well, then you just create a bulk access solution. Don't tie bulk access to rate limiting and don't tie it to captcha, you know, create a policy that says you have to have some mechanism for doing that and create a solution for that. And that becomes an independent discussion at some point in the future. So anyway I guess I'll allowed but not required for all of them is kind of where I'm coming from. Thanks.

Chuck Gomes: Thank you, Jim. This is Chuck. And you did what I hoped would happen in the sense that you are sharing views and rationale for these, and you did it for all four questions so that's fine and that's good. I want to go back to Scott because I didn't – Scott, I'm assuming you left your hand up because you had a follow-up so let me allow you to do that now. Just didn't put his hand down. Okay thanks. I wanted to give you a chance…

((Crosstalk))

Chuck Gomes: No problem. Okay Stephanie, it's your turn.

Stephanie Perrin: Thanks very much. Stephanie Perrin for the record. I was just responding to your question about whether rate limitation was a policy issue. And I guess I'm replying with another question. Given that bulk access – requirements to limit bulk access are provided for in the RAA that does strike me as a policy requirement. And my very imperfect understanding of rate limitation is that it is a mechanism to comply with that bulk access restriction so that makes one, a mechanism to serve a policy requirement. Have I got that right? And if not can someone explain to me the difference?

Chuck Gomes: Stephanie, this is Chuck. I think you got it right. As you know, because you've been involved long enough to recognize this, there are things in contracts, and registry and registrar contracts, that didn't necessarily come from a policy development process. They are policy built into the requirements for registries and registrars. So yes, I think you're right, and I appreciate your explanation there. And that helps me understand the point, so thank you for that.

Now everything in contracts, like I just said, are not always the result of a policy development process. If we had to develop policy for everything in contracts it would be crazy how many PDPs we'd need going. So – but thanks, Stephanie. That's helpful. Rod, it's your turn.

Rod Rasmussen: Thanks Chuck. Rod Rasmussen. So Jim kind of got to it as he was walking through the points, most of the points I was going to make. But a couple of thoughts on this. In the first two points, and by the way I agree with the sentiment that it is probably allowed but not required on all of these. But there are some important considerations here.

One – on 1 and 2, you don't want to create a system – I'm thinking of this from policy driving bad design. And you don't want to create a system where if you think about it if we do end up with some sort of gated access regime we probably want to have sort of – you probably want to end up with an interface where you can send your queries in, but the same interface regardless of whether or not it is a gated with purpose, blah, blah, blah all the other, you know, bells and whistles we can come up with thing.

So if you do that then you do something like disallow the A option in the first couple, then you actually have to create a separate kind of query system or at least not track based on the type of query that's being made so you end up a really kind of a convoluted system there. So you don't want policy to kind of get in the way of that.

On 3, the rate limiting thing, I think there is a lot to unpack there. We have – and I think the bulk access is one question. There is also kind of a question around kind of games that we see in the current marketplace today where registrars or registries, but mainly registrars, are providing let say less than adequate access to their systems to the point where, you know, you end up with compliance complaints, etcetera. So there is certainly a policy issue around, you know, you're saying – you can say your defending your system, but if you limit your query to one per day that's not really defending your system, that's just, you know, blocking access to the data.

So there's a balance there, you know, the policy words need to be around reasonable etcetera, etcetera. But there should be something where you have an enforceable element is saying you can't unreasonably withhold access to data based on, you know, claims that you are trying to protect your system. So, you know, we want to be careful in policy there.

Just one last point I want to make, because 3 and 4 actually have an interesting current use case that interrelate the two. If you take a look at some major registrars, I'm not going to name names, they knew who they are and anybody can ask me off-line. But if you take a look at some major registrars the default on port 43 Whois is basically just been data and if you want to get the data they refer you to a Website.

On that Website you have to go through a captcha in order to get that data. So effectively you are creating a system where if you are trying to do systemic automated access, let's say you're running an email MTA type thing and you are trying to determine whether or not to accept email on a brand-new domain or not and the only way you can find out is from querying the system, you might be able to get that data that way. But if you are trying to do something where it's more complex in trying to get data at a large-scale you end up being thwarted by basically a provision of data that is – that requires a manual intervention to get it.

So you do end up with kind of – something to think about from a policy perspective is how you provide data in a way that handles various use cases as long as obviously the data can be obtained via the policy. So there's a few things to kind of tease out of this that the broad principles, sure, but the devil is in the details. Thanks.

Chuck Gomes: Thank you very much, Rod. This is Chuck. And you make some really good points. I think probably we are going to have to be careful how we work, for example, if we decided that choice B for 3 and 4 is a good choice we are probably going to have to reword it a little bit, allowed within, I mean, this is in very good wording but allowed within reason without violating the policy or whatever. We can refine the words later. But excellent points. Thank you.

Michael Hammer, it's your turn. Michael, you may be on you because we are not hearing anything. Michael Hammer, still not hearing anything. So you were fine before, not sure what's going on. We will come back – I'll come back to you, Michael. Let's go to Greg Aaron.

Greg Aaron: Thank you, Chuck. This is Greg. So a few minutes ago we had a good feeling that if thin data – that the data should be accessible without requiring the inquirers to identify themselves. So if that's the case then number 1 and number 2 seem irrelevant to me, both 1 and 2 require the requester to identify himself or herself. Am I…

Chuck Gomes: I get what you're saying, Greg. And it's a good question you're asking. In our meeting last week we put anonymity to the side a little bit, okay, and said we'd deal with that separately. So when the conclusion, you know, going up if you go back up to Slide 2 there where it says, "gTLD registration then data should be accessible without requiring inquiries to identify themselves or state their purpose," we kind of assumed last week in a call, and I hope I'm stating this accurately, that not requiring them to identify themselves doesn't mean total anonymity. Okay?

There could be, you know, maybe they have to send it – this is the probably the way it would happen but maybe they had to send an email so we have their email address, okay? Or would they just look at a screen and that's it and they see the data, you know, kind of like we do today for Whois.

So you're right, but we felt like it was – because there were a few different views with regard to anonymity we thought it would be helpful to nail it down a little bit further. Did that make any sense, Greg?

Greg Aaron: I think I understand the process, and I tried to review last week's notes. But I also think that these definitions are lacking and there are some pretty fine distinctions being made like if I give you my email address I have identified myself.

Chuck Gomes: Yes.

Greg Aaron: Okay, so I'm not comfortable – this needs a lot more work. Because this can be easily…

((Crosstalk))

Chuck Gomes: Let me ask you, Greg, what would be your answers to 1 and 2?

Greg Aaron: What I'm trying to get at is consistency with what came before. Okay so my personal views may be aren't that germane. But what I'm saying is when you say identify yourself, what does that mean? Are you giving me real information? Are you giving me information which doesn't make any difference in which case why are we even doing it? There are a lot of questions there. So I'm not comfortable with – that we have any definitions or that anybody can actually understand what identification means or that we are being consistent with ourselves. So let me state that.

Now, on Number 3, rate limiting is often something that's done for operational purposes. Stephanie assumed that people rate limit in order to enforce a bulk collection provision. Actually that's not always the case and we probably shouldn't always assume that. Registries, for example, rate limit their registrars, so registrars don't flood them with queries or commands and thereby shut down the system or shutout of the registrars. That's another example of rate limiting in action.

To date there are no requirements about rate limiting, don't have to do it and if you are a registry or registrar you are allowed to do it. You are given leeway to manage your system to an extent so that it functions. So that's the current state of play and it has an operational component and that is the way it is currently kind of managed in a lot of ways. Now it could be also used to enforce policies but I don't think that's been the purpose in the past to date.

And as far as Number 4, Rod intimated that captchas are only relevant to web-based Whois. Which are a minority of Whois queries that are made or probably would be made in an RDF in the future. So a captcha is a barrier, it's a very specific kind of a barrier. It does not require anybody to identify themselves in any way, it's just a way to tell if the party who is making the query is a human or not, that's the purpose of a captcha. Thanks.

Chuck Gomes: Thank you, Greg. I may come back to you for more useful wording of the first two or of any of these to be thinking about that, maybe you are to have. Andrew, it's your turn.

Andrew Sullivan: Hi, thanks. It's Andrew Sullivan here. So I think I agree with Greg that I don't – I'm a little concerned in particular about Option B for 1 and 2, because certainly in the case of 2, Option B makes it possible for somebody to create a new barrier that doesn't exist today to some subset of the data that is available today. And I thought we had just agreed that we, you know, we weren't going to – we weren't on board for that. And so that really means that the answer to 2 has to be A, it has to be disallowed. You can't allow people to start putting barriers in front of this stuff if we think that everybody is supposed to have access to that data.

Option – Question 1 involves this requester identification. And I don't understand exactly what that means. But, I mean, supposedly there some email identification loop or something like that, what that really is is a weak authentication mechanism. If it's, I have to give you some data, like I have to give you my name but you don't have any mechanism to check that it's real, then this is less – it's a bad idea, like it's going to create a phony data. This is the kind of high ceremony, low value thing that people sometimes put in place that looks like a good idea but it depends on everybody telling the truth; and on the Internet that isn't a reliable thing you should do.

So I think actually 1 not only should be like disallowed, I actually think that we shouldn't consider 1 at all, it's just a bad idea. And I'm a little concerned about the discussion around captchas because captchas only work for humans, right? The whole point of a captcha is to distinguish between a human and a machine. And there are two problems with captchas, the first is that in fact they are not that good at distinguishing between humans and machines; they're fairly easily gamed.

But the other thing about them is this system is not only for humans. Some of the things that we want from this data is in fact to enable machines to use it in a reliable way and to get humans at a loop. So I think that 4 should be also disallowed for that reason. But the reason in the case of 4 is because I think it is a goal that we are failing to keep in mind that we want to enable certain kind of machine to machine transactions in here while yet protecting, you know, personally identifying information, which was the way we got started on this thin thick work distinction. Thanks.

Chuck Gomes: So Andrew, Chuck following up with what you said. Could I fairly conclude then you would support total anonymous – anonymity with regard to access to thin data elements?

Andrew Sullivan: Yes, I thought that was consistent with the rough consensus that we just heard, but I think that people who want identification without authentication are asking for a system that on the Internet won't work. And so you either have authentication or you don't have – or you don't have any identity at the other end because people will lie.

Chuck Gomes: Thank you.

((Crosstalk))

Andrew Sullivan: Which is a problem in a – sorry. Just one more thing. Of course that's the problem with the correctness of Whois data today, right, that people lie because they don't want their data to be out there. So we don't want to re-create that problem in a new place in a new system.

Chuck Gomes: Thank you. No, you've clarified – that's what I understood, I just wanted to make sure so thank you, you made some good points. Michael, are you able to speak now?

Michael Hammer: I am back.

Chuck Gomes: Yes.

Michael Hammer: Do you hear me?

Chuck Gomes: Yes.

Michael Hammer: Thank you. So, thinking about the discussion – oh, Michael Hammer for the record. I think we are perhaps, and I'm talking about Question 1 and 2 as a start, so we talked about requester identification and we think of somebody putting in an email address or something like that. But we also have things like machine identification, right? So the issue at hand may be slightly different than what we've been talking about with regard to identification.

Switching to rate limiting, there's also I think – Rod made the statement that it needs to be unpacked, and I agree with him. So for example there is rate limiting by individual who is let's say lock-in or cookied, there may be rate limiting by IP address, there may be rate limiting by the querying domain. There may be overall rate limiting by the system. I'm only going to accept so many queries per time interval globally. So we need to think about this perhaps a little bit differently.

And I want to reiterate what I wrote in the chat which is why we tend to think of rate limiting as strictly operational it does have implications when it comes to policy and can be used as a policy implementation mechanism, not just as anti-abuse. That's all I got.

Chuck Gomes: Thanks Michael. And you reinforced something that Rod said, so let's just jump right to Rod.

Rod Rasmussen: Thanks Chuck. Rod Rasmussen. So I've been putting in the chat that we've got – I agree with Andrew and Greg have been talking about in that we've got this idea around – we said that domain data should be made available without authentication. So if you do do B, you could allow – based on that wording some people say while fine, then I'm going to require authentication.

My concern was around being efficient in your query and that if you are in a gated situation where you're asking for data that's not available via policy you should get the thin data as well; you shouldn't have to make a separate anonymous query so to speak for thin data. Just want to make one query and get all the data that you're entitled to based on your purpose at the time.

And if your purpose or you're just asking for thin data then you can do it and not be fettered, so to speak, by the thing. So you end up with a situation, and hopefully I wrote it out in the chat that makes a little more clear, it's disallowed so let's say for Number 2, because Number 1 I agree with Andrew is what's the point. But for Number 2, disallowed however aloud if you are making a more complex – query or something along those lines, so basically you don't have to go and make two queries to the system to get the data you're looking for because that's just stupid and inefficient. Thanks.

Chuck Gomes: And, Rod, isn't it correct that the EWG, that's what they were envisioning? Right?

Rod Rasmussen: Yes, pretty much. Yes.

Chuck Gomes: Yes, yes, that's what I thought. Okay. All right, good, thank you. Okay, Jim Gavin, your turn.

Jim Galvin: Thank you, Chuck. Jim Gavin for the record. I just wanted to repeat the distinction that I had made earlier, and I want to make it big in so that it doesn't get lost. I think that – I've knowledge that there are policy issues that affect the use of rate limiting and captcha. So for example, you know, Andrew was making the comment that captcha is really only useful to humans, well I suppose, but he kind of made that point too. And I view rate limiting, there is a side of rate limiting that, you know, from my point of view applies to operations. And I think that we just need to be careful that we don't restrict the use of rate limiting for operational reasons, you know, protecting one's infrastructure.

But I've knowledge that, you know, people to use rate limiting and captcha I guess that in all things you can create tools and services and such and you can use them in bad ways, right. Guns don't kill people, people kill people kind of thing I suppose, I don't know. I hate to bring that politics in here.

But in that respect we can have a policy that says that, you know, you can't use rate limiting in the sense that you are going to use it as a way to prevent access. And so that's an important consideration. But I don't want to – I just don't want to tie bulk access to rate limiting and captcha. And I feel like that's the path that we are headed down. I want to make sure that bulk access and ready access to a volume of data is a separate consideration.

And, you know, if we need a policy that says bulk access has to be allowed that's fine, but solve that problem. But let's not in the process of solving that problem say that we are not allowed to use rate limiting or captcha because that just is other problems. And so that's the distinction I want to draw. Thank you.

Chuck Gomes: Thanks, Jim. Chuck again. And I'm going to come back to what I suggested before, and if somebody objects please speak up. But can we separate the rate limiting and captcha from the first two and focus on the first two right now? Is that a problem with anybody? Now we are going to come back to rate limiting and captcha, some very good points have been made on multiple sides of the issue, and we will deal with those. But is anybody strongly opposed to focusing on 1 and 2 for the moment, just raise – if you're opposed to that put a red X in the Adobe or speak up.

Okay and again we are going to come back to rate limiting and capture, okay, so because I've learned some things today myself, not that I don't always do that but there's some good points that have been made on at least a couple sides of the issue so that's good.

Okay focusing on 1 and 2, now Stephanie, you can say what you wanted to say and if it involves rate limiting and capture that's okay for just you though.

Stephanie Perrin: Thanks, Chuck. Stephanie Perrin. My point was a more general one, I'm kind of coming back to your response that if we had a PDP process for everything that was in the contracts we'd never be done. And I agree that that's true and

I also am well aware that the registries don't particularly want us NCSG-ers looking over their shoulder when they negotiate their contracts.

However, there are things in contracts that appear to have been passed on as legacy items since the early days of ICANN when they might've been there for, for instance, competition reasons when we had a couple of registrars and not a couple hundred, right, registries. Ditto for registrars.

So we do have a different marketplace. And I'm just kind of putting in a plea that when we look at something that all you gentlemen take for granted, and I say gentlemen because it's mostly gentlemen speaking today, that we have a look at why it's there and whether it makes any sense in the environment today when things have developed so that we can maybe get rid of some of their staff that have policy implications that in my view are, you know, actually violations of law for instance and haven't been queried in terms of the purpose for collection and distribution of data.

And that would not really be the case of bulk access, although I won't claim to understand it well enough to know whether I have an objection to it. I suspect I might but, you know, that'll come later. Thanks.

Chuck Gomes: Thank you, Stephanie. This is Chuck again. And as you know, Stephanie, there are means to do what you're talking about. To the extent that an issue is identified that maybe has just been a legacy contractual term that no longer applies, there are ways of dealing with that. One of them just kind of happened with regard to the Registry Agreement and the amendments that were made to that.

Some of the things that were changed were along the line you're talking about. But there are also – there's also the possibility that there would be policy issues that may now need to be visited because of a change in circumstances. And that can be identified, you know, by the GNSO, by any particular stakeholder group or constituency and raised as a possible policy issue. So I think they're a means to do that and that's certainly reasonable to expect.

So now coming back to 1 and 2, okay, I'm guessing, just from the comments I've heard, we started out with a lot of comments supporting disallowed for 1 and 2 – excuse me, allowed but not required, and more recently the case has been made that they should be disallowed; there shouldn't be any – it should be total anonymity basically if that's the case. Sorry about the interruption. Hopefully our staff will identify that line and mute it. Can you still hear me?

There we go. Okay thank you. Okay so for those that are supporting disallowed for 1 and 2, and I think that translates into total anonymity for access to thin data elements, that's one option. And we can kind of summarize both of them in that option. But for those that still support allowed but not required, I'd like to hear from you how would you get – what kind of counter argument would you give to the total anonymity statement or position? And we probably should come back to some of the chat in a minute, and maybe Lisa will do that now.

Lisa, go ahead.

Lisa Phifer: Thanks, Chuck. Lisa Phifer for the record. I'll try to encapsulate some of the chats on this topic which is that if you have a query that involves potentially more than thin data elements and to disallow identification or authentication then you're also disallowing it for queries that would involve more than thin data elements, that you'd want to be able to make a single query and obtain only the data elements that you are authorized to get to. If you don't authenticate yourself may be all you get is then data elements. If you do authenticate yourself maybe you have access to additional data elements. We are not deliberating on the latter part yet, but that is the rationale for allowing it.

Chuck Gomes: Thank you. Okay so and I think that makes sense but as far as the data is concerned there is no requirement for requester identification even though the identification may be needed for thick data. Did I say that right? Andrew, I was hoping you'd come back in. Go ahead.

Andrew Sullivan: Yes, thanks. So I understand what Lisa is saying and I agree that the way this is phrased in these questions what's happened is we've introduced an ambiguity because of this disallowed verses allowed. This goes back to what Scott was asking about earlier because the actual way that the protocols that we have in the world works is that you've got one protocol and then depending on who you are you get a different answer.

And so it you are unauthenticated then you might get a small answer, and if you are authenticated in some way then you might get a different answer, and maybe it's small in a different way like for instance you bypass rate limit and you don't actually, even the registrar ID perhaps that you get bulk access so that you can tell how old names are, you know, this would be something appropriate for (unintelligible) server to have for instance.

And in another way you might have access to contact data or something like that, like there are lots of different possible possibilities here. But the unauthenticated thing is a simple path and it's just the thin data. And the difficulty is the way it's written here we are talking as though you have an identity sort of implicitly, and then the question is which elements are you allowed to access.

But as Scott pointed out, you know, you don't query for specific elements, you just make a query. And so what we really ought to be saying is something closer to unauthenticated data must have access to this minimal set or may not have access to limited set or something like that so that we have, you know, different options for what happens if you've got a query from an unauthenticated source. That's really I think the way that this would be a little bit clearer. And we wouldn't have this ambiguity about what happens if you are authenticated, can you get access to the subset of data that you would be allowed to have access to. The answer ought to be yes, but the questions as they are phrased sort of prevent that.

Chuck Gomes: Thank you, Andrew. Michael, it's your turn.

Michael Hammer: Okay thank you. So what Andrew was saying in the chat kind of doesn't match up with what Andrew was saying – speaking just now. So for example, and this goes back to maybe there needs to be some minimum required offering in the agreement with ICANN. So if you are an unauthenticated user you get at least X queries per time interval. But then the option of the provider, whether it is a registry or registrar, if you are authenticated maybe those limits get upped or removed. So there's a lot of nuances to this.

Chuck Gomes: Andrew, did you want to respond to that?

Andrew Sullivan: So there are lots of different kinds of limits that could be in place. One of them is the rate, another one is the elements that you would get in return, and so on. But there are lots of different policies that you could put in place, and I use policy in the geek sense, not in the ICANN sense. Lots of different operational rules that you could put in place for how your system operates that would do these things.

But it's one interface, and the point is that what we don't want to have – let me put this another way, when – on Number 2 here, you know, querying and data elements, requester authentication should be allowed but not required. If we do it that way then what that opens up is the possibility for some registrar or registry to say oh no, no, no, we're going to actually put gated access for everything, and then there just isn't access to this data.

And I think that that is not the outcome that we want, and therefore I think that the way that this is phrased doesn't work, even though I think we are all talking about the same thing and I think we've all got roughly the same model, but of course the point of chewing the silver is to try and make sure that that is the case.

Chuck Gomes: Thank you. Stephanie, it's your turn. Stephanie, are you on mute? We're not hearing anything. Okay let me throw something out in my simplistic thinking. Instead of saying querying…

Stephanie Perrin: Hello?

Chuck Gomes: …thin data elements – oh there you are, go ahead, Stephanie.

Stephanie Perrin: Yes, I do know what happened there. It looked like it was talking. Stephanie Perrin for the record. I apologize for making life complicated, I just wanted to point out that the moment you identify yourself in order to pass the gated access screen, the problem that I don't have an answer for is you have to identify your purpose. It is not because you are a paralegal working for a major motion picture organization that you all of a sudden get the next few layers of data for everybody, right? You have to have a good purpose that is accepted. So I just wanted to throw that complication in there. Same for law enforcement, they have to have a purpose. Thanks.

Chuck Gomes: Thank you, Stephanie. So let me throw something out and this may be way off base but I'll throw it out anyway. So as assuming we could come to agreement on total anonymity for access to thin data elements, we should be talking about just looking up thin data elements, not querying, not requesting, just looking them up like people do today.

And then for gated elements, you would submit a query or a request, and then we get into all the other issues there. So if there is total anonymity really all people should have to do is just go to a site where the information is, they obviously have to put in a domain name, and they get the data. There's no request, they are just looking at the data and once they've identified a domain name.

So I guess you could say that putting in a domain name is somewhat of a query but I think it's very different than where authentication would be needed. Michael, is that an old hand?

Michael Hammer: Yes, apologies.

Chuck Gomes: Okay, thanks. So let's try and reach some sort of a tentative resolution on 1 and 2. And help me out on the wording if you can, one way to ask a question that people could respond to in a live little poll here is how many would support total anonymity fourth and data elements as we defined them, understanding that we are going to get back and look at data elements individually, but for now, following up on the rough consensus conclusion that we've already agreed to last weekend today, how many would – and don't respond yet because I'm going to let Lisa jump in, she may have a better way to word it, would support total anonymity for access to thin data elements, okay? Lisa, go ahead.

Lisa Phifer: Thanks, Chuck. Lisa Phifer for the record. I think the problem that we are having, Chuck, is not having a definition of total anonymity and not agreeing on whether that is a requirement or something that allowed. I've suggested a possible requirement framed out of Number 2 here in the chat, which would be in addition to last week's agreement. So last week's agreement was that thin data should be accessible without requiring identifiers, or excuse me, requiring inquirers to identify themselves or state their purpose.

The building on that, there may be a possible requirement that thin data elements must be accessible with or without authentication, so it doesn't require authentication but it allows it. That's one possible way of building on last week's statement.

Chuck Gomes: Any comments on that suggestion? Anybody see a problem with that wording? Okay, you like it, Jim, okay thanks. And Andrew, I'm going to pick on you because – well, I'll call on Greg first, but I'm going to pick on you in a minute as one who, you know, was really supporting without authentication definitely, so that with authentication might be a problem for you so I'd like you to respond to that if you can. But let's go to Greg. Greg Shatan.

Greg Shatan: Thanks. This is Greg Shatan for the record. I do have, you know, problems with the allowed but not required formulation. I think that, you know, first off that creates, you know, some sort of differentiated access by different – based on who the access is coming through or other variables that we haven't even begun to discuss. And, you know, therefore we're kind of engaged in a form of access discrimination where if a party who is providing access is, you know, gating it that is kind of going against, you know, I thought where we stood and certainly goes against where I think we should stand which is with disallowed.

I suppose if what we're saying is that we're going to allow requesters to put their information down for some reason, then that – I don't know why we would do that and that creates a whole load of data protection issues on the other end. And clearly we haven't identified a purpose for that. So I don't know why we'd go there. So I think this sort of neither fish nor fowl formulation doesn't satisfy any concerns; it raises a lot of new ones and gets in the way of the concept of unidentified or anonymous access. So I'm troubled by it. Thank you.

Chuck Gomes: Thanks, Greg. Chuck speaking. Andrew, what do you think about Lisa's wording there? Thin data elements must be accessible with or without authentication.

Greg Aaron: I can live with it. I think that the – I think the reason that we've got into this is because we've got the wrong mental model of how the system – how any actual system works but it solves the problem that I was trying to so I'm okay with it. Another way to put it, you know, that I will say I think is equivalent s so we don't need to change the wording, but the point is that there's a minimum subset of data that anybody can get no matter who they are or what they are or anything like that without authenticating themselves or anything like that. And then there are super sets of that data that maybe accessible under other circumstances.

Chuck Gomes: Thank you. Okay, so we have a statement in front of us, thin data elements must be accessible with or without authentication. If you are comfortable with that put a green checkmark in Adobe. If you're not, put a red X. And Daniel or anybody else that may only be on audio, please speak up. So I see some red Xs, I don't see any green checkmarks. Oh there’s one. Let me scroll down so I can see more. So there’s a couple green checkmarks. So there’s still mixed views.

Daniel, can you tell us why you put a red X? And you can keep entering your checkmarks or Xs.

Daniel Nanghaka: Daniel for the record here. There is (unintelligible) – hello, can you hear me?

Chuck Gomes: Yes, it’s hard to – it’s a little hard to understand, I’ll mute myself just in case it’s our two lines that are causing that. Go ahead, Daniel. Daniel, we’re not hearing anything now. Would you try again please? Okay, I’m not sure what’s going on with Daniel, but let’s go on – we’ve got a hand raised. Andrew, do you want to jump in?

Andrew Sullivan: Well, actually I was going to try to put Greg Aaron on the spot because he says in the chat that this could be interpreted – reason I haven’t put my checkmark or anything is because he put that there could be two ways to interpret this, and I don't understand what the two ways are. And so now I’m – now I don't know what to say. So that’s why I would like an explanation.

Chuck Gomes: Yes, let’s go to Greg Aaron, okay?

Greg Aaron: Hi, Andrew, this is Greg. So the evil lawyer can interpret this to mean that thin data can be accessible with authentication or it could be accessible without authentication. And what it means is you can have either. It's inseparable in other words. You could say this means thin data elements must be accessible with authentication. Your other option would be without authentication and either of those would be possible.

((Crosstalk))

Greg Aaron: The language…

Daniel Nanghaka: Yes, Daniel here. Can I say something?

Greg Aaron: Yes, well it's both. And that means that you could have mandatory authentication and that's not what we want.

Chuck Gomes: Yes, I got you. That was kind of bothering me too. This is Chuck. Daniel, go ahead.

Daniel Nanghaka: Yes, the reason I put the red checkmark is because one thing is – this data here – the thin data can be accessed in both ways. So when the requester makes an authentication, they can say to access the data and (unintelligible) if is not accessible there is still another alternative way of accessing this data here. And that's why – meaning that there are multiple ways of accessing the same data and that's why I put the checkmark.

Chuck Gomes: Thank you. Appreciate that. Greg Shatan, go ahead. Why'd you put a red X?

Greg Shatan: Thanks. Greg Shatan for the record. It goes back to the same issues that I expressed before and also what I put in the chat that as the other Greg – my concern is that it can be read to allow a requirement of authentication by a given access point, even though it's not a requirement that they have authentication or identification. So I think, you know, not being an evil lawyer but carrying out the requirements of clients who may or may not be evil in the eyes of some, if I wanted to use this language to put a requester identification requirement in place in a given place, if I'm, you know, controlling a data access point, I could use it that way. And so that's not what we need to say.

Chuck Gomes: Yes.

Greg Shatan: I think we need to be a lot clearer.

Chuck Gomes: Thanks.

Greg Shatan: About what we are actually saying. Thanks.

Chuck Gomes: Thanks. Okay, and I'm going to rush a little bit because we're running out of time and there's a couple other things we have to close on and it'd be nice if we could get closure on this. I'm not sure we'll succeed. But, Nick, have you got a quick comment as to why you put a red X? I hear your mic. I think. Nick Shorey?

Nick Shorey: Hi, can you hear ?

Chuck Gomes: Yes.

Nick Shorey: Can you hear me, Chuck? Okay, yes, I share the concerns expressed by the two Gregs really. I think it can be read a couple of ways. And I think generally I think (unintelligible). Thank you.

Chuck Gomes: Thanks, Nick. Steve Metalitz. Are you on mute, Steve? Not hearing anything. So and if you get audio, Steve, jump in if you would please, and I'll go to Alan in just a second. But the question I'm having, and based on all the discussion, and I really don't have a issue one way or – a personal issue one way or another on this. But why wouldn't we just say thin data elements must be accessible without authentication, unless of course you disagree with that.

But what does the with or add? And maybe Lisa, you can explain why you did the "or" but before I go to you, let me go to Alan.

Alan Greenberg: Thank you. Something Greg said wearing his evil lawyer hat, sorry, that's a joke, (unintelligible) something. There's a difference between saying the data is accessible without authentication and you shall not request authentication. There are services around on the Web that will fetch Whois information for you, but they in fact ask you to sign on before they'll do it. Now that doesn't mean the information isn't available from somewhere else on the Web without authentication, but if we are going to use words which end up saying you must not request authentication, that's getting into a territory that I think we don't want to be in. So again, it comes down to exactly how these things are worded. Thank you.

Chuck Gomes: Yes, and we're probably going to have trouble reaching some closure on this. But, Lisa, could you respond real quickly, and then we're going to have to jump to a couple other agenda items and unfortunately continue this discussion next week, and maybe we can come up with a couple poll items based on the discussion that'll help us, not to conclude anything, because we're not there yet I don't think.

But Lisa, what does adding the "with" or "without" instead of just "without authentication" add? Why was that added? Is that the – I'll let you answer.

Lisa Phifer: Thanks, Chuck. I'll keep it brief. Lisa Phifer for the record. The reason for allowing both alternatives is to not preclude either. So in last week's agreement, there would be access to thin data elements without authentication, without requiring it. But the adding the "with" or "without" allows for authentication and again, the reason is so that when a request involves more than thin data it could still be authenticated.

Chuck Gomes: So it seems to me we need to be more specific and I know it's going to be a longer sentence, but if that's the reason – and I suspected that was what the reason was, we probably need to say that. And let's try as a leadership team, to work that and come out with a statement and maybe we can even poll it just to get people to think about it. But let's take that as an action item for the leadership team to try and tweak that to accomplish what you're trying to accomplish and avoid what several people that had red Xs pointed out as a problem. Okay?

We won't discuss that any further because we're out of time or just about out of time. But we have a couple agenda items that we need to get to. Guys, I know we didn't reach any rough conclusion today, but the discussion in my opinion, was very valuable. A lot of really good points were raised. And we'll come back to those. And try and next week make some more progress on this.

The ccTLD questions and plan for distribution, Susan, you have a quick comment there?

Susan Kawaguchi: Yes, we've taken all of the edits and comments into consideration and finalizing the document and should get – start getting those questions out to the targeted ccTLDs this week.

Chuck Gomes: And what I did as chair, just to be transparent with everybody, I followed all the discussion, okay, but I asked Susan to go ahead with her small group, make some decisions, let's get it out and they will send the final questions to the group so everybody's aware. And then if we need to follow up with some other things that some of you have suggested, we can do that later. So that was kind of a command decision I made so that we get that moving and hopefully get some responses back from some CCs. And thanks for all the suggestions for additional CC operators on that.

And David, you – it looks like you're on, do you want to give a quick update on the authoritative issue? I don't know if you have audio, David, or not, we're not hearing anything. David Cake? Okay, let me – because we're out of time let me jump in. So again what I asked David yesterday to do with Andrew and probably Sam too if they want, who's been helping a lot on that issue to come up with a specific recommendation and rationale for us by the end of the week that people can look at so we can hopefully discuss that in our meeting next week.

Jumping ahead then, I think we as a leadership team have an action item to come up with some wording to tweak Lisa's wording a little bit and maybe get out a poll on that if for no other reason maybe not to reach conclusion; if we do that's fine, but just to keep the thinking going on that.

Note that our next meeting is – and I'm going to jump to you, Lisa, just a second, I'll just go ahead and say our meeting next week is at our alternate time, 0500 UTC. Hope a lot of you can still make it. And even though that will be a less desirable time for some. So let me note that and turn it over to Lisa.

Lisa Phifer: Thanks, Chuck. Lisa Phifer for the record. I just wanted to add a couple of actions. We had – from last week's poll the action to go ahead and incorporate the working group's agreement from last week in our working document. And assuming that we put a poll out to test some of the phrasings that we came up with in today's call, then all working group members have an action to participate in that poll.

I'd also like to suggest for any working group members especially those that are new, if you have an interest in attending a one-hour tutorial on some of the reading material that's required for working group members, I've put the link in chat of a small survey that we're running just to assess what topics people would like to cover in that one hour tutorial and get a sense of interest in particular dates so that we can get that on the schedule.

Chuck Gomes: And, Lisa, that also went out in an email to the whole list, right?

Lisa Phifer: Correct, it did.

Chuck Gomes: Yes.

Lisa Phifer: But just to raise awareness that survey is not this week's poll, it's just a survey to assess interest in the tutorial. And that closes this Friday so if you're interested in helping to frame what a tutorial might be about or what day it would be held on or dates, please respond to that poll.

Chuck Gomes: Yes, thank you very much. And thanks, staff, for putting that together in follow up to a need identified several weeks ago. Anything else before I adjourn? Thanks again, everybody. Have a good rest of the week. And we'll talk on the list and in our meeting next week. Meeting adjourned. And the recording can stop.

END