ABU DHABI – ICANN GDD: Accredited Privacy & Proxy Program Update
Wednesday, November 1, 2017 – 09:15 to 10:15 GST
ICANN60 | Abu Dhabi, United Arab Emirates

UNIDENTIFIED MALE: This is the ICANN 60 ICANN GDD Accredited Privacy and Proxy Program Update on the 1st of November, 2017, from 9:15 to 10:15 in Capital Suite 7.

JENNIFER GORE: Good morning, everyone. Welcome to the Privacy Proxy General Session Update. My name is Jennifer Gore with ICANN staff and I want to thank all of you that have attended the session this morning. Caitlin Tubergen is joining us remotely and will be providing the update, the presentation as she's not feeling very well this morning. So, we will field any questions and she will be on remote, so we will kick it off to Caitlin.

CAITLIN TUBERGEN: Thank you, Jennifer. I want to confirm everyone can hear me before I continue with the presentation.

JENNIFER GORE: Yes. We can hear you.

CAITLIN TUBERGEN: Okay. Thank you. Welcome, everyone, to the presentation on the Privacy and Proxy Service Provider Accreditation Program. This presentation is a general update on the program itself and the progress and implementation Review Team has made thus far. Apologies. I'm just adjusting the slide.

So the agenda for today's presentation is to be begin by discussing a little bit of the project background, and then we'll talk about the activities to date. We'll go over an overview of proposed accreditation program, and then we'll discuss the project timeline and talk about the specific inputs that we're requesting for the public comment period. And then we'll have a time for a Q&A. So, I'll begin by going over the project background.

So, the 2013 Registrar Accreditation Agreement includes a specification that provides for new requirements for privacy and proxy service providers. The specification is a temporary specification and it was put in place policy development process to create a new accreditation program for privacy and proxy service providers. That PDP was officially launched in 2014 and the working group completed its work in January of 2016. The ICANN Board approved the working group's final recommendation in August of 2016.

So, following the Board's approval of the working group's recommendation, the Implementation Review Team was first convened on October 2016. In November of 2016, the implementation confirmed the overall program structure and the way the structure of the program is currently designed is to allow for anyone to apply to be a privacy or proxy service provider and that means entities that are affiliated with currently accredited ICANN registrars and entities that are not affiliated with currently accredited ICANN registrars.

In December of 2016, the Implementation Review Team requested an expedited timeline of the original program design was a timeline of about three years and we will be introducing the first accredited proxy service providers and the Implementation Review Team asked if we could speed up the project plan. And so we condensed the timeline to aim to produce the document for public comment within one calendar year. So, with that timeline in mind, the Implementation Review Team has been meeting every week and going over the documents that comprise the program.

So, in March 2017, the Implementation Review Team completed its first review of the draft policies. In June 2017, the PSWG disclosure framework proposal was delivered to the IRT. And in July of 2017, the IRT began reviewing the draft Privacy Proxy

Accreditation Agreement, and the IRT is currently still reviewing that draft contract.

The IRT's work includes review of several documents concurrently, so as I mentioned back in March, the IRT first reviewed the draft policies. The IRT will complete a second review of this policy after the draft Accreditation Agreement is complete [so that] the two documents are [synced up].

Secondly, there is the draft Accreditation Agreement, which looks very similar to the Registrar Accreditation Agreement. Implementation Review Team began reviewing this document in July and we're currently slated to complete the review of this document by the end of this year. There's also the application/accreditation processes and the IRT has reviewed the draft application as well as the proposed accreditation process.

And lastly, the IRT has been reviewing the draft deaccreditation process, which would, of course, be the process that we utilize in the event any accredited privacy or proxy service provider was voluntarily or involuntarily terminated.

This slide is an overview of the proposed accreditation program. So, as I mentioned before, the proposed accreditation program is very similar to the current registrar accreditation program. When the program is officially launched, registrars must not

knowingly accept registrations involving a privacy or proxy service provider that is unaccredited, and that was one of the working group's recommendations.

So, any entity that would like to become a provider must submit an application for accreditation similar to any entity that wants to become an accredited ICANN registrar, and similarly those applications will be evaluated for both the capability to be an accredited privacy proxy provider as well as a declared willingness to comply with any program requirements, including policy contract, etc. Following the launch as a program, there will be an ICANN-managed compliance program.

And lastly, just a note that those providers that are affiliated with accredited registrars, there are some requirements in the contract and policy that may already be covered via their Registrar Accreditation Agreement, and a couple of examples of that include data escrow and data retention.

Any applicant that would like to apply to be an accredited privacy or proxy service provider has to complete a provider educational program and that will be a program that ICANN creates and scores. It must also undergo a due diligence screening and demonstrate the understanding of all of the policy and contractual requirements.

So the current plan is to launch an initial application window where ICANN will begin receiving applications, and those applications must be submitted during a limited time window. That first batch of applications, once they've been received following the deadline of that initial window, will be evaluated simultaneously and all accredited first round of accredited privacy and proxy service providers will be announced at the same time.

Immediately after we first announce first round of accredited privacy and proxy service providers, the program will transition to an ongoing program maintenance phase, and all that means is it's going to transition exactly what we have with the current registrar accreditation process. So, rather than having a deadline of when you can apply to become a service provider, there will be a rolling application basis, so there will be no restrictions on when an entity can apply to be a privacy or proxy service provider.

We also envision that the applications received after that initial announcement will probably be processed more quickly due to the lower volume. For the initial processing window of that first batch of applications, we're estimating that it may take six months or more, depending on how many applications ICANN receives.

This slide shows a timeline to the final implementation as a program and I would like to note that these dates are heavily dependent. The Implementation Review Team's work as well as a couple of factors outside of the Implementation Review Team's control. So, this is just proposed for discussion purposes but these dates may change.

Currently, you'll see that we're aiming to have the documents that I discussed earlier out for public comment by the end of the year. And that's assuming that all of the feedback that you receive has been incorporated into the draft document, so that that date is pending the Implementation Review Team's work and review.

Provided that the documented are posted for public comment at the end of this year, we begin the analysis of the public comments and that analysis is in conjunction with the Implementation Review Team. That analysis will begin early next year. And again, that is dependent on when the documents are actually [inaudible] for public comment.

This timeline assumes that the public comment receives will be able to be discussed and agreed to by the Implementation Review Team around April of next year, so of course that's going to be depending on what type of comments are received during the phase. So, provided that the Implementation Review Team

gets through all of these comments in a [timely] and expedited fashion, this program could be announced as early as April of 2018. Given the three-month window of accepting the first round of applications, that could mean that the initial application window would close as early as July of 2018, which could mean that we will be announcing the first group of accredited providers by December of 2018.

The second timeline allows for a more, a longer review of the public comments received. So, you'll notice the first two bubbles are exactly the same. However, this shows that the final program requirements will be announced on May of 2018 with the initial application window closing in September of 2018, and the first group of accredited providers announced in March of 2019. I previously mentioned that the IRT is currently still working through the draft contract or the Privacy Proxy Accreditation Agreement, but I did want to note a couple of things where there might be diversion of opinions within the IRT or some things that will be specifically flagged for public comment. And those items include the data retention requirements that are currently in the contract, the law enforcement authority to closure framework, as well as the fee accreditation procedure. And I just wanted to note that community feedback will be requested on all of the program materials, but we are going to specifically highlight

some of the things where the IRT is looking for further feedback on.

So, that concludes my presentation and now we're happy to open up the floor to anyone who has questions or concerns that they'd like to bring up. Thank you.

JENNIFER GORE: Alex?

ALEX: Can you just unsync the slides so I can –

JENNIFER GORE: Sure. Can we unsync the slides?

CAITLIN TUBERGEN: The slides are unsynced.

ALEX: Maybe I can just ask a question on that. So, you had two proposed timelines. So, what will drive which one we take?

CAITLIN TUBERGEN: Thanks for the question, Alex. Sorry. I'm hearing an echo in the room.

So, you'll notice that the divergence in the timelines is the amount of time the Implementation Review Team… Sorry, the echo is really bad. The divergence in the timelines is due to the number of public comments we receive and how long it takes the Implementation Review Team to review those comments. So, this will be unique public comment period, the public comment period. Sometimes the public comments that an Implementation Review Team receives and the ICANN receives, we're able to review them quickly. Other times, substantial issues are addressed in the public comment period that require more time to review. So, to answer your question, it's largely dependent on the kind of feedback we receive from the community and public comment as to which timeline we're able to stick to.

And again, I'd like to emphasize that those timelines are contingent on the IRT's review of all of these materials to be completed this year and that will depend on the IRT's review, so there's no guarantee it will be complete. We may uncover some issues that require more discussion, but that's the goal would be to have those materials published for public comment by the end of the year.

JENNIFER GORE: Alex.

ALEX: Okay. Thanks for that. So, I think what you're saying is that we as an IRT have a job to make sure we review and comment on these docs between now and the end of the year. And assuming that happens, then it goes forward for public review beginning of next year, and if there's a boatload of comments, substantial comments, it will take time to incorporate those comments and it may require another comment period.

JENNIFER GORE: Caitlin, do you want to take that or do you want me to take that? Depending upon the material size of the comments, we may require to go to another comment period.

ALEX: Okay. All right. Thank you.

JENNIFER GORE: Alex?

ALEX SCHWERTNER: This is Alex Schwertner from Tucows. Thanks, Caitlin, for the presentation and thanks, everyone, on the IRT team who has worked on that. I was following the policy development process. I have not followed the IRT and I'm just getting back in and I was

looking at the draft yesterday for the first time and I was surprised to find the size of the document. Honestly, I did not expect that heavyweight document like that and I wasn't expecting an implementation process heavyweight like that. I was expecting something that is much lighter and would still implement the spirit and the requirements of the policy or of the outcome of the PDP.

So, I think it is important for us as Tucows but I guess for us as registrars to closely look at that draft and see what kind of feedback we need to give in the comment period. I think the document right now is not in a good place given all the uncertainty that is going on around how GDPR will affect processes, when ThickWHOIS will come in to place. There's are no provisions related to GDPR in that document, and I feel it is not a good idea to put a new contract in place just month before we may see major changes as to how policies are implemented on a broader level and privacy and proxy services are one way how some registrars may try to become at least part [inaudible] part GDPR compliance, so it is something that will become even more important.

I have worked through the implementation of IRTPC, which was a policy that in the IRT phase got really flawed and almost impossible to implement in any meaningful way. And I would strongly recommend this IRT team as well as the community to

not repeat those mistakes. We can't get a policy that has been agreed upon in the PDP phase so wrong again as we did IRTPC, where we're ending up with something that really no one's happy right now.

So, I would encourage everyone to look closely at this document, use the comment period, and see that we get this right, because it is an important piece of everything we do in terms of how registrars use that and how we move forward with proxy privacy. The whole PDP wanted to fix this and if we don't get this right in IRT, we're not fixing anything.

JENNIFER GORE: Thanks, Alex. Anyone else? Ben?

BEN ANDERSON: Yeah. I'm just going to echo what Alex said, actually, but just a bit more to do with the timeline of the implementation. Have we seriously considered the impact of GDPR here? Because Goran spoke yesterday about possibilities. One of the possibilities that registrars have in order to remain compliant with law is to switch on proxy across every single domain name registration for an individual. That is a possibility and quite a strong one. When you look at this timeline, why is that not taking any of this into consideration?

JENNIFER GORE: Ben, thanks for the question. Obviously, staff is directed by the Board and I think your comment is relevant. And as we discussed this earlier in the Registrar Stakeholder Group, Theo I was expecting to be here today but he's probably in the Compliance session, had mentioned that the registrars were going to submit a letter and raise that concern. Obviously, we are considering that but the IRT is still moving forward.

BEN ANDERSON: Thanks, Jen. I mean, I think in that letter will come. I know that we are talking about it at the moment. I just think it's where the Board spoke to the registrars and the registries yesterday and talked about possibilities, there's three possible ways, there's no real thought or they haven't got the legal advice yet. I think the feedback from staff to the Board is that there's going to be a train wreck of quite a lot of different things at exactly the same time, so do we need to consider whether or not this timeline is appropriate pending the advice from Hamilton to the CEO?

JENNIFER GORE: Thanks, Ben. Yes.

PETE ROMAN: Hi. Pete Roman, U.S. DOJ. I just have a quick question about all this. So, during the process of the IRT, have you not been thinking about the GDPR in putting this together? Because that seems to be the implication of both of these comments is that there's been no consideration whatsoever given to the potential implications of the GDPR on the privacy proxy system.

JENNIFER GORE: We have a fairly sizable internal effort going on, including with outside counsel, to evaluate it. But we also have provisions in the document that allow for us to comply with laws to the extent that we get advice back as to how we need to make changes for the GDPR.

MARY WONG: Sorry to interrupt. This is Mary from ICANN staff. Just a reminder to everyone to please state your name before speaking for the transcript. Thank you.

JENNIFER GORE: Yes.

PETE ROMAN: So if the GDPR is considered and there are provisions within this to deal with local laws, does that alleviate at least some of your concerns about the timing?

BEN ANDERSON: I don't think it does at all and I'm not entirely sure that have it waiting for outside counsel to provide advice and letting everyone know that advice may be coming and to implement a policy a month before wider implications are implemented, I'm not entire sure is a sensible approach. I mean, I think everyone wants to wait and see what this advice is from outside counsel. I just don't think it's sensible to implement something that will probably be impacted significantly by that advice and everything else going on. It just doesn't make sense to implement something and know you're going to have to change it.

ALEX SCHWERTNER: Yeah, addressing the same concerns, the provision would be to change the policy to comply with law. Well, I mean, that's the place where we all with many policies exactly right now [inaudible] – I'm sorry, this is Alex Schwertner from Tucows – where we have this policy and then we have the law and it's not compatible in any way, and really hold this question is how do we bring this back together? And now we're deliberating starting

again from two separate places where everything points towards some incompatibility and we don't [inaudible] there if we can avoid this going with the policy that doesn't even exist to go to the same place where we are with all the other policies today. Of course, we can do that but to me, that doesn't make any sense whatsoever.

JENNIFER GORE: We look forward to the feedback and I know the forthcoming letter from the registrars. Any other questions? Comments? Mary.

MARY WONG: Hi, everyone. This is Mary from staff and I'm going to speak on the policy side because that's the team I'm on, so I just wanted to remind everybody that there is a distinction between whether it is the policy itself that is or is not compliant or that where subsequent developments such as on the legal side may raise issues with the actual policy recommendations. There's a distinction between that and specific contractual provisions or other requirements and criteria, which are developed during implementation. So, hopefully, in comments that anyone in the community sends back, it would be really helpful if any concerns that you had, you could point where they're specific to the policy

recommendations or to particular details with the proposed implementation. Thank you.

JENNIFER GORE: Thanks, Mary. That's very helpful. Alex?

ALEX [DICKENS]: Yeah, hi. It's Alex [Dickens]. Mary, I agree with that. So, I'm looking forward to seeing this letter from the registrars and I hope that it actually proposes a path forward and doesn't just say kind of you that it's broken and nothing can be done. I'm hoping that it's helpful and not only is it raising a concern, but specifying how the concern could be addressed and how the IRT could, perhaps, suggest how the IRT can move forward in its progress. I think that would be great.

JENNIFER GORE: Thanks, Alex. Any other comments?

PETE ROMAN: I'm new to the process, to this process, I'm new to the IRT, so if I'm asking questions everybody else knows, I apologize ahead of time. I was under the impression that there was a deadline in January for some reason where something about the current privacy proxy system was going to be expiring. What provisions

do we have here since this process clearly is going to go on beyond that to continue what the current process or to do something to allow privacy proxy to continue with some sort of program given that deadline?

JENNIFER GORE: Peter, great question. So, we face the same deadline about this time last year with the registrars and the interim spec, privacy proxy spec within the 2013 RAA. And I know the registrars have just completed a vote recently and, hopefully, the results of that vote will be shared with the community shortly as far as whether or not the registrars are willing to extend that deadline for another year.

PETE ROMAN: What exactly happens if they do not extend that deadline and this process goes on through December 2018? Is anybody going to be allowed to continue? I mean, are we going to go back to the old system where privacy proxy was done on a completely ad hoc basis with no supervision of the folks who were providing it?

JENNIFER GORE: Obviously, we want to try to work with the registrars to get that extension. If not, the service can remain operating by registrars in an unregulated manner.

BEN ANDERSON: And outside of my capacity on the registrar ExCom say if there's no extension, then there were no provisions. I mean, the registrars are fully supportive of this. I think we all understand the need for it, and the vote is going on at the moment, so I expect the results by next week.

JENNIFER GORE: Thanks, Ben. Any other questions, comments? Yes, sir.

JONATHAN [MICHALSKI]: Hi. My name is Jonathan [Michalski] with [inaudible]. This topic is of particular concern and interest to me and I'd like to have some just suggestions of how I can get more actively involved to understand what's going on besides for what's on the wiki in terms of participation. Thanks.

JENNIFER GORE: Yes, absolutely. I'll be happy to talk to you after this session.

JONATHAN [MICHALSKI]: Thanks so much.

JENNIFER GORE: Sure. Going once, going twice. Thank you, all, for joining us today and thank you to Caitlin, who's unfortunately not feeling so well this morning, so we appreciate her joining remote. And thank you so much.

[inaudible] no? Okay. Thanks so much for joining this morning. Oh, I'm sorry. Oh, sorry. Peter.

PETE ROMAN: I'm clearly the talkative one today. My understanding was that there were still some piece that needed to be negotiated concerning disclosure and timing, where when a request was made to a privacy proxy provider, how long it's going to be before they return and said whether they, I think whether request was properly formatted and the information was available. Is that still under discussion?

JENNIFER GORE: That is still under discussion and I actually will turn this one over to Caitlin because she's a subject matter expert on this open item. Caitlin, are you still there?

CAITLIN TUBERGEN: Thank you, Jennifer. Can you hear me?

JENNIFER GORE: Yes.

CAITLIN TUBERGEN: Okay. Thank you, Peter, for the question, and that's correct. There isn't currently an agreement within the Implementation Review Team for that timing, so it is an open matter.

PETE ROMAN: Is that something we need to be discussing now? Or is there a provision to do this at some other point?

CAITLIN TUBERGEN: in one of the slides, I mentioned that some topics that we will specifically flag for public comment, and those topics are things that there might be some divergence within the IRT. So, that would be one of the items that we would flag for public comment. I believe that registrars on the Implementation Review Team, feel free to chime in here, but I believe that at least within the registrars, the registrars did not agree to the current 24-hour timeline of response. And so if you have another proposal that you'd like to bring to them or bring to the IRT, we

are happy to discuss it. Otherwise, we can leave the framework as is and flag it for public comment.

PETE ROMAN: I actually do have some language that I wanted to propose to the IRT. We have the PSWG has been in negotiations with the registries on a similar emergency disclosure provision that I thought might be acceptable to this group. We could use more or less the same language that essentially says that at least my understanding of it is and I haven't really dug into the details yet but my understanding is, is that what it does is if there is a request that's an emergency, there's a life and limb emergency or there's a child abuse, act of child abuse going on or something like that, that their registrar needs to or the privacy proxy provider needs to respond immediately, but if there is not that kind of an emergency time pressure, then the privacy proxy provider can respond in I believe it was two business days was what everybody was looking for. I'm not sure it's two business days but something equivalent to that.

JENNIFER GORE: So Peter, I suggest that we pose that to the IRT list and we can talk about that after the session as to how to move forward on that regarding next steps. Did we get another question?

JONATHAN [MICHALSKI]: I'm just trying to understand what part of this process potentially conflicts with the GDPR. It seems from the outside having not looked at, I want to get on top of everything going on, but it would seem that GDPR makes this all the more compelling and important, but what exactly about this process is potentially conflicting without – I'm not trying to say it's not, I just don't understand.

UNIDENTIFIED MALE: [inaudible] speaking for the record. It's not necessarily a conflict. It depends on what the consequences of each action are. I mean, when you have an escrow piece, then you have to look at how that escrow piece fits in to the [inaudible] of the GDPR. If you have a reveal piece, then you have to see whether the reveal is possible on the GDPR. I don't think that it's generally impossible to do any of these. I think all of them are possible. You just have to make sure that the stay within the requirements of the law. So, there is an impact but it's not a problem. It's more like of we have to take care of the fits.

JONATHAN [MICHALSKI]: Okay, so now I'm starting to understand a little bit better. Thank you. So, I just wanted to express the significant need for

compromised phishing sites and malware sites that we're able to in the cybersecurity community be able to get the information we need to contact these people to help remediate this threat within a reasonable timeframe. I would say 24 hours seems like the maximum amount of time that would be reasonable, according to industry standards that's been in place for a long time to get this information.

It seems like from what I see, the left hand and right hand at registrants with proxy services have no clue – the right hand and left have no idea what they're doing. So, the companies that can remediate threats are not even able to figure out that they're responsible for helping to remediate the threat. So, in other words, it's being used to avoid accountability, so this is really important to address, so I hope that we could take this opportunity of GDPR to get something like this up and running quickly. Thanks.

JENNIFER GORE: Thank you.

UNIDENTIFIED MALE: Well, I think you should differentiate as we have between two factors. The one is reveal and the other is relay. As long as there's a relay function and you have the contactability, even

though you do not know whom you're contacting, a lot of the need for the reveal becomes lesser, I think. Because once you have the ability to contact directly or indirectly, for example, through a mail forwarding service at the privacy proxy service provides, that's automatic, then that does not need to have to be an immediate or as urgent reveal function and you also have to bear in mind that many of these privacy providers, they are very, very slim, so that's maybe one staffer, the CEO [inaudible] himself or whoever operating all these functions in themselves, so and usually they have another day job, as well, so basically, look at the business practices, look at the size of these operations, and think about what they can logistically achieve in a reasonable timeframe. I think two business days is good. 24 hours is a bit problematic because people have weekends, people have holidays and are away from their computers for a while.

JONATHAN [MICHALSKI]: I would just say to that, that exactly because of the lack of maybe resources to proactively stay on an incident and mitigate it, you need to – not you personally – but we together need to collaborate to be able to provide incident responders with the information they need so that they can proactively mitigate these threats and that it does not, in my experience, work through relay. So, we hopefully, just like we're tackling the

issues with WHOIS, we can tackle the issues of what you need to change in terms of service. Like, we're tackling these issues now, so the same issues that need to be tackled on the WHOIS side need to be tackled, I would think, in the terms of service to make sure that when there's blatant violations – and I'm not talking about the wrinkles, I'm not talking about outlier cases, I'm talking about blatant violations of terms of service that we figure out a way to update those terms of service to be consistent with GDPR. And I'm not saying I have the answers to this. I'm just saying there's an urgency here that we address this. Thanks.

PETE ROMAN: I'd like to echo those comments because I'd like to make a point on this business argument, which is that if I have a terrorism problem, I've got somebody who's threatening to blow up a bomb in the next 24 hours, or I've got a kid who's actively being abused online, I don't care whether you're on vacation. I don't care whether you're a small shop. If you cannot meet those requirements so that I can protect people out there in the world, maybe you shouldn't be in this business.

UNIDENTIFIED FEMALE: So, my name is [inaudible], I'm from one.com and I'm a registrar. So, as far as I remember, I joined the session in Copenhagen, there is rules in there on how fast you have to relay e-mails to

the real owner, so I don't see the problem. You also have the abuse contact for stuff like that already now, so I don't really get the problem.

UNIDENTIFIED MALE: I can give you anecdotal illustrations from just yesterday or from every week it's another issue that I see personally in escalations that come my way. And I'm not saying that there's one party – like I'm not putting the responsibility specifically on the privacy and proxy provider or on the registrar. I'm saying we need to collaborate to solve this problem because it requires proactive constant vigilance by a 24/7 team to be able to get to the person who's able to mitigate these threats. And you don't have the resources to do it. We need to collaborate to figure out how to make the system work so that those who do have the resources to contact the party respond can get the job done.

And saying that "I'll get back to you tomorrow" is just simply unacceptable and worse, registrars don't even know affiliates. They don't know. It seems like companies are taking safe haven in privacy and proxy providers in order to avoid accountability and the registrars say, "Sorry, I don't have access to the information. The privacy and proxy service providers have their concerns, too, in protecting the registrants." I'm not saying a lot of the times this is compromised and not necessarily, but you

have to presume at some point that what was assumed benign becomes malicious. When there's a pattern or practice of these kinds of services being abused. And I think that some privacy and proxy service providers cooperate more than others and there's a way to solve this problem together. I am not caught up on everything going on here and I do want to get caught up on it because it's become an emergency that we solve this problem because we can't let the open Internet become the darknet. It's simply unacceptable and that's what's happening. Thanks.

UNIDENTIFIED FEMALE: Can I just respond to that? It's [inaudible] from one.com. What I'm hearing from you is an existing problem, not something that comes along with this process. So, what you're talking about is already an issue now and you're trying to solve it through this new policy or –

UNIDENTIFIED MALE: I'm hoping that these policies can help solve existing issues and maybe I'm wrong to assume that. I'm not fully caught up, so I will get caught up. I'm just hoping that some of what we're working on here would solve some of these issues but I might be mistaken in that regard. Thanks.

UNIDENTIFIED MALE: [inaudible] speaking for the record, sorry. The new policy is already mitigating a lot of these issues because you will be getting an answer at all. I mean, some of these services that we have currently, they have no accountability and they have no response times. They are like a black hole and this will go away. You will have defined response times, defined processes to forward this under the new project. It's just we have to face business realities, we have to face process realities when we implement this that make it possible for the services that do legitimately operate to continue operating in a manner that is still sustainable.

PETE ROMAN: Two thoughts real quick. The first one is that, again, and I know I'm using extreme examples, I'm not talking about every request that would be made. I'm talking about a very small number of requests that will be super high priority. The really high priority requests that come from law enforcement need to be addressed quickly and the relay is not going to be the solution if the person on the other end of the relay is the guy who's going to be blowing stuff up or is the guy who's actively abusing the child. It doesn't help me for you to tell him I'm looking for him. In fact, it makes my life worse. Right?

And I do get the business realities. I understand that there are limits but maybe we've got to find some way in which these folks can meet these deadlines in the emergency situations because there are going to be emergency situations. There are not going to be a lot of them, we don't do it all the time. All the other providers who do other kinds of things like Facebook and Google and whatnot have provisions where they get turnaround for us on an emergency basis in these kinds of situations.

So, this isn't a new requirement for the industry, either. This is a requirement that's been met and addressed and people have reached compromises. Small providers are able to do this, so it's something we need to think about is if there are business limitations like that, then how do we help folks who are that limited in terms of staffing to meet this requirement? I mean, maybe this is another business opportunity, right? Maybe somebody could set up a service for privacy proxy providers to handle emergency requests for them so that they can go on vacation and they can have a life. Because I'm not against that, either. I like to have a life, too.

UNIDENTIFIED FEMALE: This is [inaudible] from one.com. You are aware that everyone contacts us as a registrar thinks it's an emergency.

PETE ROMAN: They're defined standards. They're very particular defined standards. It's imminent loss of life and limb, active abuse going on, active abuse, not cyberabuse necessarily, although potentially depending on how bad it is, but abuse of children, stuff like that. This is not a I think it's an emergency, it's got to be sort of objectively an emergency and that language would be hashed out in the conversation so that it's not always being put on you as an emergency. I understand that. Yeah.

UNIDENTIFIED MALE: To give some context on this, two points. Sorry.

ALAN WOODS: This is Alan Woods, former Donuts, and I'm the Co-chair of the Security Framework Drafting Team for the registries and the conversation has somewhat moved on since my point but it was going to be but everything that's been talked about here is very reminiscent of the conversations that we have for a period of a year and a half as specifically about the 24-hour turnaround and just to give it a bit more color and context on that. That there were very hard lines on both sides in [inaudible] all three sides, really, in the argument on this, 24 hours again for the specific need for public interest intervention that the need for this, but then again, a lot of dialog and a lot of conversations brought us to the point where we're saying yes, well obviously a registry or a

registrar who is in a position to do that who is a good actor will, of course, do that, but there's a huge difference between stating that and putting that into a document, which people are going to be bound by. And we have to take into account things such as the difference of from even up to the local laws to local considerations to the terms and conditions of the individual registry operator themselves, and of course, then to the severity of the actual report itself.

So, as I said, I'm hearing all this and it's bringing back flashbacks for me of this discussion. There is a way that you can easily come to a compromise on this but it is a compromise on both sides. I think you need to accept the fact that registrars are also trying to be good players, most of them, and the ones that are going to be signing up and following this properly and to this process are going to be wanting to be good actors in this, but you can't just have the conversation on saying but what about the children? We've had that conversation before and it doesn't help the discussion, so I would just from the experience of the security framework and also I'm very proud parent and hearing that maybe the language that we have put into that document might influence this, I would just say obviously, just think about where you're both coming from because you'll cut months of discussion on this [inaudible].

UNIDENTIFIED MALE: Maybe just one further or two further things to color this discussion. We're taking first step here to regulate this industry. We're taking the first step to make sure that there is a response, and I think there will be second steps that will be further steps.

For example, once we have a tiered system, a tiered access system with law enforcement will have their own access. You can automate this. So, I envision as part of the results of the RDS Working Group that we will also have a tiered function for privacy proxy service providers that will be implemented at that stage. So, we're taking a first step now, second step later on. I think if you look at it in that context, I think it becomes much more manageable and much more reasonable.

Another point being just a little bit of color, I would like to add. I mean, as a registrar, we once got a takedown request for a domain name that was used by terrorists as a forum for exchange of information and they were talking about all kinds of stuff on there and we got to a takedown request from a European law enforcement agency and while we don't have to react on those, we did because we felt it was right. Half an hour later, a phone rang in the office and a German law enforcement agency asked us with quite an angry voice what the hell we were doing. They were monitoring that site.

So, sometimes fast reactions [inaudible] we've always contacted German law enforcement first before we take certain action, such a case. So, sometimes a fast reaction is not the thing that you want.

PETE ROMAN: We actually have language that I was going to propose. I had shown it to her before. The registry group already agreed on language that I thought we could use as a model that talks about emergency disclosure and whatnot, and lets us maybe not rehash all of the conversations that they've already had and create post-traumatic stress disorder over here.

JENNIFER GORE: Yes.

JONATHAN [MICHALSKI]: I just feel personally and in my own personal capacity, I have to say I really hope we can move to a world where like there's no question in my mind that substantial bodily harm and terrorism, those kinds of things, should not be treated in the same category as other cybersecurity threats, like those need to be treated as a real emergency. I just want to live in a world where that means that can be dealt with in hours and not days. That's all. Thanks.

FRANCISCO ARIAS: Hi. This is Francisco Arias from ICANN Org. Just because [Volker] mentioned differentiated access, something in table, I just want to take the opportunity to [inaudible] on that here for an effort that is trying to work on that regard. It's not totally related to the discussion here but I thought maybe interest to you, Pete, and others.

In the context of RDAP, RDAP being the protocol on the Internet to replace WHOIS, hopefully, in the future. We have a session today at 1:30 in which we are working on a pilot with contracted parties and one of the topics of interest there is, of course, differentiated access. How do we make that work? And so if you're interested, please be there at 1:30 and raise this important issue. Thank you.

GRIFFIN BARNETT: Thanks. I just want to note, and it's up here on the slide, law enforcement authority disclosure framework, and it discusses in the draft framework things that you're talking about, about urgency. In fact, some of the language in here is disclosure within 24 hours and it specifically lists things like high-priority requests, including a threat to life, serious bodily injury, and things like that. So, it has been taken into account. I think you want to look at the draft, law enforcement authority disclosure

framework, something you should do but it's being considered. Thank you.

JENNIFER GORE: Good point. Thank you. Well, thank you for the lively discussion. There is any other comments, questions, feedback. All right. Thank you. Have a great day, everyone. Please stop the recording.

[END OF TRANSCRIPTION]