COPENHAGEN – ICANN GDD: Privacy and Proxy Service Provider Accreditation Program Implementation Review Team (IRT)
Saturday, March 11, 2017 – 13:45 to 18:00 CET
ICANN58 | Copenhagen, Denmark

AMY BIVINS: I'm Amy Bivins from ICANN staff and this is the Privacy and Proxy Service Provider Accreditation IRT Meeting. I know this is a long meeting but we're going to do everything we can to make this interactive and conversational. We'll have roving mics around when we start asking questions, so please participate and watch for these guys in the front and they'll have the mics.

So this is our agenda. From now until about 3, we have a few topics. We're planning to checking on our timeline and I'll also share some information about the updated Policy document. And then, we'll talk about Third Party Request and Abuse Reports and then we'll take a break. From 3:15 until about 4:45, we've invited the Public Safety Working Group to talk about their progress on creating a proposed law enforcement disclosure framework. And, in the initial agenda we sent you where you had plan to talk about some other questions but we're not quite ready to do that yet, so we're going to extend the Public Safety Working Group discussion a bit.

We're planning to take a break at 4:45 and we'll come back at 5. And then, from 5 to 6, we have a discussion related to registrar questions. I wanted to ask the IRT members that are up here to introduce themselves. And anyone else in the room who's on the IRT, if you could introduce yourself, that would be great, too.

ROGER CARNEY: Hi, this is Roger Carney. I'm with Go Daddy.

ERIC ROKOBAUER: Hi. This is Eric Rokobauer from Endurance.

GREG DIBIASE: Greg DiBiase Amazon registrar.

THEO GEURTS: Theo Geurts, Realtime Register.

DAVID HUGHES: David Hughes, Recording Industry in IPC.

AMY BIVINS: Do we have any other IRT members in the room?

UNIDENTIFIED MALE: [Inaudible] DNS Africa.

JANELLE MCALISTER: I'm Janelle McAlister from Mark Monitor.

AMY BIVINS: So, do we have anyone else? No. So, we have drinks and snacks up here. Please help yourself. Raise your hand anytime if you have questions or comments. We want to hear from you and a lot of this is going to be focused on discussion, so the more participation, the better. Otherwise, this maybe a very short meeting.

So, an update on our project timeline. As you may remember, our initial project plan projected to this implementation could be complete by the beginning of 2019 but based on the IRT's recommendation, we're working to speed that up a bit. Based on our current pace, it looks like we should be able to have a draft Policy document and contract ready to post for public comment by September of this year. And, after that, the timing will really depend on what kind of changes are needed in response to the public comments.

The next slide shows the topics that we know we have to cover before we get to public comment. And, we're estimating that

we'll be discussing the Policy document through most of March and April. In May, we hope to be discussing the law enforcement framework and the de-accreditation process and then we'll be reviewing the contract in June and July.

This schedule could be impacted by other factors. For example, if we're directed to do additional work on transfers, that could extend the timeline. But based on these deliverables, it looks like we should be ready for public comment in late August or early September.

Do any of you have comments on this timeline or questions? Do you think it looks reasonable especially the IRT members who are here?

JENNIFER GORE: Hi, this is Jennifer Gore, ICANN staff. This is aggressive. We acknowledge that and we are delivering it based upon the IRT's request to condense it down from the three-year timeline to a one-year timeline. With that, with each one of these milestones that have to be hit including let's say just taking the contract review in the consideration. That's 60 days.

So, it would be really helpful for you guys to everyone in the room – all the IRT members – to comment on this timeline whether you believe it's conservative, whether you think that

there's disclaimers that we need to mention. But these are some pretty heavy initiatives that we need to cover in a very short period of time in order to reach the public comment by the end of August. Thanks.

GREG DIBIASE: So, I agree it's impressive and as long as we are under the – operating on the understanding that we can extend the timeline if work comes up that takes longer, then I have no problem shooting for this but as long as everyone knows that we can retain flexibility, that's fine with me.

JENNIFER GORE: Hi, just to acknowledge what Greg was saying is absolutely. We're taking direction from you, as the IRT, as far as the timeline is concerned but we're just noting that these are major milestones that we need to complete and if obviously more time is allowed, then we're flexible and we'll adjust accordingly.

AMY BIVINS: Thank you. And also, for anyone in the Adobe room, if you have questions or comments, please feel free to type them. And, if you're on the audio bridge, you can also raise your hand to speak in the room. We have someone monitoring the room, so

we'll be sure… And we want you guys to participate, so we're calling you, too.

Do we have anything in the chat?

The next slide shows a more expanded timeline to show the full year. If we go out for public comment in late August or September, that would put the public comment period closing in October roughly if we use the 40-day time period that's usually used. Depending on how close we're getting to the Abu Dhabi meeting, we might want to leave the public comment period open until after that to see what sort of input we get at that meeting.

After the public comment period, the end date of this IRT is a bigger unknown and it will very much depend on what we needed to do based on the public comments. This shows a scenario where there's very little but needs to be changed based on the public comments. If that's the case, we might be able to announce the final requirements before the end of the year but that really depends on the feedback we get from the community.

We'll be assessing the timeline quarterly roughly just to see where we are in checking with the IRT and then we'll be publishing that so the community can see it.

Does anyone have comments about the longer expanded timeline? Or do we have anything in the chat?

JENNIFER GORE: Hi, I just want to mention Sara Bockey, Go Daddy, mentioned that she believed that the August 2017 timeline was very aggressive and we acknowledge that as well, and we'd be willing to be flexible on that based on the milestones that are reached. But we are trying to stick with the direction that was provided by the IRT to reduce the timeline from three years down to one.

AMY BIVINS: Thank you. So, does anyone else in the room or in the Adobe room have comments on the timeline before we move on? We'd have a lot of discussion about the timeline so far and so we would just want to provide as much opportunity as we can for you guys to weigh in and talk about it. So, while we're here, you all please participate. The more discussion we have, the better. But if not, we'll move on to the next topic.

Steve Metalitz is in the chat. Raise your hand. You can go ahead, Steve. Your audio should be working. Steve, if you're talking, we can't hear you. The tech folks in the back can help us with that. In the inner room, if you can type your question or comment, we can read it in the room.

So, we can move on to our first substantive topic. We wanted to update you on the Policy document because you haven't seen it lately. As a reminder, we begin discussing a draft outline of the policy last year. And so far this year, most of our discussions have focused on questions related to the Policy document.

Based on the IRT discussions, we've modified the structure of the Policy document a bit, which you'll see soon. The second draft is significantly shorter than the first draft, which you saw in pieces when we were talking about questions. We decided to leave many of the details for the contract to avoid duplication, which will streamline the Policy document.

We'll start reviewing the Policy document later this month and I hope to be able to send it to you relatively soon. It probably won't be this week but hopefully in the next couple of weeks.

Does anyone have questions about the Policy document? Nothing.

JENNIFER GORE: Given the number of IRT members in the room and those at the table, how many have actually read it? Can you raise your hand? You guys read it?

UNIDENTIFIED MALE: Yeah.

JENNIFER GORE: I'm just looking for feedback on it obviously because we're 90% on the way there.

AMY BIVINS: Our second draft, when you see it, it will be roughly 90% complete. There's one section that won't be ready yet but it will be approximately 90% complete at least in draft form when you see it.

JENNIFER GORE: Thanks, Amy.

PAM LITTLE: Pam Little from Alibaba. I have a question about the timeline in relation to public comment period. Is that about the Policy document or the Contract document or both? Thank you.

AMY BIVINS: Thank you. The timeline is up on the screen. Because we're trying to pursue an expedited timeline, we're planning to put the Policy document and the Contract out for the same public

comment period instead of doing two separate ones to try to save time there.

JENNIFER GORE: Just to give you a little background on that is we work initially put out a three-year timeline and per the request of the IRT, we try to condense that down. So based on that, we're trying to consolidate the comment period to include both entities. But please respond.

AMY BIVINS: Thanks, Jennifer. So, what was the rationale for pushing or condensing the timeline? Sorry, I'm coming [to] this late, so I didn't have any background. Sorry.

JENNIFER GORE: Would any IRT member like to answer that question before I attempt to respond?

DAVID HUGHES: Many of the representatives in the business community and IPC in particular feel very strongly about this particular issue. I mean, it's business critical for many of our constituents, so we would like to see this happen as fast as possible.

AMY BIVINS: Thank you.

Comment from Steve Metalitz: "The rationale was the expiration of the interim's privacy/proxy specification on January 1st, 2018."

Thank you, Steve.

Thanks, everyone. Does anyone else have questions or comments on the Policy document or the timeline or public comment periods? Okay. So, we'll move on to our next topic.

Third Party Request and Abuse Reports. I want to emphasize for this section that we need discussion and participation from the IRT members. We have a lot of questions for you in here, so I'd encourage you to please participate, otherwise, this will be a very short session, which may be good but we need the discussion to happen, so please participate.

So, the final report had recommendations related to several types of third party request including abuse reports, [rebate] request, IP-related request, and review request. In the final report recommended that a uniform set of minimum mandatory criteria that must be followed for the purpose of reporting abuse and submitting requests should be developed.

So, based on that recommendation, we plan to do the following. First, we will compile all of the known requirements for each type of request from the final report. Then, we want to work together to identify potential gaps in criteria, thinking about who can submit a request, what does the request need to include and what does the provider have to do in response to the request. And then, where our minimum criteria need to be developed, we will consider the working group's intent and known industry practices to propose solutions.

So, we want to hear from you, does this process sound like what the working group intended for us to do during implementation? Because we really want to confirm that before we move forward with this process. And also, those in the chat as well. Any IRT members or anyone who is on the working group?

DAVID HUGHES: I think this is in principle what we had agreed to in all our previous discussions and it reflects the group's consensus as far as I can tell.

AMY BIVINS: Thank you. Do we have some other comment?

ROGER CARNEY: Yeah, I agree. I mean, I think this is the process that we're looking for and then measure this whole – be too long of a process. Hopefully, we've been in business long enough that we know most of these issues and how they get resolved, so I think this should go fairly quickly.

AMY BIVINS: Theo?

UNIDENTIFIED FEMALE: That was an old hand.

JENNIFER GORE: If you don't mind if I could put some of the registrars. I had to ask you specifically regarding these questions, the step two. Your thoughts on the intent of the final report regarding who can submit, what does the request need to include and required provider to actions and response. It's helpful to know that there is processes set up today the way that this is handled. But there will be some privacy/proxy service providers that are not necessarily registrars. So, it's imperative that you help us clarify these points.

So, if you'd be willing to elaborate now, it would be appreciated. Or any of the IRT members in the audience. We have

microphones. We can bring it to you. Just please raise your hand. Steve, if you're on the phone, please go ahead.

STEVE METALITZ: Can you hear me?

AMY BIVINS: Yup. Thank you, Steve.

STEVE METALITZ: My only question, which I actually had mentioned on the list was about the first bullet under step two, who can submit a request. And, I just want to clarify, we're not trying to restrict and prevent people from submitting these requests. We're just talking about classifying the types of request that are received. Thank you.

AMY BIVINS: Hi, Steve. Yes, exactly. We're obviously we're not trying to limit who can submit request generally to accredited providers. This was more focused on the types of request that we will have that are designed for specific entities. For example, intellectual property-related request will have criteria for who can submit the request. We expect that request from law enforcement. We'll

probably have criteria-related to who among law enforcement qualifies for submitting the type of request.

I hope that's helpful. Does that help, Steve?

STEVE METALITZ: Yes, thank you. That's helpful. I would point out that for intellectual property request, that work is basically done in the illustrative disclosure framework that was attached to the working group report. But I understand that for certain types of request, there might be qualifications if who can submit them.

I've also point out on this in general. There's actually been a lot of discussion of this involving some of the people on this IRT on the RDS Working Group list. There's been discussion about what abuse request should contain and so forth. So, perhaps we can incorporate some of that in carrying out this process that you have on the slide. Thanks.

AMY BIVINS: Thank you, Steve. As you'll know later in the slides, you noted that the IP framework is very thorough in terms of the recommendations and you're correct. That's why we actually will not be talking about those specific requests today because we don't have questions. So, that will make this meeting a little

bit shorter. But yeah, you're correct that we have very thorough recommendations there.

Does anyone else in IRT… Okay, we have questions.

GURI DHANOA: Hi, it's Guri Dhanoa. Just a question. Can you elaborate just a bit more on who can submit a request? And, you mentioned law enforcement like you said there'd be specific criteria in regards to who can submit or how's that going to work?

AMY BIVINS: Thank you for that question. And I think that is a question that we will have to resolve with the IRT. As you'll see later in this meeting, we have requested that the Public Safety Working Group develop a proposal for how the process will work and we think that criteria for who could submit a law enforcement request will probably be part of that. But it will be developed through a proposal from the Public Safety Working Group and then working through it with the IRT to be sure that it's consistent with the intent of the Policymaking Working Group.

GURI DHANOA: Thank you.

AMY BIVINS: Does that help?

JENNIFER GORE: I just like to remind everybody to state your name and affiliation for the transcript.

AMY BIVINS: All right, do we have questions or comments from anyone else?

DAVID HUGHES: Amy?

AMY BIVINS: Yeah.

DAVID HUGHES: I'm sorry to go back on the agenda. I just wanted to double check. At one point when we're talking about the review process and the deadlines we were discussing August and it was mentioned that we might consider pushing it back if we had to review at the Abu Dhabi meeting. But it doesn't start until the last days of October, so I would just like to caution against this losing two months if possible.

AMY BIVINS: Thank you. And, this was really more contemplating that. For example, if the public comment period do not open until September, if we were to start getting close to the deadline where we had a deadline that was, for example, like the week before the Abu Dhabi meeting, we might want to leave it open but thank you.

Theo, did you want to say something?

THEO GEURTS: Just a few things. So, as Steve mentioned, we already put a couple of things in place for IPC making request when it comes to reveal or disclosure. When we're talking about abuse, we really need to define what abuse is because we don't want to end up as registrars or as privacy service providers in a situation that abuse gets reported to the wrong entity. That would be actually pretty bad because in the case of phishing malware, it could increase the uptime of such practices and that is definitely something we want to avoid. Thanks.

JENNIFER GORE: So, Theo, are you recommending that a subgroup be formed in order to define abuse? What are you proposing as the next steps?

THEO GEURTS: That could be a solution though from a high level. We pretty much know where abuse should be reported to. So, I don't think there needs to go a crazy amount of time into this. I think we could do this in a subgroup flush it out a little bit and then just structure it, what goes where, it shouldn't be something very complex but it should be in the PDP itself where it should end up. Thanks.

AMY BIVINS: Thank you, Theo. And, I just want to point out we'll actually be talking about this topic in about five slides, maybe fewer. So, what exactly is abuse, so hopefully we'll get some input to start that process.

UNIDENTIFIED FEMALE: A comment from Luke Seufer: "Regarding step three, I briefly met with AFNIC, the French registry, who has such system in place since years and they would be ready to provide and present such data if asked."

AMY BIVINS: That's great. And we'll follow-up on that. Thank you.

Does anyone else have questions or comments on this process?

So, we will move on and we started by identifying all known requirements from the final report. It applied to all types of third party request and I've put them here on the next two slides for you. With respect to receiving reports, the final reports of that provider should have the ability to categorize reports and that reporting form should include space for freeform text and that provider should publish a link to a request form containing minimum mandatory criteria for request, which we will be developing through this IRT.

The final report also so that providers must publish and maintain a mechanism for requesters to follow-up on or escalate request and so this will be for all requests.

The final report also had terms of service requirements related to third-party request and these are on the screen. The report said that terms of service shall indicate clearly the grounds upon which customer details may be disclosed or published or service suspended or terminated. In terms of service, it shall indicate clearly that requesters will be notified in a timely manner of the provider's decision to notify a customer of a request and

whether or not the provider agrees to comply with the request. So these we know are going to be baseline requirements for all types of request.

Is everyone with me so far before we get into the specific types of request? Does anyone have questions?

GURI DHANOA: Guri Dhanoa with the RCMP. I'm just looking there it says, "Indicate clearly that request will be notified in a timely manner of the provider's decision and notify custom of the request." Is there any caveats in regards to reporting to a customer?

AMY BIVINS: Thank you for the question. On the slide, it should have said it will be notified of whether they will notify or they will notify the requester of whether or not they will notify the customer. And there probably will be caveats especially related to law enforcement request. There's a recommendation that I believe that providers should keep request confidential if they request it too by law enforcements, so that will be one caveat.

GURI DHANOA: Okay. Because I had to look at some of the documents produced and –

AMY BIVINS: Sorry. Can you hold the microphone, sir?

GURI DHANOA: Yeah, sorry. Yeah, so I had the review of some of the documents and in certain areas, it indicates that – to the caveat for law enforcement and then, as you keep reading further down, so there's certain inconsistencies in regards… I don't know if I should be posing that question right now or maybe you're going to cover that later on. But there are certain inconsistencies I found like where it says for law enforcement purposes whether a customer will be notified. But then further down, it just indicates that the customer would be notified. So, I just want to bring that to the forefront, to your attention.

AMY BIVINS: Thank you. We will certainly keep that in mind and if there are specific places when we start talking about specific law enforcement requirements where you see that and want to point it out, please do. We're taking the approach that where the recommendation is specific with request to the law enforcement, we would follow that above the more general recommendation. But obviously, we'll be running it by the IRT to ensure that the way we're proposing to implement was

consistent with what the working group intended. So, we'll be asking where it's unclear, what was intended here to confirm that we get it right.

GURI DHANOA: So, how are the registrars going to take – if we have a legal authorization and it indicates there that not to notify the customer because of the sensitivity of the investigation – now, who decides on that? Like who's decision is it? Like if the customer data is going to be… or if the customer is going to be notified? Is there a consistency base in regards to the registrars like if one registrar is going to comply and say, "Okay, they're going to notify the customer," and another registrar who abides by the legal authorization will not report it? So, is there going to be some sort of basically consistency in regards to how the registrars are going to follow the policies?

AMY BIVINS: With respect to law enforcement request, that is a topic that we will be discussing in the context of the law enforcement framework when we're trying to set it up and design it. With respect to requests that are not from law enforcement, we'll be discussing that as well. But the way the final report was written seems to leave discretion to the provider in terms of

notifications to customers in many cases but we'll be running through all the requirements with the IRT to ensure that we're reading the language and the final report consistently with what the working group wanted.

GURI DHANOA: All right, thank you.

AMY BIVINS: Yes, and as we're talking about the issues, please raise them. We're going to be talking about law enforcement issues in a little while on the agenda, so, it may come up then. So, please –

We have Steve Metalitz on the phone.

STEVE METALITZ: Yes, thank you. Just in terms of the last comment, there isn't really a requirement that all privacy/proxy service providers follow the same policy here. So, you might have a situation where one privacy/proxy provider would handle it differently than another one. What's on the screen is that that should all be set out in the terms of service. So that if a requester, someone is going to make a request, they will know whether or not the customer will be notified of that request.

I assume that in most cases, most privacy/proxy service providers will notify customers of the request, again, leaving aside law enforcement. But this should be spelled out in the terms of services and so as terms of service are publicly available, a requester will know that in advance before they make a request and can decide how to fashion a request accordingly. Thank you.

AMY BIVINS: Thank you, Steve. Does anyone else in the room or in the chat have questions or comments?

So, we will move on then to the first type of third-party report and we'll be talking about abuse reports. So, going through the questions that we talked about earlier that we're asking with respect to the various types of request, the first question is who can file an abuse report? And there were no restrictions on that in the final report, so we're not planning to have any in the final requirements.

How can abuse be reported? The final report did not include a requirement for this and so we need to work within the IRT. There was language in the final report that reference similar to the RAA in some places. And so, we're going to be asking about similarities and differences between RAA requirements.

The RAA requires registrars to have an abuse reporting e-mail address. However, the final report had some language and it's on the screen but seem to indicate that privacy and proxy providers might be able to have some other option other than an e-mail address. It reference potentially using forms and that would be I think to address spam going to the abuse e-mail address.

And so, our first – a substantive question I guess for the IRT today is based on the language in the final report, do you think that the abuse reporting process could have the option of using a form instead of a dedicated e-mail address? And we're asking because the language in the final report, it wasn't clear on that, so we want to hear from you.

Greg.

GREG DIBIASE: Yes, I think that language should allow providers to use a form and e-mail address just invite so much spam that it creates unnecessary inefficiencies and if providers are allowed to use forms, I think that's better for both parties. It's more specific on what information is needed for the report and it reduces spam, so providers can prioritize the reports coming in, so I think that's a no-brainer that forms should be allowed.

JENNIFER GORE: Thanks, Greg. So, just to clarify, are you saying that the preferred method or the only method would be forms that e-mail is or is not allowed?

GREG DIBIASE: E-mails should be allowed as well.

AMY BIVINS: Thank you. Theo, did you have your hand raised?

THEO GEURTS: Yes. When we're talking about e-mail addresses and WHOIS output when it comes to abuse, that we might want to look at that more in-depth and we come to it because I think it would be really confusing to have a registrar abuse e-mail address and a privacy service provider abuse e-mail address. Again, we are going back to the question what is abuse. Thanks.

AMY BIVINS: Thank you, Theo. And, just to point out, you mentioned that we should look at it I guess when we get there but we're here, like we're asking it now. And, with the expedited timeline, we're trying to address these issues and sort of them out and that's

what we're doing here. So, if you have questions about using an e-mail address versus not using an e-mail address, this is the time to really talk about it, so please share further input if you have it, you or anyone else in the room or in the chat.

Roger, is your hand raised?

ROGER CARNEY: Thank you. I was just going to second what Greg said is, yeah, and definitely forms should be one of the options. I'm not going to not recommend e-mail. If someone wants to use e-mail, that's fine. This inefficiency thing, if they don't get that many, that's fine. It seems to work okay. It's good for them. So, I would say a form should be allowed in our policy.

So, as far as what Theo mentioned, it's interesting about the abuse contact and just thinking off the top of my head as he's suggesting that that registrar abuse contact in WHOIS would be replaced by a proxy provider abuse contact if it was protected under proxy?

JENNIFER GORE: Theo, would you like to address that question? As Amy said, this is the time to have the discussion and clarify.

THEO GEURTS: So, actually that is very interesting what Roger is mentioning there, replacing an abuse address, I'm not sure how that works in reality. That's definitely interesting to explore perhaps a little further. Thanks.

AMY BIVINS: Do we have a comment in the room or question?

RUSSELL WEINSTEIN: Russ Weinstein from staff**.** I had a question for the IRT along those lines. If the registrar is the privacy/proxy provider, are we envisioning just a single common method of submitting abuse or complaints or distinct between the registrar function and the privacy/proxy function? I think from the public perspective, I would think a single method would be preferable.

AMY BIVINS: Roger?

ROGER CARNEY: Yeah, maybe it seems straightforward from the public standpoint but it would be a lot easier and more efficient I would think from a processing perspective. It would just be one or more of those filters that we could use in saying, "All right, these

deals with a proxy issue and not a standard issue on any domain."

So, to me, I would think they would probably be different, abuse contacts if they were available.

JENNIFER GORE: Just to confirm what you're saying, Roger, is that you see a separate set of abuse contacts required if the privacy/proxy providers also a registrar? Were you saying that the same abuse processes that are in place today for the registrar would also then satisfy the requirements for the privacy/proxy service provider?

ROGER CARNEY: What I'm saying is I think that should be an option for the registrar to to have one or both or one or multiples for the proxy.

JENNIFER GORE: Thank you, that's noted. How do you foresee abuse complaints being addressed by a privacy/proxy service provider that is not a registrar? And that's a question for anyone in the IRT.

AMY BIVINS: Thanks, everyone. And, we'll be talking more a bit later about the issue of providers that are not affiliated with registrars, so we'll probably get back to that, too, hopefully.

Does anyone else have comments about the mechanism for reporting abuse?

DAVID HUGHES: I'm thinking it's not my problem per se but it has been raised in the past that the abuse of the abuse records can become a problem and I wanted to just ask the registrars if they think that a form would mediate that problem. I don't know.

I certainly think a form can be helpful but that doesn't mean it should be required because different registrars have different operations and priorities, and size frankly. So, from certain registrar's decisions, being able to implement a form, yes, it will help. But making a requirement seems like overkill because I can't speak to all registrar operations that e-mail address might work for some companies.

JOTHAN FRAKES: Hi, my name is Jonathan Frakes and I'm the CEO of a registrar called Private Label Internet Kiosk but I've played a policy role in a number of registrars over the years. Towards the point of

abuse of the abuse, as long as there could be a threshold defined to determine what abuse of abuse is to where there might be a circumstance that the bulk abuser person could be recently ignored or filtered. And so, there would be room for something like that to filter that.

And that a form may not be precluded from using [captcha] or some sort of an automation filter. I think that that I would suggest that those might be reasonable mechanisms to forward abuse of abuse. Yeah, thank you.

AMY BIVINS: Thank you. Does anyone else in the room have comments? Howard?

[HOWARD]: This is [Howard] from ICANN staff. Just some pleasant opinion. I think forms and also e-mails should be allowed for registrars and I think the requirement should be that those reporting mechanism should be obvious for the reporter say if they're using an app, a mobile app like they're selling the domain names through the mobile app, it should be like from page of their life. After reloading, we're obviously placed on the app or sometimes they do it through I say the public account of their WeChat accounts. It should be a very easy access for those.

So, I think the requirement can be something more targeted to not just the mechanism of reporting but more towards that it should be easier too for the reporter to find. So, here I think with the report requirement, actually, we can see the alternative reporting options, which is we should give them the registrar the option to do it besides e-mail and form, and possibly other means to accommodate some of the either the registrar or the PM people [wider] according to the local situation. But the requirements should be defined that it should be easy to find when the reporter trying to submit the report.

AMY BIVINS: Thank you. Do we have comments in the chat?

UNIDENTIFIED FEMALE: We have a comment from Griffin Barnett, and Griffin says that he agrees that use of a form or an e-mail point of contact for reporting abuse is okay. For a form, they'd want to see ability to upload or attach documents as evidence supporting a report. Steve Metalitz says, "Agree that, 'easy for the reporter to find' is critical, whichever mechanism is used."

AMY BIVINS: Okay. Does anybody else in the room have input on the mechanism for reporting abuse before we move on? Okay. The next question that we have on abuse is how to define abuse. Thank you, Theo, for raising this a few minutes ago.

The final report gave us a starting point for this. It suggested starting with the new gTLD registry agreement PIC specification and the Beijing communiqué from the GAC.

So this next slide has a lot of text on it. You don't have to read it. The point of this is to show you that the list of abusive activity that were referenced in the final report are basically identical. The only difference between the list and the Beijing communiqué and the PIC specification was that the PIC specification added the word abusively before operating botnets.

The definition of abuse in the PIC specification included distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity that's contrary to applicable law. So we want to open it up to you, the IRT members and anyone else in the room about this abuse definition that's in the PIC specification or the Beijing communiqué.

There would be a potential benefit to using the definition that's in the PIC specification because it's already in an existing ICANN contract that would provide some consistency across the contracts. Our question for you is, what would you think about adopting this definition of abuse form the PIC specification? Do you think that this would work for privacy and proxy providers, and is this what was intended? Or did the working group intend, and do you think we need to do further work on the list of abusive activity? Theo?

THEO GEURTS: Thanks. So actually, when I'm looking at this definition of abuse, I would actually think this should be reported to registrars, most likely hosting providers, but not to any privacy/proxy services, because most of the stuff in here defined by this definition is in the case of a third party privacy provider not able to do anything about it. A third party privacy provider cannot take down a domain name that is distributing malware or a botnet or phishing, so most of this stuff is not applicable to them in my opinion.

Copyright infringement however, and piracy, that could be applicable to those privacy providers. But for the rest, I think it's all up to the registrar and hosting companies. Thanks.

AMY BIVINS: Thank you, Theo. And we'd be really interested to hear from other IRT members about this as well. Given that this is the definition that the final report pointed us to, this is where we felt like we should start. So we really need to hear from you about your thoughts about what would be appropriate to include in the definition here, keeping in mind that the final report told us to start with these definitions. Steve, you can go ahead on the audio.

STEVE METALITZ: Thank you. Can you hear me?

AMY BIVINS: Can you speak up just a little bit, Steve? But we can hear you.

STEVE METALITZ: Can you still hear me?

AMY BIVINS: Yes.

STEVE METALITZ: Sorry about that. This is the starting [inaudible] Theo's comment [inaudible] the thing that privacy/proxy service provider can do, this abuse is [inaudible] is these are all going to be violations of the term [where] privacy/proxy service [inaudible] so they can terminate that service [inaudible] contact [inaudible] for their customer. So it's potentially [inaudible] these forms of abuse. I agree that intellectual property [inaudible] that's really what we're looking [inaudible] we're not asking the proxy provider [inaudible] we're asking them to let us know who is [inaudible].

So potentially could [inaudible] types of abuse as [inaudible] although I would leave it to those [inaudible] in combating these to say whether that's [inaudible]. Thank you.

AMY BIVINS: Thank you, Steve. Theo, would you like to respond to that, or anyone else?

THEO GEURTS: Yes. When we are talking about abuse and in terms of a violation of the contract or of the privacy service, I think that is a question that can be asked after the incident has been resolved. If we are looking at URL infection, most likely the privacy service provider customer has no idea what's going on and is most likely not a fraudster or a criminal or anything of the like.

So when we're talking about violation of such terms of service, that cannot be defined within this proposed definition of abuse. So again, we still are required to actually investigate what is abuse and what goes where when it comes to in terms of reporting abuse. Thanks.

JENNIFER GORE: Theo, appreciate that. I think there's definitely a need for the definition of abuse and the actions associated once abuse has been determined. So with that, again, I plead to the IRT – and it's the reason why we're here – to help us define if this definition that we have put forth that has been previously agreed upon is not acceptable or we have not reached consensus on this. Please tell us what would be added, removed or revised definition. Or if there are particular pieces of this that you have issues with, please raise it now. Thanks.

AMY BIVINS: Greg?

GREG DIBIASE: I'm actually okay with using this as a starting point, knowing that as Theo mentioned, the registrar might not be always able to respond to the abuse. But these are certain – if we're defining

abuse, this makes sense. I guess the one clause in there that I don't really know, the deceptive practices, I don't know what that means. Is that someone lying? So I guess that seems kind of vague to me, but in general I'm okay with it as a starting point.

AMY BIVINS: We've got two people in the room.

UNIDENTIFIED MALE: Yes, I'm [inaudible] from India. This proposed definition of abuse is fairly good, except the last line, I have [my wonder]: "Otherwise engaging in activity contrary to the applicable law." It is quite debatable. Thank you.

AMY BIVINS: Thank you. Pam?

PAM LITTLE: Pam Little from Alibaba. I have a question about trademark infringement. I was wondering why you would need to resort to this framework or this regime to get the underlying registrant data. Because you can do that through the UDRP mechanism where a provider could seek that information, and usually

registrar would just reverse the data to whatever the underlying registrant data is. That's one question.

The other one is the concern that Greg already mentioned about [forging] or deceptive practices. This is very difficult to determine from a service provider's perspective, or even from a registrar's perspective. So that one, I have a little concern about being included in that definition. Thank you.

AMY BIVINS: Pam, there's a response from a remote participant to one of your comments, and it's from Griffin Barnett who says, "It is helpful to be able to investigate the underlying registrant before reaching the point of filing a UDRP complaint, hence why using the abuse reporting mechanism is a helpful preliminary step." Theo?

THEO GEURTS: Thanks. I'm not too keen on deceptive practices being mentioned there. It's vague, it'll lead to discussion, so I think this should be removed. And just to point out there again, if we are talking about abuse and we're talking about registrars and privacy providers and third party privacy providers, we're going to mix up the responsibilities of what the abuse should be reported to, and that should be clarified also when we move

along with this to make sure that we end up at the correct parties. And this can be quite confusing, being a registrar but not being the privacy provider as it is being carried out by a third-party provider. So that can get quite interesting there. Thanks.

AMY BIVINS: Thank you, Theo. If you were going to clarify this, how would you do it? You or anyone else in the room. And we have one comment in the chat, too.

JENNIFER GORE: A couple of comments. I think this is in response to Pam's question. Steve Metalitz says, "This process should be a faster and less expensive way of obtaining this information compared to initiating UDRP. And Michael Flemming says, "There are mechanisms that allow for the domain takedown that this definition is tied to, but that does not include things like malware or phishing."

AMY BIVINS: Okay, so who else in the room has thoughts about abuse or this definition of abuse? To start, we've had some comments about

the language about deceptive practices. Does anyone like that language in the definition? And if so, can you tell us why?

DAVID HUGHES: For the record, I don't like or dislike it, but deceptive practices is a legal term of art, and depending on jurisdiction, I'm sure that there are some pretty specific definitions. If that is what the group is looking for, then when we get to that work, we should further define deceptive practices. Or if fraud covers the concerns that the concerns that the constituents have, then we can rephrase it. I think that when we get there, we'll deal with it.

NICK SHOREY: Hi. It's Nick Shorey for the record. Sorry I was late, first of all. And then just on this, I recall – and Theo might recall as well – having a similar discussion about terminology in the specification 11 group that we've got. It might be worth us sort of digging through the e-mails and correspondence, and recalling what came out of that, because it's exactly the same question. And there might be something that we get out then, so I'll take that away.

AMY BIVINS: Steve, your hand is raised again. You can go ahead on the audio.

STEVE METALITZ: Thank you. Yes, this language came from the GAC originally as you can see from the Beijing communiqué. It's in the PICs, which means that the vast majority of registries have obligations based on this, so that's why it makes a good starting point. Yes, if it can be specified or clarified further, we're very open to that, but that's the basis for this. And I think it's important to remember, here we're just talking about the kinds of abuse that people can try to bring to the attention of the privacy/proxy service provider.

This doesn't necessarily obligate the provider to do more than receive it and look into it. It doesn't necessarily mean they have to, if you will, adjudicate it. But I'd also suspect that the terms of service of many privacy and proxy service providers today probably have similar language to this. So this is bringing to the attention of the privacy/proxy service providers something that might violate their terms of service. So while I don't think this language is necessarily essential, I think there's a reason that it's here and it has some pedigree. And we should keep in mind that here we're just talking about what kinds of complaints can be received. Thank you.

AMY BIVINS: Thank you, Steve. Theo or anyone else, do you have a response to any of the comments that have been raised since, or do you have suggestions for things that you would recommend that we consider looking at in this definition, or suggestions for potentially improving it? Again, we're raising this topic today for discussion. We're trying to discuss it now and not in the future because we're trying to move ahead with designing these requirements, so if you have input, now really is the time to provide it to us. Obviously, we'll also be following up with the other IRT members on the list who aren't here today, but we want to hear from you and take advantage of being here in the same room to really talk through this. So, please.

JENNIFER GORE: I just would like to remind everyone that when items come up like this that are being discussed, if we can't reach a consensus or it stays open, that that just further delays our timeline.

AMY BIVINS: Thank you. Does anyone else have comments on the definition of abuse? Anyone in the chat? Okay.

DAVID HUGHES: I guess the question on the table is, do we have consensus that this language is good enough to be the basis to move to the next phase? That's just the question.

PAM LITTLE: I guess the question would depend on what the reporter actually needs to provide in addition… It's one thing to agree on the definition of abuse, but when the reporter actually files a report, is there a requirement to provide evidence to support that request or the alleged abuse? My understanding is all the provider needs to do is reveal the underlying registrant data, that's all it is required. If the evidence is provided, or what is evidence threshold or criteria that needs to be provided when someone files a report? Thank you.

AMY BIVINS: Thank you, Pam. I'm glad that you raised that question, because we really want to turn that back to you. Because our follow-up question to this is, do you see any other gaps where minimum criteria are needed for abuse reports? So we want to hear from you about this is what we're starting from from the final report, but with respect to issues like this one, what should be submitted in an abuse report? That's what we want to talk to you about today.

So for everyone in the room, do you see this as a need in terms of implementing an abuse reporting requirement that we have criteria for what exactly should be submitted with an abuse report? And while we're asking this question, also any other gaps you may see in what actually needs to be included in the abuse report. Pam, would it be your recommendation that they have specific information that needs to be included in an abuse report?

PAM LITTLE: If I'm a provider, I'd definitely like to see some supporting evidence. It is my customer's information that I was contracted to protect, or the privacy of the information. Now I'm required or being asked to reveal that data, right? So I think it is incumbent upon me as a service provider to see what's being alleged against you with evidence. Does that make sense?

AMY BIVINS: Yes, thank you. I will probably follow up to ask what types of evidence. If we want to mention that evidence should be provided, to give examples at least. But I'd be interested to hear what others on the panel think, especially those who work for registrars who are experienced in receiving abuse reports. That would be helpful.

GREG DIBIASE: I think from a registrar perspective, the most important thing is allowing a registrar to set their criteria for determining what is a valid abuse report. So if in our abuse reporting form, for example, we say we need the fields like the URL, allowing that flexibility for the registrars to require that to process an abuse report, I think that's what's needed. I'm not sure we need to list out as a requirement in the policy everything that's needed for an abuse report. We need to allow the registrars the flexibility to define what we need in the form or the reporting process that we have, because we're looking for the relevant information to be able to respond.

JENNIFER GORE: Thanks, Greg. I just want to clarify, obviously today registrars have flexibility regarding materials that are provided by the reporter to support abuse complaints, and you're stating that for privacy/proxy service providers, you'd like them to be provided with the same criteria to allow them to determine for themselves what's supported and not supported. Correct?

GREG DIBIASE: I'm saying that providers need to be allowed to request certain information to deem an abuse report valid, to know, to be able to identify the abuse and take action.

JENNIFER GORE: Correct. I just wanted to clarify it was privacy/proxy service providers and not registrars. Yes, thank you.

GREG DIBIASE: Privacy/proxy service providers. Excuse me.

JENNIFER GORE: Thank you. Yes.

AMY BIVINS: Comment from a remote participant, Griffin Burnett: "I support using the PIC language as our definition, also I would be open to trying to refine some terms if necessary, for example, deceptive practices. We may be able to look at case law and agency guidance, for example from the U.S. FTC to try and see if we can refine legal terms of art like that." And I believe Steve Metalitz has his hand raised, so please go ahead.

DAVID HUGHES: I just want to reiterate something, I don't know, Steve Metalitz or somebody else already mentioned. There's already an obligation to comply with this language in the existing contract, so I don't have a problem with defining what information is required, or even having a discussion about further defining exactly what deceptive practices is. Mostly just to make everybody's life easier. But I think we need to agree on this language. It's already something that the parties are compelled to comply with anyway. So I don't mind discussing the details, but I think we have to get past this or we're just going to get caught in a loop.

AMY BIVINS: Does anyone else in the room have comments, or would you like to respond? Alright, does anyone… Steve, is that a –

UNIDENTIFIED FEMALE: [inaudible]

AMY BIVINS: It's an old hand? Greg is a new hand?

GREGORY DIBIASE: For the purpose of moving on, and when I'm looking at the definition of abuse, if you could tweak the language to say take out deceptive practices or add fraudulent or deceptive practices that amount to activity contrary to applicable law. As it looks right now, they're separated. If the deceptive practice is illegal, then yes, I'm okay with that being within the definition of abuse. But if it's just a deceptive practice, I think that should be taken out for clarity of abuse reporters. But then I'm okay with moving on.

AMY BIVINS: Okay, thank you. Does anyone else in the room have comments on this? Anybody in the chat?

I want to let you know we're running a little bit behind schedule, which is good because we're having discussion. We had invited the Public Safety Working Group to join us at 3:15. We have a few more questions on abuse reports that we're going to get through, and then we're going to shift gears and talk to the Public Safety Working Group. And then we'll get back to third party requests, if that works for everyone, hopefully. And we'll give everyone a break too as soon as we get through these last couple of questions on abuse reports.

Okay, so our next question when we're looking at the recommendation on abuse reports is what is a provider required to do once it receives an abuse report. The final report said that a provider must maintain a designated point of contact that is capable and authorized to investigate and handle a request. But that's the only explicit requirement from the final report.

We see this as a bit of a gap to work on an implementation. The language in the final report seems to be similar to the RAA in some places where it talked about abuse, so we're wondering whether the working group intended for us to follow the RAA language where the language in the final report wasn't different, or if you wanted us to develop minimum criteria completely separate from the RAA requirements.

So generally, our question is for you – and in the next couple of slides, we'll go through a couple of RAA requirements, but we just want to hear about the working group's intent in terms of following the RAA requirements or abuse versus coming up with different requirements. So please speak up. Any registrars ion the room? What do you think about – Greg?

GREGORY DIBIASE: I don't think we need to create any requirements beyond the investigate and respond appropriately within the RAA. I think

that allows for flexibility, that will allow registrars to respond. Sorry, providers to respond.

AMY BIVINS: Okay. Thank you. What do others think? Darcy needs a mic?

DARCY SOUTHWELL: I think your question though is what the working group thought, and that's exactly what we thought, was to mirror the RAA.

AMY BIVINS: Okay, great. Thank you. Does anyone else have comments on this? Anybody in the chat?

JENNIFER GORE: Just thank you for the clarification, because that's what we're seeking in order to be able to move forward on these open-ended questions.

AMY BIVINS: Okay, so on the next slide, we have put on the screen a couple of RAA requirements. We just want to hear from you about whether applying them to privacy and proxy providers would be what was intended by the working group. It seems like based on the

discussion so far probably, but we want to confirm with you. The first requirement on the screen is rewritten from the RAA to apply to privacy/proxy providers, and it would state something similar to this, if not exactly.

"Providers shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse." The RAA just uses the word registrars instead of providers, so that's what we substituted here. So our question for you is, would a requirement that a provider take reasonable and prompt steps to investigate and respond appropriately to claims of abuse be consistent with what the working group wanted us to do here?

DARCY SOUTHWELL: What question are you trying to answer from the final report? I guess I'm not really sure.

AMY BIVINS: The question that we're asking now – and it's not directly from the final report, but it's that you told us just now that you intended for the requirements to generally mirror the RAA requirements, and the question is, this is one of the RAA requirements. If this was written to apply to privacy and proxy providers, it would look like this. The question is, is this what the

working group wanted, or is this what they intended when they were writing recommendations about abuse reports? Is this what they expected that the requirements would be?

Because this is what the requirement is in the RAA.

DARCY SOUTHWALL: Thanks, Amy. I actually think that it's not an all-encompassing answer, because for example the final report has a copyright infringement complaint framework in it. So I think there are some differences. There's not a single answer to abuse reports. I think there were some differentiations in the final report.

AMY BIVINS: Thank you. There's a comment from Steve in the chat.

UNIDENTIFIED FEMALE: "Capable and authorized to investigate and handle is pretty close to investigate and respond appropriately." Also, Steve notes that the RAA language is consistent.

AMY BIVINS: Thank you. Would anyone else like to comment on this? Okay, and a follow-up question would be whether the working group intended any greater specificity here beyond the RAA

requirement. We wanted to ask. We heard from you that generally, the working group intended to mirror the RAA requirements, but just to be 100% clear, was there any intent to be more specific here than what's in the RAA? Anyone?

JONATHAN FRAKES: Hi. Right, so I don't have any problems with this, gratefully, with as my registrar, and I don't offer proxy services, but I do have exposure to this. I think the topic came up earlier, and it's really a sensitivity to me, because often with the abuse of abuse, folks have you chasing Frisbees sometimes without a lot of effort or burden of threshold of proof. So the topic comes back to the abuse of abuse, and leaving some room in this that there's a threshold or burden to prove the abuse report, if there's a requirement that they shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse.

It doesn't necessarily include room for if there's abuse of abuse, for them to determine that they didn't have to make a determination, or they didn't have to work on this. Thank you. Did that make sense?

AMY BIVINS: It did, thank you. And we'll certainly keep that in mind when we start actually drafting proposed language to talk about here, and we will probably be asking more for the IRT's input about how to define this and deal with this. But we'll keep it in mind. Does anyone else on the IRT or anyone else have comments, questions?

UNIDENTIFIED FEMALE: There's a comment from Steve.

AMY BIVINS: Okay, there's one more comment.

UNIDENTIFIED FEMALE: One more comment from Steve Metalitz. "The RAA are general requirements, but as Darcy noted, there are specific standards for IP complaints and might be more specific requirements for law enforcement, etc."

AMY BIVINS: Yes, exactly. And thank you for clarifying. Okay, so one more requirement from the RAA, that we are – next slide. We wanted to ask about applying here to privacy/proxy providers, and this is really long, so I'm sorry. But the RAA requires that registrars

publish a description of their procedures for the receipt, handling and tracking of abuse reports, and registrars are required to document receipt of and response to all abuse reports and maintain records related to such reports for the shorter of two years, or the longest period permitted by applicable law, and during such time shall provide records to ICANN upon reasonable notice.

So our question for you is, would applying this to providers, is this consistent with the intent of the working group?

DARCY SOUTHWELL: I'd have to go back and review the final report, but I don't think that we talked about this. And to kind of clarify what I said earlier, I was answering a very specific question about applying RAA standards. I wouldn't say that we wanted to take the RAA and completely mirror it in every case. I think in this case, I don't think we discussed this. What we discussed was more about terms of service and being very transparent with registrants to understand how privacy/proxy services work.

I'd have to go back and check the final report, but if you're saying it's not in the final report, then I don't think the working group considered this.

AMY BIVINS: Okay, thank you.

JENNIFER GORE: Darcy, thanks for that. Since a few are stating that this possibly is a gap, we're identifying that this may be a gap, how does the IRT want to address this?

DARCY SOUTHWELL: I think this is something we need to discuss among the IRT members. I don't know how many are here today. I think we definitely put a framework in for IP complaints that sort of addresses this, and I believe there are some standards in there for how we disclose within our terms of service what that framework looks like. I don't know how the IRT would feel about creating something the PDP didn't provide for, and that may not mean – it's not necessarily an actual gap in what needs to happen.

JENNIFER GORE: Agreed or acknowledged, so the action item is for the IRT to discuss whether this should be addressed or not addressed. Is that correct? Okay, thank you. Appreciate that.

AMY BIVINS: Thank you. So I think our question to you is, do you think this is a gap that should be addressed? And we can discuss it again, but this is why we brought it up today, was to discuss. Anyone? Any of the registrars or anyone else on the IRT?

UNIDENTIFIED FEMALE: I have a comment from Steve. A comment from Steve Metalitz. "Agree with Darcy on this. Not specifically discussed. These look like best practices for providers to follow."

AMY BIVINS: Anyone else? And we'll discuss these again on the list, obviously. I'll be sending around a summary after the meeting to tell the members who aren't here what we talked about, and we'll keep discussing this. Okay.

Since we're a little behind schedule, we're going to take a quick break because the Public Safety Working Group folks are here to talk to us, and then we'll get back to third party requests after we talk to them. But let's take a break until 3:30 and try to be back on time so that we can go ahead and start that discussion. Thank you.

Okay, everyone. We're going to get started again in just a couple of minutes.

All right, everyone. We'll go ahead and get started. I'd like to welcome Nick Shorey, who's here with us, to talk about the Public Safety Working Group's work.

As some background on the topic, as you know, the final report included a detailed disclosure framework for intellectual property-related requests. The working group but ultimately did not create a similar framework for law enforcement requests. The report did include a few recommendations related to law enforcement. There's a requirement that providers at a minimum relay requests from LEA official and third parties containing allegations of abuse.

The final report stated that accredited providers should comply with LEA requests to keep a request confidential where this is required by applicable law.

The final report also included some minimum requirements for any future LEA framework. The requester must agree to comply with all applicable data protection laws and to use any information disclosed solely to determine whether further action is warranted to contact the customer or in a legal proceeding. The framework should exempt disclosure where the customer has provided or the provider has found specific information, facts, or circumstances showing that disclosure would endanger the customer's safety.

In December, the Board directed the ICANN organization to encourage dialogue between this Implementation Review Team and the Public Safety Working Group to address GAC concerns during implementation.

In response, we recruited a subteam to focus on LEA issues, and 16 IRT members have signed up. If anyone else would like to sign up, you're more than welcome.

We think that the most efficient way to develop an LEA framework would be to have the Public Safety Working Group develop a proposal that we can then define within the IRT to ensure that it is consistent with the intent of the policy recommendations.

So we drafted a request to the Public Safety Working Group, requesting that they develop a proposal. I asked the LEA issues subteam to review the document in early January, and then we sent it along to the Public Safety Working Group.

I'm going to turn it over to Nick now to talk about the status of their work. Hopefully you guys have lots of questions for him, too.

NICK SHOREY: Thank you, Amy. Good afternoon, everybody. My name is Nick Shorey. I'm a member of the GAC for the U.K. I've been involved with the Public Safety Working Group to try to lead the development of this strawman proposal for you all.

Building on what Amy said, and just to take it back and get the context for why we're here and why we care so much, I'm sure many of you will recall that, last year, when the PDP final recommendations came out, the GAC submitted some advice to the Board, requesting an opportunity to engage with the IRT to hopefully address some outstanding concerns that we had with the final recommendations, which we felt still needed to be addressed if possible.

Those particularly were around law enforcement and consumer protection authority requests for information from providers maintaining the ability for confidentiality, not disclosing to the customer that there's been a request received. The reason for that is an operational sensitivity and safety of individuals.

There was also a question of jurisdiction, where the GAC felt that there was a need for potential further clarification.

The ICANN Board, in response, said, "Well, okay. Go and sort it out with the IRT." So here we are. As Amy said, she has handed to the baton to us to hopefully take a first stab at trying to

develop something that we can bring back to yourselves and get the discussion and get the language down.

So what did we do? I launched a call for volunteers at the backend of December from the GAC and from the Public Safety Working Group, and we've now got a small but perfectly formed team of people working on this and considering these issues.

Yourselves developed a guidance document for us, which was really, really helpful, so thank you very much for that. We're really keen to create something that obviously addresses our concerns but also stands alone as a really positive document and provides some real clarity for all parties on how governments engage on these issues.

Attached to that guidance document, you also referenced the IP disclosure framework and suggested that as a starting point. That's been really, really helpful as well.

So we've gone away within our team. We've looked back over our advice, back to the RAA. We've consulted this IP disclosure framework document and taken your guidance as our starting point and tried to look at what is relevant from this IP disclosure to us, what's not relevant, what additional information we think that we would need to add in there, and also, without trying to preempt too much, what we think we need to include that is

beneficial for yourselves. So I think we've got some of those things listed on the slide there: definitions of requirements for acceptable disclosure, etc. – all that kind of stuff.

So we've taken that IP disclosure framework document. It has a series of headings and all that kind of thing. Within the team, we've set on round about five or six areas so far. The first section, the preamble, is setting up this definition of a law enforcement authority. The second section is looking at the minimum standards for requests to be accepted. Section 3 concerns the process for receipt by the privacy/proxy service provider. That includes a lot of things that we've just discussed in the previous session around abuse, point of contact details, and that sort of thing.

Then we have a section on prioritization; when you receive a request, how that's prioritized within the business based on the type of issue for which disclosure is being sought. Associated to that, there's a timeline for response and then a series of actions within that timeframe that need to take place.

We're also considering if there's any additional accountability requirements an escalation mechanism in cases of non-compliance, potentially as it were. But that's something we've still yet to look into.

We've held mailing list discussion and several conference calls, which have been really productive and helpful to me. We're collaborating at the moment on a document which we hope to get to you as soon as possible. I think the original timeline was that we would provide something to you prior to this meeting. We're not in that position, unfortunately, yet, but the discussion has proven to be really productive and really helpful on that.

We're going to be discussing this with the full Public Safety Working Group in our meeting later today to continue working on it, and we hope that we might be able to have something we can present to the full GAC on Tuesday. I don't know whether they'd be in a position to sign that off, but – I've mentioned this to Amy before – because this is all pertaining to GAC advice, obviously we need to make sure that the GAC is fully cited. They're largely happy with the way we're going before we then share it back.

So I hope you understand that the speed is maybe slightly slower than ideally everyone would like, but I hope that the outcome and what we do provide to you will be worth the wait as a result.

I'd say that's largely it. I don't want to go into a too much detail and too many specifics about some of the minutiae of the argument and the debates and discussions that we're having,

but hopefully you can see from that structure the areas we're looking to focus on and we think ought to be included.

What I think we all feel as a team would really help is if there's any feedback or observations from yourselves – thoughts you've had from your side – on what you think might make this document beneficial to yourselves as the business operators of these services when you receive requests from us.

So I really, really welcome your questions and your feedback and your thoughts. I think we can turn it over to whoever wants to have a go and take the mic.

THEO GEURTS: Thank you, Nick. That was a substantial update. I'm missing, actually, the sense of urgency in the work that you guys are doing. We have an extremely aggressive timeline. I hear a lot, but I don't hear a lot of action. Is it perhaps, even though you cannot have the GAC sign off on what you guys are working on, actually trying to make sure that we actually get the language at an earlier stage than when you guys want to disclose to us? I have the feeling that we might have some issues going through that language so we can actually identify chokeholds/barriers that will delay our work. Thanks.

NICK SHOREY: Thank you, Theo. I recognize your points. Ideally, we would hope that we would have been able to bring an actual document to the meeting, but we're not in that position and I'm not prepared to do that.

However, there is a sense of urgency. We've moved pretty quickly, I think, overall, and we're making good progress, for sure. We have a document that we're working on, and it has text and ideas in it. So I think we're making good progress.

We are two weeks behind on our deadline so far. I hope that we won't fall too much further behind after we get agreement through the PSWG and the GAC. So I think we're two weeks behind. I know we've got a very tight deadline and we've given ourselves a twelve-month timeline for this. I don't think it's too bad, given the challenges we're trying to reconcile. Amy and I have kept in regular contact, and I've kept her updated on the progress. So I would hope that, not too long after this meeting, we can get something over to yourselves, not least because I want to get this out the door as well. Thank you.

GRAEME BUNTON: Thanks, Nick. Great. First of all, only two weeks behind is a monumental ICANN victory, so congratulations.

I guess, as I think about this and maybe share this with you, in my head anyway, sharing earlier is probably better in getting feedback from the rest of the IRT as soon as possible because I think the frustration you might see, where you've got it done and it's then going to the Public Safety Working Group – it's not going to the GAC as a whole – and then it's being fed into the IRT and then you're having it torn apart and rejected – getting stuff at the last minute like that can be super-frustrating, and it's not a very pleasant place to be.

So I would suggest, if you can, share it earlier. I think we can we're probably mature enough to recognize that it is a work in progress. So I'd push for that approach, but I can understand why that might not also be possible. Thanks.

NICK SHOREY: Thank you, Graeme. I totally hear your point and understand that. What we're very conscious of – this is me with my GAC hat on now – is the engagement that the GAC and its working groups have with the rest of the community. We're aware of the level of scrutiny that comes to anything the GAC says and does, and rightly so. So because of that, it may not be, in the eyes of this group, the most pragmatic or dynamic process from that end to just say, "Okay, we've got something," chuck it over to you, and then you chuck it back and we have quite an iterative thing.

We've got this process to ensure that everyone is cited and everyone is content. On something particularly that pertains to GAC advice on quite a sensitive topic, in the whole of ICANN there are few topics more contentious often than law enforcement and privacy in the same sentence. So we just want to make sure that we've got that initial sign-off.

And, yeah, we might send it back to you guys and you guys tear it apart. I hope that doesn't happen, but if does, well, that's just the way it goes. Then we'll go back and work. That might mean then that this process takes longer, and if so, so be it. We've just got to try to get it right. So there's maybe seemingly a bit less flexibility there, but it's for the broader benefit. I think it's quite important, particularly on this.

GRAEME BUNTON: Thanks, Nick. I understand why you can't share earlier. As a point of humor, I think we would call that the inverse GACeging, where you would spend some considerable time on something and then lob it out to the community and then have some last-minute feedback.

AMY BIVINS: Do we have questions or comments from anyone in the room? Or in the chat, please? We have Nick here.

UNIDENTIED FEMALE: A comment from Steve Metalitz: "Earlier sharing is better, even on a provisional basis. Could it be shared as an individual contribution without PSWG or GAC? Just a suggestion for consideration."

NICK SHOREY: Thanks, Steve. We've got several members of the GAC on the IRT, so they're obviously welcome to share their contributions in their capacity as representatives of their governments and agencies within the group.

The task that was set before us here was to go away as the PSWG and come up with a document for you. As a subgroup of the GAC, we therefore need to ensure that we're doing that and conducting that in a way that is in keeping with the wishes of the GAC and the GAC leadership.

But I do recognize the benefits to the group of getting this over to you as early as possible. That's why we've been working really hard and having calls every week and discussions. [It's] working fairly dynamically for the GAC, if I may be so bold on this. But yeah, there's a limit to what I'm able to do; ultimately, it's the bottom line in terms of just chucking stuff out to you.

There was another point I think I was going to make, and I can't remember it. But hopefully that covers his question.

I mentioned that one of the elements we're looking at is developing a minimum standard, a minimum set of criteria, that any request to a privacy/proxy service provider must contain in order for it to be accepted. I noted – I think it was Greg – you were saying earlier on that you'd like, on the other stuff, some sort of discretion to set out the information that you would need to be able to action a request.

So I'd be interested to hear your thoughts. What is that? What do you need? If we're talking about verification of identity, for instance, that's often a topic of discussion in some of these things. What sort of information would you typically wish to see within a request? How would you like that formatted as well?

What's the most effective formatting mechanism of such requests that ideally you would like to see? We may not be able to go down to such detail in this document, but we would like to try to do is make sure that we get a base standard that works for you so that things can be then actioned and responded to as quickly as possible.

One of the key elements for us is the importance of time. When we seek disclosure, it may be for cybercrime investigation, but it

may be for a threat to life. So time is important, and getting the right information in as soon as possible in a clear format is helpful to you as businesses in being able to respond.

So I welcome your thoughts on what you would ideally want from such a request to include.

GREG DIBIASI: As a general proposition – obviously it's going to vary from different types of abuse – we need enough information to make it actionable; things like the URL, things like the specific type of abuse alleged, or information like source IP addresses. That's something the registrars have been working on, and maybe that's something we can follow up with with more information or feedback on general requirements.

But I don't know. Let me bring that to our group. Maybe we can give you something more specific. So as a general proposition, more information is better, and we're just trying to get enough so we can act when needed.

DARCY SOUTHWELL: I think the other thing I would recommend, in addition to that, is that we need to be able to look at what you're asking for and have enough information. But I actually think the illustrative

framework – I realize that what's in the final report is geared towards IP complaints, but it has a lot of detail that a privacy/proxy provider would need in order to be able to sufficiently look at the situation.

NICK SHOREY: Thanks, Darcy. Yeah, that's one thing that's been really, really helpful with that IP framework. We've been seeking to build on that as well. So we're looking at some clear criteria that would hopefully help us help yourselves and try to raise that base standard and enable requests to be actioned in a timely manner.

AMY BIVINS: Do we have questions or comments from anyone else? Oh, Steve Metalitz has his hand raised in the room.

STEVE METALITZ: Yes. Can you hear me?

AMY BIVINS: Yes, Steve. Thanks. Go ahead.

STEVE METALITZ: Thank you. I was interested in the last couple of comments. I know that this was the first topic that we talked about in this meeting: the mandatory minimum criteria for any abuse complaint. Obviously, that could be built upon for law enforcement, and it has already been built upon, in a sense, in the illustrative disclosure framework.

I wasn't clear – is there a group of registrars that are currently working on this? If so, when do they expect they might have some work product to bring forward to this group? Because we would certainly welcome that, and anything we can do to facilitate that, I think we would be glad to do. But I wasn't clear whether there is already a group of some registrars that is already working on this. Thank you.

GRAEME BUNTON: Hi, Steve. There is a group of registrars working on this. We've been working on it for a long time. A new draft was circulated to registrars a couple of weeks ago ahead of this meeting. We hope to talk about that here.

If I can get myself into the Adobe Connect room, I will share a list of things that we think is at least a starting place for conversation around the minimum requirements for abuse reporting because I don't think there's any secret there about

the things that at least make an abuse report actionable and easier to action. Thanks.

AMY BIVINS: Anybody else in the room? This is your chance to ask questions.

All right. No comments about the law enforcement framework or the working of the Public Safety Working Group? Questions about next steps?

Okay. All right. Thank you, Nick.

NICK SHOREY: Thank you.

AMY BIVINS: Do you have any more comments?

NICK SHOREY: No.

AMY BIVINS: Okay. All right. So we can shift back a few slides, and we'll go back to finish up our discussion on third-party requests – slide 22.

Okay. We're going to move on. We finished for now talking about abuse reporting criteria. We're going to move onto the topic of relay requests.

Following the same general format of questions we're asking about requests, we're just going to follow the same format here. For who can request relay, there was no restrictions in the final report, so we're not planning to incorporate any restrictions into the requirements.

For how to request relay, the final report referenced relay request received electronically, including through e-mail and web forms. Does anyone see any issues with either of these points? Or do you have questions or comments?

Okay. Moving on to required provider actions in response to relay requests, the final report said that providers must relay all communications required by the RAA and ICANN consensus policies. Second, providers can choose between two options. They can either relay all electronic requests received but may implement safeguards to filter spam and abusive communications. Or providers can relay all electronic requests received from LEA and third parties containing allegations of domain name abuse. So those requirements will be part of the program requirements.

On relay, a first question that we have for you is: for this option two, where, if a provider chooses to relay communications from law enforcement and third parties that contain allegations of abuse, should be abuse be defined consistently with the way that abuse reporting criteria defines abuse? We would probably support that for clarity and consistency and lack of confusion, but we want to hear from you if anyone agrees or disagrees.

Darcy?

DARCY SOUTHWELL: Thanks, Amy. I don't think I understand your question. And I'm reading your question up there. I'm not sure what you're asking.

AMY BIVINS: Thank you. To clarify the question, there is a requirement for relay where a provider can choose the option of either relaying all electronic communications or relaying all electronic communications from law enforcement and third parties that contain allegations of abuse. So our question is: should abuse here for the relay requirement mean the same thing as abuse means for the abuse-reporting criteria. So there would have to be a requirement that the list of abusive activity that we adopt for a relay request would have to contain allegations that would be covered by the abuse definition. Or, as an alternative,

whether any sort of abuse could be adequate for this relay requirement.

DARCY SOUTHWELL: Thanks, Amy. The final report actually specifies illegal activity. I think that's addressed in the RAA, if I'm not mistaken. So I think that's the answer there.

AMY BIVINS: Thank you. I know the reference that you're talking about. We had an IRT call, and – I'm not sure which one it was, but I can find out – we asked whether abuse – and then it had in parentheses "illegal activity" was intended as an example of abuse or as the only type of abuse. The IRT seemed to indicate that that was an example and that abuse wasn't limited to illegal activity. So that's why we're asking, because we didn't think that it was supposed to be limited to illegal activity, based on the discussion that we had.

DARCY SOUTHWELL: Thanks, Amy. I don't recall that, but it says IE (illegal activity), which usually means specifically illegal activity. Maybe that was my assumption from the final report.

AMY BIVINS: Thank you. And that's the exact question that we asked: whether it was intended for it to be IE or EG. The sense in the room seemed to be that it was an example and not exclusive, but we can go back and see.

If anyone else in the room would like to comment on this, if you believe that this should be limited to illegal activity, please speak up. We're just trying to be sure that we're clear on what the intent was.

Steve Metalitz on the phone?

STEVE METALITZ: Thank you. I do recall that discussion. I think we, on the working group, had a little problem with our Latin abbreviations. It was more like EG than IE.

But let me put this context. We provided two ways that provocateurs could handle these relay requests. The first way is automated. Basically, anything that comes in through the relay portal and that passed through a captcha or something like that to screen out abuse would be relayed. The other option requires the provider to look at all of these relay requests and say, "Oh, is this coming from law enforcement, or is this alleging some type of abuse?"

I don't think that many of the providers sitting around the table today would be likely to adopt that option because, again, it requires looking at every single request for a relay. But if they do, I think the easiest way for them to apply it is to use the same abuse definition that we've already talked about for abuse reporting. They'll be applying it in the context of an abuse report. I'm not sure why it would be difficult to apply it in the context of a relay request that's labeled as such. Thank you.

AMY BIVINS: Thank you, Steve. Does anyone else in the room have comments on this? Darcy, would you want to respond? Or anyone else?

DARCY SOUTHWELL: Thanks, Amy. I guess IE or EG – I think that illegal activity is something that's defined in the RAA. My recollection was that that was one of the reasons we used that: it's already a defined term.

But Steve is also right: you're talking about two different processes and it's a manual process for Option 2. But when we have a defined term that we're talking about, it seems like we should stick with that.

AMY BIVINS: Thank you, Darcy. The challenge here is that we seem to be getting inconsistent feedback. Steve, correct me if I'm wrong but it seems as though you were treating the illegal activity as an example rather than an IE Not to get into the minutia of the minutia of discussions of IE versus EG but it's important to get it right whether we're talking about just illegal activity or broader abuse.

The sense that we got on the call where we discussed this with the IRT was that we were talking about something broader, and we're not necessarily hearing the same answer now from everyone. And so if anyone else in the room would like to comment on that, that would be helpful just so that we can make sure that we get it right because we've heard answers both ways.

JENNIFER GORE: We're under the impression that if we cannot reach a consensus on this, we will take it to a poll to make sure we get clarification. So if anyone would like to speak up on it now, that would be helpful. If not, we will consider it an open item and therefore we will have to perform the Doodle poll to make sure we reach a consensus on this.

AMY BIVINS: Roger, your hand is raised.

ROGER CARNEY: I don't know what the intent was because I wasn't part of that PDP, but if we're going to use the term "abuse" then we should be consistent about it. If we're going to define it, then it means the same thing throughout the whole document.

AMY BIVINS: Okay. Does anyone else have comments on this now? Obviously, given the limited number of IRT members that are here we'll be following up with the full IRT on this on the list, too, so this isn't your last opportunity. But for anyone who's here that would like to add additional input on this, please speak up, or anyone in the Adobe room as well.

Okay. Steve, I'll defer to you.

STEVE METALITZ: Yeah, I raised this in the chat. I'm not clear what the difference is between illegal activity and the abuse definition. I guess there probably are some type of malware activities. Malware is not illegal in many, many, countries so it is perhaps a more restrictive definition, but I guess it would be helpful to have an example.

Okay, and Darcy's put in the chat the RAA definition. Okay.

Is Darcy saying that they would not consider malware exploit as abuse because it's not illegal in some countries?

DARCY SOUTHWELL: If my memory is correct, what we talked about in the PDP was this is a privacy/proxy service and so we're talking about abuse of a privacy/proxy service provider's services and so it's not literally every single abuse activity related to a domain name or even a hosting issue. It's abuse of a privacy/proxy provider's services.

STEVE METALITZ: Could I respond?

AMY BIVINS: Absolutely.

STEVE METALITZ: I think we had this discussion, too, Darcy in a previous call that there can be all kinds of abuse that are being carried out by someone who has registered a domain name using a privacy/proxy service. Now that's probably going to be in violation of the terms of service of that provider, so I guess that

in that sense it's an abuse of the service, but I thought we were talking about something broader here.

AMY BIVINS: Thank you. Does anyone else have comments, questions, on this?

Okay. So we'll take this one to the list for sure.

A second question on relay requests. Do you see any gaps in require provider actions on relay where additional criteria may be needed? We want to ask you first and then we have a couple of topics we want to talk about that we see as possible gaps but we want to ask you guys first if you see any gaps.

Okay. Anybody in the room? If you see no gaps, that's fine, too. But you can tell us that, too, if it's helpful.

Okay. I'm not seeing anyone in the room raising their hands to speak so I want to go through a couple of potential gaps that we saw and talk through them. The first potential gap is ensuring that relay communications reach customers or ensuring that at least there's a check that the system is working properly. And Jen Gore I think wanted to talk a little bit about this.

JENNIFER GORE: Thinking about the way communications are transmitted from privacy/proxy customers, at times registrars will rotate out e-mail addresses to limit spam perhaps. The question is related to should providers be required to test e-mail forwarding to customers to ensure rotation or the forwarding activities are working properly?

AMY BIVINS: Theo, your hand's up.

THEO GEURTS: As Jennifer already mentioned, there are a lot of privacy profiles who change the e-mail addresses on a frequent basis to prevent spam. So if you are going to test the forwarding, that's going to be quite an interesting puzzle there if the e-mail address is being changed each week. I don't think that our customers would be favorable if we are starting to send them e-mails each week to test if it's still working. That's quite interesting what's being said there.

I'm not sure if we should do it, but my sense is we're going to create a whole lot of problems there. Thanks.

JENNIFER GORE: Thanks, Theo. I think there's multiple mechanisms for testing that might not include sending an e-mail to every privacy/proxy customer. However, I think that there is a gap around ensuring that communications are relayed to the registrants associated with privacy/proxy services.

The question is, does the IRT believe that there is a gap regarding [ensurance] that communications are received by the registrants? And if so, what is the proposed mechanism for ensuring that communications are relayed in a manner that's commercially reasonable for instance?

THEO GEURTS: I don't think there is a gap. Second, I think one of the lessons we could learn from the WHOIS/ARS project that is going on – it was my understanding but I could be wrong here – that the only way the ICANN could really test the e-mail addresses was to send an actual e-mail to the registrants. So if that group is already struggling with how to test an e-mail address, now I don't see how we can come up with another method to test it. I would love to hear it, by the way. That could help maybe deal with the ARS project out a little bit. Thanks.

JENNIFER GORE: Obviously this is the point of this discussion now and like to understand your perspective on this and the importance of ensuring the communications are received by the registrant.

AMY BIVINS: Roger?

ROGER CARNEY: I don't think there's a gap here. I think that even if you read the first part of that, it may not even be by e-mail. So you're going to verify the e-mail even though the preferred communication is by phone or by postal or whatever. So I don't think that's a gap that we need to address.

JENNIFER GORE: Any other IRT members want to comment on this item? If not, we'll move forward.

AMY BIVINS: Okay. We don't have any in the chat, do we?

Okay. So another question that we have for you on this – and we've raised this before – is whether there should be a required time frame for the mandatory relay of communications. The final report says that, "Communications alleging abuse should

be promptly relayed," and that, "Requestors will be promptly notified of a persistent delivery failure." But what about other communications?

For example – and the reason why we see this as a potential gap is – for example, a notice to a customer that a registration is expiring soon wouldn't be very helpful if the customer didn't receive it in time to be able to respond to it and take action. And so this is why we want to hear from you about imposing potential timeframe requirements for relay here. It doesn't necessarily have to be as specific as number of days, it could be a reasonableness standard or something. But we just want to hear from you on what you think as far as what the working group intended here in terms of the timeframe for the required relay.

So for IRT members in the room or anyone, do you see a need to go beyond the relay requirements that are explicitly written in the final report to include any sort of timeframe requirement for the relay? And as importantly, if you think there shouldn't be any sort of timing requirement, please let us know that as well.

Steve Metalitz's hand is raised, and then Theo.

STEVE METALITZ: Yes, thank you. This was discussed at length within the PDP Working Group and we ended up with a bullet under Recommendation #17 that, "All third party electronic requests alleging abuse by a PP service customer will be promptly relayed to the customer." That was as specific as we were able to get. And you're right. It's only about abuse. This why it comes back to Darcy's suggestion that we reopen the definition of "abuse" here and look at it differently, we were kind of relying on this that, for example, if intellectual property violations were involved, that that would be promptly relayed. Now if that's not going to be considered abuse, then your question becomes relevant. But if that is considered abuse, I think it's covered by "promptly" and I'm not sure we can get more specific than that unless the providers are willing to agree to a 24-hour or 12-hour time limit, which I think will often be the case in the option one world where they're not doing individual review of each relay request. Thank you.

AMY BIVINS: Thank you, Steve. Theo.

THEO GEURTS: I agree with Steve here. We need some flexibility here, so the term "promptly" will just work just fine here. Thanks.

AMY BIVINS: Thank you. Would anyone else like to comment on this?

Alright. In that case we can move on to reveal.

So there were very few requirements related to reveal in the final report outside of the IP framework. All of the requirements focus on terms of service and ensuring that a provider's practices are adequately explained and disclosed. There are no restrictions on who can request reveal or on how to request reveal. The final report seemed to indicate that a form-based option could be used for reveal requests, too.

So a question for you is: do you see any gaps on reveal where we may need minimum criteria?

All IRT members? Anybody in the chat?

Okay. So a potential gap that we saw here that we wanted to discuss with you is similar to relay regarding the timing of responding to reveal requests, and we wanted to talk to you about when a provider receives a reveal request should there be a target service level commitment for a response? Do you think that that's a gap that we need to work on here?

Theo, your hand is raised.

THEO GEURTS: I haven't been present with all the discussions and deliberations of the working group, but my impression was here that we have very few requirements for revealing because it's a rather complex matter and it also depends on the circumstances when there is a chance of reveal of the registrant. So I don't think there's an actual gap here. I think this was intended by the working group, but I stand corrected. Thanks.

AMY BIVINS: Thank you, Theo. Darcy, your hand is up.

DARCY SOUTHWELL: Thanks. I agree with Theo. Obviously none of us attended every single meeting, but we have to have flexibility from an operational perspective for privacy/proxy providers to do their job, and sometimes that's going to include investigation before either a publication in the WHOIS or a disclosure is made. And so I don't think you can just pick a number of days that would work in every situation. There has to be flexibility there.

AMY BIVINS: Thank you. Does anyone have a response or comment on this in the room or in the chat?

Okay. So these are the terms of service requirements from the final report related to reveal and I read them to you earlier so I won't do it again, but these will be included in the requirements.

That's the end of our substantive questions on third party requests for now, but there was a suggestion on the list that I want to talk about briefly yesterday for how to handle coming up with and developing minimum mandatory criteria for third party requests. It was suggested on the list that we could form a subteam to work on this, and we're open as staff to doing that if you guys would like to form a subteam on this topic rather than working on it in the full IRT. Does anyone have a preference on the process we use for developing the minimum criteria here?

Based on our discussion today, it doesn't seem like there's going to be a lot of work on this but there will be some, so there may be benefits to using a subteam but we want to hear from you.

DARCY SOUTHWELL: Do you have, beyond what's in the final report, do you have suggested language already?

AMY BIVINS: For minimum criteria?

DARCY SOUTHWELL: Yeah.

AMY BIVINS: The only suggested language that we had was posted on the screen with respect to abuse reports. And that was just taken from the RAA requirements. But beyond that we don't have suggested language. If you want us to, we can draft suggested language.

DARCY SOUTHWELL: That's not what I'm suggesting. Because I know the terms of service requirements are up there so I wasn't sure what else would be drafted that would warrant a subteam, but I see Steve's in the queue. He may have additional ideas there.

AMY BIVINS: Steve.

STEVE METALITZ: Yes, thank you. I'm a little confused. Are you asking about the mandatory minimum criteria that we were talking about earlier today and coming up with those, or are you talking about mandatory minimum criteria for disclosure requests?

AMY BIVINS: Thank you, Steve. I was asking with regards to all types of requests, since we were directed to create minimum mandatory criteria for third party requests and abuse reports we're really viewing this as a package – so all of them. If the IRT feels that we don't need additional criteria on some types of requests, then we won't be creating those. But the subteam work I think would be focused on all types of requests that need minimum mandatory criteria.

STEVE METALITZ: Okay. This was my suggestion to form a subgroup because I suspect that the registrars are pretty advanced on this and Graeme's intervention kind of confirms that. Now that's for abuse reports generally, not necessarily in the privacy/proxy context. But that probably provides a good starting point.

I think the registrars who are also providers are in a good position to take the lead on this and if there's anything we who are not registrars can do to facilitate it or to react to a draft, we would be happy to do that. So I don't know whether a formal subgroup is needed. I haven't looked at what Graeme just posted, and maybe that's a good starting point. But I agree with you. This shouldn't be a big task but it would be good to have a draft out there that everybody could look at.

And again, I think we have it in the illustrative disclosure framework, but that's only a small subset of this universe. Thank you.

AMY BIVINS: Thank you, Steve. Does anyone else have comments on this?

Just a comment generally about the work that the registrars have been working on with respect to criteria generally. There's a timing concern, too, with respect to the progression of the IRT versus the work of that group, and so as we're trying to move along this IRT the question becomes, are we waiting for the registrars to finish their work before we start drafting minimum criteria or what the process is? But we can follow up with the registrars on that.

I don't know if anyone in the room has comments. Graeme?

GRAEME BUNTON: I posted a link to a screen shot of the abuse reporting requirements that we've been working on – and this is not formal or official in any way yet – but I agree it's probably a reasonable place to start discussion. I think for us, the requirements for a report are not controversial. I think that in general they're quite logical. The bit that is taking us a

considerable amount of time to figure out and work through is response. But if we're just tackling that first piece I think we should be able to move relatively quickly. Thanks.

AMY BIVINS: Thank you. And we'll follow up with you on that. Does anyone else have comments, questions?

Okay. So we've reached the end of our questions for third party requests for now and we're a little ahead of schedule, but that's okay. So we'll go ahead and take a break before we start our final section of discussion. If you guys could come back in about 10 minutes, around 4:45, we can go ahead and start our last section of this early.

And as a reminder on the last section we're going to be talking about a couple of registrar focused questions, so it should be an interesting discussion.

Okay, everybody. We'll get started back in just a couple of minutes.

Alright, everybody. One minute warning and then we'll go ahead and get started.

Okay, everyone. For our last piece of this meeting we want to take a step back and talk about a couple of registrar-related questions.

The first issue we want to talk about is the issue of providers that are not affiliated with the registrar. We know that most providers are likely to be affiliated with registrars – at least that's what we expect – but the working group made clear that the possibility of unaffiliated providers should be left open, and the issue of unaffiliated providers has come up from time to time already in the IRT in discussions about how data escrow and WHOIS labeling is going to work. And the discussion has been largely limited to the idea that there could be challenges related to unaffiliated providers, especially related to labeling and de-accreditation.

So we want to talk to you now, given that the working group clearly intended for unaffiliated providers to be part of this ecosystem. We want to talk to you about the working group's expectations for how you see unaffiliated providers operating in the marketplace to assure that we are drafting requirements that will work for that expectation.

And so I want to open it up to you, especially the registrars, who work with privacy/proxy providers now. Can you talk a little bit about what the expectations were for unaffiliated providers in

this overall ecosystem and how you saw this process of having unaffiliated providers working, especially related to things like the registration process and who's going to be putting in the information and we have to deal with WHOIS labeling requirements and how would a label get into the WHOIS record if the provider is not affiliated with the registrar. So we want to hear from you now on that.

Theo?

THEO GUERTS: I don't see the issue here. This language is already in the RAA 2013. We now and then encounter these privacy/proxy providers who are not doing it correctly. We could make sure that it is corrected. We engage with them and any issues that are just being taken care of. We've been doing this for many, many, years so there is, in my opinion, not really an issue here.

I think we will continue to do that work when we have accredited privacy/proxy providers. We will use the same mechanisms to engage with them and make sure that everything goes accordingly to the accredited requirements. Thanks.

JENNIFER GORE: Thanks, Theo. You referenced the 2013 RAA but the unaccredited service providers may not be registrars, therefore they are not subject to the 2013 RAA.

THEO GEURTS: I'm not sure of the specific language, but it talks from my recollection about resellers who deploy privacy services. I don't have the language in front of me, but the bottom line is here there isn't really a problem here. Thanks.

DARCY SOUTHWELL: Regarding your specific question about the registration life cycle and impacting labeling and other requirements, at the end of the day the registrar for a domain name controls those things. So I'm not sure I understand your question about whether a privacy/proxy provider is affiliated or not. The registrar controls those items. So is there something more specific you're looking for, because in that case I totally agree with Theo. There's no issue here.

AMY BIVINS: Thank you, Darcy. We are thinking about, for example, we were talking about labeling requirements. The discussion came up that there would be challenges imposing labeling requirements

where a provider is not affiliated with the registrar because the registrar controls the information that's in the WHOIS record. And so because it was clear that we're supposed to leave the option open for there to be unaffiliated providers in this ecosystem and because we know there are going to be challenges with unaffiliated providers with respect to things like labeling, we want to hear from you how when you were thinking about drafting these policy recommendations how you saw it working – the process for unaffiliated providers.

GREGORY DIBIASE: I guess I'm confused, too. Is this related to, at one point we discussed that if we found out a privacy/proxy provider was not accredited we would just treat it as inaccurate WHOIS and use the procedures that we already have in place. Is that what we're referencing?

AMY BIVINS: No, sorry. To make this more clear we actually are talking about that question next. But this question is, where there's a privacy/proxy service provider that's accredited by ICANN – they follow the process – but they're not affiliated with the registrar but they're going to serve customers that may be working with the registrar that the provider isn't affiliated with. And so the

challenge becomes during the registration process, how did you see the process working for the provider's information to be taken from the provider and put into the WHOIS record, for example, when they're not connected to the registrar?

GREGORY DIBIASE: I guess that would be between the provider and the registrant contracting with the nonaffiliated provider. Some web hosting companies for example put their information – that's the assumption I was operating on but I'm not sure.

DARCY SOUTHWELL: I think the other challenge we had in the working group is the fact that we have not yet found unaffiliated providers that truly exist and so it's difficult in the working group to imagine – those of us that have a registrar and a privacy provider – we know how it operates for us. We don't know how it would operate with a third party we can't talk to yet. Not to say that they're not out there. We just can't find them.

So I don't know that we have a true problem that we need to fix at this time.

AMY BIVINS: Thank you. And that is the challenge that we're facing as well. But at the same time we're charged with drafting requirements and creating requirements that will work for them, and so to the extent that we can, we just want to encourage dialog with you guys and with IRT members who have experience working with privacy/proxy providers to ensure that to the extent we can that the requirements work because we were directed, or the final recommendations indicated, this should be an option. So we don't want to draft requirements that aren't going to work for that option.

Theo, your hand is raised?

THEO GEURTS: Thanks. Regardless of the old situation or a new situation, we already are facing the facts that there are nonaffiliated privacy providers. That's a given. It is also a given that regardless of their status, they always have to go through a registrar to make these registrations or to publish the WHOIS data. So if you're talking about the impact of the labeling and the other requirements, there is no difference in the current situation or in the proposed new situation. There is no change. It is always up to the registrar to make sure that the WHOIS format and labeling is correct. We registrars will take care of it. We'll just get the info from the nonaffiliated providers and we'll make sure that when it comes

to terms of labeling it will be correct. If it isn't correct, registrars will be noncompliant and we go through a compliance process. Thanks.

JENNIFER GORE: Thanks, Theo. So you reference correct versus non-correct, and I pose the question back to you. How will ICANN enforce compliance if we're not clear on what's correct versus not correct? It sounds to me that there should be some processes identified by the IRT for affiliated versus unaffiliated.

THEO GEURTS: I think the question – and we circle back to this – the ones who are operating the WHOIS is the registrar, and if that is a registrant giving us information or a unaffiliated privacy provider or an affiliated privacy provider, it is always up to the registrar to make sure that in terms of labeling, the output is correct. That is the requirement of the registrar. That is the contractual obligations of the registrar. Who is bringing us the information is in my opinion not so relevant. So that's why I'm bringing this up. There is no difference between now and the future because we will still be dealing with the labeling requirements for our WHOIS servers and it is regardless who is bringing us the information. Thanks.

JENNIFER GORE: Thanks, Theo. In response to that, do you conclude that there's not a verification process as far as who submits the change on behalf of the registrant?

THEO GEURTS: There is always a sort of procedure in place but if you talk about labeling and those sort of requirements, those are just WHOIS specifications – or I'm missing the question here – but regardless of how the information is being supplied it goes through the process that we already know and so I don't see a change in the future coming because we still go through the existing processes already laid out in the RAA 2013 when it comes to the WHOIS and its output. Thanks.

JENNIFER GORE: I just want to note that Amy put it in here that it could be example of the labeling but I think there's some further clarification needed regarding the process of registrars or privacy/proxy service providers ensuring that the request change the WHOIS out part on behalf of the registrant is valid.

FRANCISCO ARIAS: I guess my reference would be in what is the next question there, should there be authentification for unaffiliated providers? Imagine the scenario, Theo, where the unaffiliated provider is telling you the registrar that this registration they are making has a privacy or proxy service and that is something that will eventually be identified in WHOIS in whatever way, it doesn't matter. The point is, they are telling you this is a registration that has a privacy/proxy service, the question here is should you as a registrar have to verify that that's indeed the case and what's the identity of this unaffiliated provider to which you probably don't have any relation? Does that make sense?

THEO GEURTS: Thanks. I'm not actually sure. I don't think there is an issue there because these are going through all automated systems and basically we get information all the time from various parties and it's all being done automatic and it's all being done within the references that we are required to process it and that is not going to change, and how we're going to deal with non-accredited privacy providers I think that's a different question there. But if we talk about the impact of labeling and other requirements, assuming that they are tied to labeling, I don't see an issue there. Thanks.

FRANCISCO ARIAS: I just wanted to clarify – this is not about unaccredited providers. I'm talking about providers that are accredited but they are not affiliated in any way with the sponsoring registrar of the registration. So how do they tell you that this is a privacy or proxy registration and whether you have to verify that they are an accredited provider or not? That's the question.

THEO GEURTS: Okay, so if they are a non-accredited privacy provider and they are using a registrar to register domain names, we don't know.

FRANCISCO ARIAS: No, this is an accredited provider.

THEO GEURTS: Again, the answer is the same – we don't know. We cannot know if a privacy provider is accredited or non-accredited. There is no tag within the EPP or something that such a provider could provide us. So the answer is, we simply do not know. But the same applies already in the given current situation. We don't know, and in the future we still won't know, if it is a privacy provider who's accredited or not. It doesn't change.

FRANCISCO ARIAS: Sorry to insist there, but if there is a way – whatever the way is define – for example, in which suppose there is through a prefix in the name of the contact or there has to be a way for the indication that a certain registration has a privacy or proxy service that has been inserted by whoever is making the registration with you which is not through EPP but through a web page probably and they are saying this is a registration that has a privacy/proxy service, the question there is if you have to do something about it or not.

I take it from your answer that you think the registrar doesn't have to authenticate that information and just leave it as it is, unless I am misunderstanding what you are saying.

THEO GEURTS: I'm still wondering or struggling with the fact how we actually would know if we are dealing with a accredited privacy provider. I think that circles back to the question if there is a problem with unaccredited service providers and how registrars should be dealing with them. That isn't exactly the question that is being phrased here, but it could be a question in terms of should we do something about it. Thank you.

GREGORY DIBIASE: So it sounds like you're asking, are registrars required to authenticate a nonaffiliated yet accredited privacy/proxy provider? And my response would be, if it's not in the recommendation, if it's not a recommendation in the final report, then no.

JENNIFER GORE: Thanks, Greg. I don't necessarily believe that we were asking the question if it should be required, given the fact it could be or could not be in the final report I don't have that section right in front of me. It was more or less the question around this is an unknown entity that exists today – unaccredited privacy/proxy service providers. At some point in time we have to account for the fact that this entity might exist. So we're posing the question to the IRT, which include registrars, to answer it simply is how do you envision treating an authenticated versus unauthenticated provider? Do you treat them equally? Do you need an identifier like an IANA number in order to know if they're accredited versus non-accredited? Will you use that as a mechanism to validate whether they're accredited or not? Do you not want to use that as a mechanism?

DARCY SOUTHWELL: Sorry, I jumped too soon but I think that I'm not sure there's one answer for every registrar on that issue, to be honest. Different registrars operate differently in how they collect information from their registrants, including through resellers, including web-based, including API – and I am not a technical person so there's probably other options. So I think you're asking a question that we collectively as a registrar group can't answer for you. There's no mechanism today to – what everything Theo already said, so I'm not sure we have an answer, nor will we, for this purpose.

AMY BIVINS: Roger, your hand's been up for a while.

ROGER CARNEY: I was just going to follow up. I think this started with Amy and Greg talking about how is the data going to get there, and as for a registrar I don't think that we really care. The registrant comes to us and puts in the data, and what data they put in is what they put in. So if they're providing accredited information from their privacy provider it is such and it's going to go in. Our obligation is to validate the e-mails works. So as long as that works, we don't care and it's going to go in and, as Theo was saying, we already have processes. If someone's going to

complain about it, we'll treat it as invalid WHOIS at that point and it'll work.

Sitting here, I can't think of a reason why we would need to know if they're accredited or not because, as Theo was mentioning, all the mechanisms still work today as they would work tomorrow if it was accredited or not accredited.

AMY BIVINS: Thank you. And Theo, your hand is raised?

THEO GEURTS: Just to circle back to what Darcy was saying. I think most of us when we get abuse reports and we're looking at WHOIS data and we're seeing – I sometimes see those what I call "fantasy privacy providers." They are made up on the spot by the registrant. It's completely bogus information. We already got existing processes to deal with that and I think most of us are dealing with it because it's going to result in WHOIS complaints anyways. So I think most of us are proactive there, but there is no set procedure for every registrar there. Thanks.

AMY BIVINS: Thank you. Does anyone else in the room have comments on this or questions? Anyone in the chat?

Okay. In that case, we can move on to our final question of the day which is – we started discussing this question a couple of months ago and it was suggested that we could talk about it here, so now we will.

There's a recommendation in the final report that says that, "Registrars are not to knowingly accept registrations from privacy or proxy service providers who are not accredited through the process developed by ICANN." So the question that we initially raised in January was, what should a registrar be required to do when it becomes aware of a registration that involves an unaccredited provider?

There were a couple of different possibilities that were suggested. The first was that this could be treated as a WHOIS accuracy issue and trigger a requirement to verify or reverify the contact information, but this may not solve the underlying problem because the WHOIS information could be accurate- even if it's not an accredited provider the e-mail address could be working.

Another possibility might be that the registrar could be required to notify the unaccredited provider of the requirement to be accredited and to give the provider and the customer some period of time to remedy the situation before suspending the registration.

We know that in all cases there will need to be a significant onboarding period at the beginning of this program. This isn't intended to take a bunch of providers offline that are applying for accreditation just because they don't have it yet at the beginning and there'll be an onboarding process. And this is separate. This is after the program is up and running, what should a registrar be required to do?

So we want to open this up for discussion again here, and we hope that you guys have some suggestions for what you think the steps a registrar should take in this situation.

GREGORY DIBIASE: I think the WHOIS accuracy way does work because our obligation is to investigate and take steps to make sure it's accurate. It's not just verifying an e-mail. So if the registrant name is an unaccredited provider, then that's wrong information that we need to take steps to correct. We don't just verify the e-mail. That's not the whole process. So I don't think there's a gap. I think that procedure can work to remedy that situation.

DARCY SOUTHWELL: Similar to what Greg is saying, that's one piece of it and then I think the other piece – and there's a footnote in the final report

about this – that when a registrar is notified of a problem – now it knows – and that it should treat it like an abuse report. And similar to other parts of the PDP, there are already requirements that privacy/proxy providers have in terms of service, identifying what is abuse, what actions are going to be taken. And so between the WHOIS requirements and those abuse situations in the terms of service, I personally feel like this is covered.

AMY BIVINS: Okay. Thank you, Darcy. Theo, your hand is raised.

THEO GEURTS: Yes. I'm just going to pile up on what Darcy and Greg just said, and I think we have discussed this on the list also and from most of the registrars from what I've read on the list, we don't see an issue here and we got already existent procedures to deal with it if required. Thanks.

AMY BIVINS: Thank you. Does anyone else have comments on this, questions? Anyone in the chat, on the phone?

JOTHAN FRAKES: I don't have an issue where this would cause a problem, but the one thing that I notice that is a big cost structure for registrar with very small margins – and I don't think anybody's going to have sympathy for registrar margins – however, it's very expensive to have proactive action ongoing with dealing with abuse and reports, and it's really the substance of why I am commenting.

In this case, could it not be the case – I notice that it's mentioned that registered name holders have obligations – could this not simply be pushed to the registrant to identify whether or not a proxy or privacy provider is accredited or not so that that burden isn't pushed to the registrar to address? It seems like it could, as a suggestion, be a way to put this burden onto the registrant and not have the registrar having to deal with this.

AMY BIVINS: Thank you. And that's a possibility that we could discuss and I'd be interested to hear others' thoughts. I think the one challenge with that is when you refer to the registrant, whether you're referring to the unaccredited provider or the customer because if you're referring to the customer there may not be a way to contact them if there's an unaccredited provider because there may not be access to the information directly.

JOTHAN FRAKES: Thank you. I guess if we point to the same conditions that exist in the Terms and Conditions of Registration as a registrar, perhaps it goes into the T&Cs of a registrar to simply state it's the responsibility that the registration could be in jeopardy if it's not identified or if there is a provider that's not accredited. Perhaps that could be a way to bridge that.

AMY BIVINS: Thank you. What do others in the room think about this?

[HOWARD]: I think just from hearing what everyone's said, especially Jothan Frakes just said, I think the registrars tend to use the 3.7.7.5 or something of the RAA 2013 that identifies that if the registrant licensing the domain name to someone else it's still be the ultimate holder. So basically if as a registrar, getting a registration from an unaccredited or an unaffiliated provider submitting their contact information, they're ultimately being the registrant but under the situation they will need to review under – [allow] seven days of a request they need to review the true user of that domain name, the true identity of the person who actually using the domain name, and then if they don't respond, the registrar will follow the 3.7.7 procedure like either

suspend or terminate the registration. That's my understanding. Did I get it right, Theo and –

THEO GEURTS: You caught me off guard. Sorry about that.

[HOWARD]: [Inaudible] I get what you guys saying. My understanding is that we don't want to get extra authentication to those provider not accredited or unaffiliated with the registrar itself because in that case is more like a proxy service instead of a privacy service in those case because they're actually using that provider's information to being their own registration information to register the domain name with another registrar. Is it too complicated?

JONATHAN FRAKES: I can think of a simple case where an Intellectual Property firm submits a domain name and they're essentially providing themselves as the proxy for that client but they may also register names in their own name for their firm. We won't know the difference as a registrar. And I think that the consequences of loss of domain and pushing that accountability to the registrant ultimately for potential loss or jeopardy of the name, that that

should be substantial and we shouldn't be having to contact law firms to see, "Is this yours or is this your client's?" That's just a burden that may not be reasonable here. And there's so many law firms that do such activity, they may or may not be accredited. It's hard for me to determine that. And it puts a lot of burden on a registrar business to take and do that.

Not suggesting any of those would be bad actors. I'm just suggesting that there's a situation, a perfectly normal, reasonable, situation, where that might put a burden on a registrar depending on how this is worded where we could push that accountability out to the registrant and the jeopardy of loss of name rather than have a consequence to a registrar that may not really solve a problem here. Thank you.

AMY BIVINS: Thank you. Roger's hand was raised then we can go to Francisco.

ROGER CARNEY: I think that what you mention is good but I think it's already there. The Registrant's Agreement already detailed those things that if they're not kept accurate and everything like that, they can lose their domain. So I think that it's already handled there and I think you're right. It is their responsibility.

And then something Howard brought up that Steve just mentioned is privacy and proxies are supposed to be treated the same under this agreement except for the fact that there's a definition difference and the proxy provider is responsible, they are the registrant, whereas the privacy provider is not the registrant. So there is a slight difference.

FRANCISCO ARIAS: Jonathan, please correct me if I'm saying something wrong here, but if I understanding correctly what you are saying, that seems to imply that there is in practical terms there is no way to have unaffiliated providers because there is no way to differentiate between unaffiliated providers and unaccredited providers that are not supposed to happen. Unless I'm missing something it would seem like there is no practical way to have these third parties that are not related to the registrar.

AMY BIVINS: Theo, your hand is raised.

THEO GEURTS: Francisco, I think you're actually right there. At the current moment that is not possible, and I'm not sure if we should actually put any time and effort into this IRT to explore it. But I

do think – and maybe this IRT should give a heads up to the RDS Group – that we encountered this problem or I'm not sure, I don't really think it is a problem but that this scenario could play itself out and we maybe should address this within the RDS. So maybe that is the right venue there to address it. Thanks.

AMY BIVINS: Thank you. Does anyone else have a comment on this topic, or anyone in the chat or on the phone?

UNIDENTIFIED FEMALE: This is a comment from Steve Metalitz to Francisco: "Unaffiliated providers are to be publicly listed if they are accredited."

FRANCISCO ARIAS: The issue I'm hearing from Jonathan and Theo and others is that the difficulty on authenticating those providers which in my mind renders the differentiation between unaccredited and unaffiliated but accredited providers impossible to discern.

UNIDENTIFIED FEMALE: Steve, I'm not sure you heard that, but I think Francisco is referring to unaccredited providers not unaffiliated providers and how registrars are supposed to know if the provider is not

accredited based on some of the comments we've heard from the room.

FRANCISCO ARIAS: Just to clarify, what I'm trying to say is that I'm understanding that what is being said is that there is no way to differentiate between the two – between unaccredited or unaffiliated but accredited providers. So in practice you will seem like you could not have privacy/proxy providers that are not affiliated with the sponsoring registrar if I am understanding correctly what is being said.

UNIDENTIFIED FEMALE: Steve says, "This has been a recurring issue. Maybe best to wait until an unaffiliated provider seeking accreditation steps forward and encounters those problems."

And then Steve raised his hand. I guess he wants to –

AMY BIVINS: Steve, your hand is raised. Did you want to speak or did your comments cover that?

Steve, if you're talking we can't hear you. He's typing, okay. We'll [give this to you] in just a second.

Alright. It looks like we don't have any additional questions in the chat or comments. Do we have additional – okay, we do have a comment.

[LU LIMEI]: I just have one thought about whether this service provider is accredited or not. Perhaps in their application for this domain name [while] they are few in their registrants information there will be one blank to fill that whether you will use privacy or proxy services and let it to check the box so if [it's use] this privacy or proxy services you're going to have two fill in like the accreditation numbers or ID so that this problem will be solved. Did I make myself clear?

AMY BIVINS: Thank you. What do others in the room think about that?

PAM LITTLE: I thought Theo actually flagged that as a potential issue for the RDAP to deal with because what [Limei] is suggesting to me is not consistent with the current display or label displaying requirement. There's no field for that so you need to create a new field to display that? Is that right?

FRANCISCO ARIAS: I didn't hear the suggestion as being as creating another field but just a way to do some sort of authentication of the provider. That's what I understood.

[LU LIMEI]: You don't need to display it but where you fill in the application form you need to [fill] certain information.

VLAD DINCULESCU: A comment what Darcy said earlier about that many registrars use various ways to take information – web forms, APIs, various other mechanisms – that means they don't [have to make particular] changes across the board for those things. They have to [cater all of that through]. That is a very large undertaking to do, to be honest.

UNIDENTIFIED FEMALE: A couple of comments from Steve Metalitz: "Since all privacy/proxy registrations must be labeled as such, one could require that the registrant name include the accreditation number of the provider. And in previous meetings we have decided that creating a new field is not necessary to satisfy the labeling requirement."

AMY BIVINS: Thank you for that, Steve. And we, as Steve mentioned, we have discussed labeling and will be discussing it again soon. That's one option that we could talk about. I think we'll be talking about that more soon.

Francisco.

FRANCISCO ARIAS: Thank you. So without getting into the labeling question but regarding the potential way to provide that information from an unaffiliated provider to the registrar, the issue with that is, again, you are receiving the information – you as the registrar are receiving that information – but then you will have to authenticate it in some manner in order to ensure that that's an accurate information and that's the [problem] I understand. It's difficult to solve from a registrar perspective.

AMY BIVINS: Thank you, Francisco.

JENNIFER GORE: I promise this is the last question I'll ask of the day – well for this session. Let's just leave it at that.

After reading through the final report I just have a simple question which is, how will registrars identify if a registrant or a privacy/proxy service provider is making a change to a particular domain?

UNIDENTIFIED MALE: [Currently].

JENNIFER GORE: Current to a registered domain.

UNIDENTIFIED MALE: Can you clarify that?

JENNIFER GORE: Okay. I will restate the question. How will a registrar identify if a registrant or a privacy/proxy provider is requesting a change to a registered domain name? I think Jonathan referred to this earlier today, but [I'm] putting the onus back on the registrant through the Ts and Cs. But the question is more around identifying the entity of the request.

JONATHAN FRAKES: May I comment? I think there's a requirement of registrars in many cases even to have two-step authentication [and] validation of being able to access the control panels where these changes can be made [and] when logged in. So whoever would have the account credentials to log in for the particular control of this domain seems like the person who would be empowered or enabled to do this. In some cases – and I'm aware of law firms where they do this on behalf of their customers. Other branding firms will do this – but in most every case, the registrant themselves or some accountable party does this as opposed to a third party.

If you trust your proxy provider enough to give them your credentials, it would stand to logic that you have some affiliation and relationship with them. But it seems like you'd have to log in to do this if I'm not mistaken. So the burden would still be upon the registrant and their T&Cs. They're logging into an online system to make changes. Did that answer your question, Jen?

JENNIFER GORE: Thanks. Yeah. Thank you.

AMY BIVINS: Right. Does anyone else in the room have comments on this or questions, or anyone in the chat?

UNIDENTIFIED FEMALE: Jennifer, Steve Metalitz wants to know what kind of change you are referring to.

JENNIFER GORE: Any change that would impact the output of the WHOIS record for that registered domain.

AMY BIVINS: We have some typing in the chat. We'll give it just a minute.

While Steve is typing, does anyone in the room have further questions or comments on this topic?

Okay. So we don't have any more questions for you today so we can go ahead and wrap up. Does anyone else in the room have anything they would like to raise with respect to this IRT before we wrap up for today?

Okay. So as far as next steps go, following the meeting I'm going to go back and compile all of the input that we have received from the IRT today. I'll be sending that around to the list soon. I'm going to probably take a couple of days to go back and listen

to the recording and do that. And then our IRT meeting for next week is cancelled but we will be sending information about the following meeting shortly after the close of this meeting. So, thanks, everyone, so much and we appreciate your participation.

[END OF TRANSCRIPTION]