HELSINKI – Privacy and Proxy Services Accreditation Issues
Tuesday, June 28, 2016 – 11:00 to 12:00 EEST
ICANN56 | Helsinki, Finland

CHAIR SCHNEIDER: Thank you very much, Tom. So we will now move to our next session which is linked to -- or the follow-up of the working group meeting of the public safety working group this morning that was very well attended, so let me hand over the floor to Alice, one of the co-chairs of the working group.

ALICE MUNYUA: Thank you very much. We have the slide up. Julia, can I have the first slide, please? We had a very constructive early morning meeting, discussed quite a number of issues and also discussed possible way forward regarding how the GAC may want to approach this issue during the joint meeting. I'd first like to start off with a very brief background or context of where this privacy/proxy services issue and process comes -- was -- came up. It was first convened following a GAC endorsement of the law enforcement due diligence recommendations in 2010, and then those recommendations, as you recall, were implemented in the 2013 Registrar Accreditation Agreement. However, this specific issue of privacy/proxy accreditation was then deferred

to a PDP which -- the GNSO PDP which completed its work and now has the final report.

Very briefly, the next slide, please. Yeah. Very briefly, what is privacy/proxy service, and there I give an example, for example, my, you know, ww -- my alice.com using a proxy service. You can see here that it has my address as Arizona, the U.S., but I live in Nairobi, sometimes in Addis, sometimes in Johannesburg, but it doesn't really give the proper address or details, my details. So it's information that does not show the actual registrar at all and shows the name and contact information of that proxy company and the actual registrant and privacy company contact is what is provided. And then just to demonstrate how serious this is, roughly one in five domains use this service and of this nine -- it's nine out of ten. Next slide, please.

Previously -- it's good to -- to mention that as previously that there was no policy of privacy services to date until the 2013 accreditation -- registrar accreditation and very few got policies and rules existed regarding this issue. So this led to a lot of unpredictability for stakeholders affected by these services. And so while there might be a distinction between registrars that are ICANN accredited because of the Registrar Accreditation Agreement those who are not ICANN accredited do not have that obligation.

So the GNSO PDP that was working on this issued recommendations for ICANN to accredit privacy and proxy services. It was approved by the GNSO, and right now we're at -- at the point where the ICANN board is meant to be voting to adopt this -- this report. However, as mentioned during our Marrakech -- communique in Marrakech, the public safety working group raised concerns that some of the recommendations that the GAC had provided were not taken into consideration.

So the rationale provided by the GAC in terms of the recommendations we provided to the PDP was that the P/P service providers should keep law enforcement agent requests confidential as required or permitted by laws -- local laws in various jurisdiction because notifying the customer may actually hinder investigations. And in some countries they mandate confidentiality -- there's a mandate for confidentiality of law enforcement's requests.

The second issue that was not taken into consideration and that the public safety working group and the GAC had provided as a recommendation was the requests from other jurisdictions and how those would be treated. And especially taking into consideration that malicious conduct often takes place across borders and investigations often involves LEAs from outside the privacy/proxy service provider. So there is the issue of

jurisdiction and there's also the issue of cross-border cooperation.

The third issue was in commercial domains that collect money for goods and services and the GAC is of the opinion that they should not be allowed to use P/P services or conceal WHOIS identity for this to protect consumers and their financial information and also combat fraud and crime. And also the public rights to know who they're doing business with. And this is in line with disclosure obligations, especially, for example, in the European Union. Next slide, please.

So the recommendations, I think it's very important to note that the GAC mentioned that the recommendations are really positive and the GAC is not proposing to delay the implementation of the report. However, we note that it is flexible enough to allow some of the GAC concerns to be addressed during the implementation phase, and this would help avoid the GAC conflicting with the GNSO advice and also in delaying the program. So there are several ideas. Next slide, please.

Next slide, please, Julia. There are several ideas on the possible way forward that the public safety working group has proposed. The first one -- I'm sorry, the next slide is not on -- that provides -- yes. Thank you. So the first issue -- the first proposal is

regarding the confidentiality of LEA requests. What we are suggesting is the development of a framework, a disclosure framework. I think that should be possible during the implementation, especially working with the -- the implementation review team. And then the handling of LEA requests, foreign requests, possibly also through framework of disclosure. And then the issue of commercial domains. That's a much more difficult one because the working group made it very explicit that they really do support the decision for commercial domains to remain -- to continue using these services.

And then another -- another proposal is to develop a DE accreditation process for P/P service providers that conceal the identity of bad actors and do not respond to LEA requests. And also the possibility of a differential disclosure treatment in the LEA disclosure framework for domains processing financial transactions. Next slide, please. Next slide, please.

Okay. So this is more information regarding -- just to understand the process that the GNSO has followed and the process that we're at. So the implementation process is going to take about one to two years. And once the board has approved the -- the report the Global Domains Division will begin the implementation. And because there were previous concerns regarding the GDD and how they were implementing some of the policy -- the policy proposals, there's now -- it's now mandatory

for the GDD to create what they call an Implementation Review Team with volunteers from the GNSO and the general ICANN community. So while there -- I think the public safety working group and law enforcement agents could be consulted, not necessarily participate because perhaps this could be too much work overload. They could consult on at least some of the relevant areas. And then, of course, the next process now is the -- the next meeting that we -- the joint meeting where we're going to be discussing some of the concerns that the GAC discussed or raised during the recommendations that we provided. Thank you, Thomas.

CHAIR SCHNEIDER: Thank you for this very clear presentation of something that is actually very complicated in the details so that was not easy. So we have -- it was wished by the GAC that we have like first a discussion among the GAC members. Of course, the meeting is open to everybody, but that we have -- spend 15 minutes or so among us and then invite people from the GNSO and from the board to join the discussion. So this has already been presented and discussed to some extent this morning in the -- in the working group, public safety working group, but formally we need to have a quick check with the whole GAC. So please, make your voices heard now. Those who support this proposal or

those who have questions on this proposal, the floor so yours. I see Norway.

NORWAY: Yes. Thank you, Chair, and thank you, Alice, for your presentation. So really, I'm sorry I haven't the full overview of all the details but I have a question for clarification regarding the issue two, I think to handle law enforcement requests across jurisdictions. Is this mechanisms or implementations to be sort of in parallel or how do they relate to the existing law enforcement procedures to handle requests across jurisdictions, sort of the official police cooperation that exists? Thank you.

CHAIR SCHNEIDER: Thank you for this question. Who would like to respond to this one.

UNKNOWN SPEAKER: European Commission.

CHAIR SCHNEIDER: European Commission. Thank you.

EUROPEAN COMMISSION: Yes. Thank you very much for this question, which gives me an opportunity to clarify. So this would in no way impact upon the existing procedure rules. So in every country law enforcement would continue to comply with the procedural requirements, including all the rights for the protection of the rights of the defense and so on and so forth. This would simply ensure that from the contractual perspective of the implementation of the proxy and privacy accreditation processes we do not create any additional obstacles to such requests but they would, of course, still continue to be subject to the leader framework in each of the requesting countries and also in the recipient countries. So no changes would be made to the existing legal framework. We're just looking at avoiding additional obstacles for those countries which do consider under their legal framework such requests to be appropriate. Thank you.

CHAIR SCHNEIDER: Thank you for this clarification. Other comments or questions on the proposal. I see the United States.

UNITED STATES: Thank you, Thomas. This is just to offer the support of the United States for the next steps as outlined above, just with the emphasis in -- just on ensuring that the -- these next steps don't

reopen policy issues which have already been established by the PDP process. Thank you.

CHAIR SCHNEIDER: Thank you, United States. Any other views of support, expressions of support, questions, comments? Complete objection?

Do I take this silence as that you think that this is a reasonable way forward that is being proposed by our working group? I see people nodding. I can't see any shaking heads or raised hands.

So should I consider this the end of the GAC internal discussion on this, that we have support for the way ahead proposed by the PSWG? If that is the case, I think we can use the remaining time for the exchange with those who are here from the GNSO. And I see some board members are also here.

So, maybe if -- there's some spaces for you here. Why don't you come up, the ones that are the most closely working on this, the people from the GNSO working group and board representatives who have been looking into this. That may be helpful.

Thank you very much for joining us. Maybe quickly present yourself so that everybody knows who you are and how you're dealing with these issues. Thank you.

STEVE METALITZ: Thank you. I'm Steve Metalitz. I'm the co-chair of the PPSAI policy development process working group.

GRAEME BUNTON: And I'm Graeme Bunton from Tucows, another co-chair of the working group. And we should probably also acknowledge Don Blumenthal who was a chair of the working group for a period as well.

CHAIR SCHNEIDER: Maybe I could give the floor to Alice to frame the session and then we hand it over to you. Is that okay?

ALICE MUNYUA: Thank you very much. And you are welcome to this session.

Just recall the objective of this session is to discuss how GAC concerns with the PPSAI recommendations could be best addressed, notably whether they could be addressed during the implementation of the working group recommendations. And, again, it's important to note that the GAC is not proposing reopening any policy issues. We actually do -- we are -- we support the adoption of the report. But what we want to do is to explore possible ways of addressing our concerns, the concerns

we raised earlier and how this could be addressed during the implementation phase.

As you recall in the GAC Marrakech communique, we noted that the final report that you produced and submitted to the board raised some public issues regarding consumer safety and trust. And that's our Marrakech communique advice to the board to allow sufficient time for us to consider some of the issues. That's why we have this meeting.

So, once again, the recommendations are really positive -- we need to re-emphasize that -- and establish an ICANN accreditation program where there was none. So it's a good thing.

And we also note that the report seems to be flexible, and it may allow for the GAC concerns to be addressed again during the implementation phase. So that's the objective of this session, and we would like to have that discussion with you especially around the few, three or so, issues that we had addressed. Thank you.

STEVE METALITZ: Thank you very much. This is Steve Metalitz for the transcript.

First of all, I want to thank the GAC for this opportunity to have this discussion with you. And I know I sat in on some of the

earlier public sessions this morning, and it was very helpful for us to gain a better understanding of the thinking behind the comments. And we do appreciate the comments we receive from the public safety working group on our initial report.

I can assure you -- and I think I can speak for Graeme on this also -- that the issues that were raised by the PSWG were very thoroughly considered and discussed by our working group in preparing its report. In one case at least the issue regarding commercial uses -- use by commercial players, that was perhaps the single issue that we devoted the most time to discussing.

We think that looking back on our two-year process of the working group, I think that more active participation by law enforcement representatives in the overall work of the group and better communication from us to the public safety working group would have been beneficial. I think we have some lessons to be learned from that. And, hopefully, we can do a better job on both sides with that communication going forward.

I also want to very much express my appreciation for the comments that you and others have made about not wishing to hold up the implementation of these recommendations. We do appreciate that and hope that the board will be in a position to move promptly to approving these.

Implementation is going to be a difficult, complicated process. And we knew that even before the GAC advice from Marrakech. There are many issues that have to be resolved in the implementation process.

And I also appreciate your pointing out that the interim rules that are in effect right now, which are quite minimal by their own terms, expire at the end of this year. So we have no time -- we really need to be moving ahead on implementation as quickly as we can.

I did want to comment on one of the slides that indicated -- that talked about the implementation process and indicated that the implementation review team could consult with the PSWG and with GAC representatives and others in its work.

I would go farther than that, unless the staff will correct me if I'm wrong. I would hope that the PSWG would participate, that its representatives would participate, actively in the Implementation Recommendation Team, the IRT.

It's a relatively new modality that we have for handling implementation or at least it's new that it's mandatory. And this is a good example of why we need a good, strong implementation review team. And I think that representatives from law enforcement, from the PSWG hopefully will play an active role in that team. I think that would definitely improve

the quality of the implementation that we're able to recommend.

So those are at least my general responses. And I'm happy to yield to Graeme for other thoughts on this.

GRAEME BUNTON: Thanks, Steve. No, I think you covered a lot of that very clearly.

I think going forward we need to be careful about how we approach implementation and make sure we're doing that with clarity and a light touch. But it does feel like there is some room to move forward there and hopefully come to some compromises. Thanks.

ALICE MUNYUA: Thank you very much.

As you can see here, we have three areas that we would like to perhaps discuss with you further. And one of them is could a satisfactory disclosure framework for law enforcement agent requests including confidentiality requirements be developed in the implementation phase? What do you think about that?

And, also, jurisdictional issues and concerns.

And are there any ways to mitigate GAC concerns about allowing domains that seek financial information from people?

So those three we would like to share any views you may have on that and how those could be approached during the implementation phase. Thank you.

STEVE METALITZ: Thank you for those questions and those points. Let me try to take them in the order that they appear on your list.

We -- I think you can see from the working group final report that we flagged the lack of a disclosure framework for LEA requests as a gap that still had to be filled. So I think in the implementation process, that would be an appropriate time to figure out what's the best way to facilitate getting that gap filled because it exists now.

On the confidentiality point there, again, I would say -- I think I saw one slide earlier that suggested that there wasn't any requirement about this in the report. And I have to differ slightly.

The report says the working group recommends that accredited privacy/proxy service providers should comply with express requests from law enforcement agencies, not to notify a customer where this is required by applicable law.

So I think it's pretty clear that if you are in a jurisdiction where you receive a request from your local law enforcement and you

have a legal requirement not to disclose that, that if you do disclose that, that would have consequences for your accreditation. So it would be incorporated into the accreditation standards where it's a requirement of the applicable law.

I understand the concern that was raised by the PSWG was to go farther into situations where it's not a requirement for applicable law. And the report does stress that it's not intended to prevent providers from either voluntarily adopting more stringent standards or from cooperating with law enforcement. So hopefully that provides some guidance at least in that area on the first question.

On the second one, I do want to say we understand the concern about the jurisdictional issue. And really this boils down to obligation to respond to law enforcement requests that are not from your jurisdiction, you the service provider.

And we felt we had relatively little room to maneuver on that question because it had been discussed or worked out in the Registrar Accreditation Agreement which was adopted just a year or two before we started work -- or maybe the year before we started work on this process. Maybe it was the same year. It was about the same time.

And that decision that was reached there -- or the resolution that was reached there was that it only applied to requests within the jurisdiction.

We felt it would be very difficult to reopen that question when, again, if you look at who is providing these services now, for the most part, it's the affiliates of accredited registrars that are living under the 2013 RAA and have that rule about when they are obligated to respond.

Obviously if that changes, if there is a way to resolve that broader question of how service providers should respond -- should validate and respond to requests from outside their jurisdiction, we put in -- if that's changed in the RAA, our recommendation was that it automatically be changed in the accreditation standards as well. So if that broader question can be resolved, then it would automatically be incorporated within the accreditation standards.

Maybe I could stop there and just see if Graeme has anything to add on those two points because I think the third one was is a little bit different.

GRAEME BUNTON: No, I think that was well-summarized, Steve.

STEVE METALITZ: And, finally, on the third point, use by commercial provider -- use of privacy and proxy services by commercial entities, if I can summarize it that way, as I said, this was really the single issue that probably occupied the most time and energy within our working group. It was the subject of many, many thousands literally of public comments or of petitions that we received.

The views were actively debated within the working group. And I think it's fair to say that included the views that are parallel to those that were recommended by the PSWG. And we were ultimately able to achieve a consensus, I think, that there are many working group members that would share the disappointment that the PSWG felt with where that consensus came out. But I think that's kind of the essence of the process that we went through, was that even to there was disappointment about that, there was a sense that this was under the ICANN standards a consensus that had been reached.

We did point out in the report that some privacy/proxy providers have this type of restriction already in their rules. And it's spelled out in the report that there's no wish to discourage providers from adopting similar policies.

One touchstone, I think, of the report is that we do recognize the need for the service providers to have flexibility in their policies and also to have the capability of enforcing them.

So -- and we also stressed that the provider should remain able to terminate this privacy/proxy service to a customer that's engaged in commercial transactions with domain names using the privacy service that carry out illegal activities or that abuse the terms of -- violate the terms of service in other ways.

But I think the point that you raised in the -- that was raised in the -- one of the slides about possibly incorporating this into a disclosure framework for law enforcement, I think that's an excellent idea if that can be done, because we -- I think we all recognize that some uses of these services by commercial entities may also involve illegal activities and we need to be able to find some way to thread that needle and make sure that there's an obligation to deal with those.

So hopefully in the -- my view, anyway, is that in the implementation process, we can build on the experience of the service providers that have a policy like this in place.

And the other thing that implementation, I'm sure, will do -- the implementation review team -- is recommend what points about the policy should be reviewed, and when, so we can see whether we are, in practice, having a problem here, a gap here that would need to be filled.

So I'll stop there and pass to Graeme.

GRAEME BUNTON: Thanks, Steve. This is Graeme.

I think Steve is right that there is some room there for mitigation of LEA concerns specifically around the commercial distinction issue. Perhaps I can add a bit of color from the other perspective on that one, which is that there are many members of the working group much relieved to know that people like dissident bloggers with PayPal donate buttons or 501(c)(3) organizations with PayPal donate buttons would still be afforded protection under privacy services, and there are many similar reasons that the working group found and ultimately, I think found quite compelling, to not provide a distinction there on the commercial services question. Thank you.

ALICE MUNYUA: Thank you very much. If GAC colleagues have questions or comments? Indonesia.

INDONESIA: Can I ask a question from your explanation there where you mentioned that if an operator discloses information to the law enforcement agency which is not in line with the bylaws or regulation internally, that will affect their accreditation, something like that.

Now, my question is: What is the effect of this accreditation for that local organizations? Will -- will it -- say will it reduce -- because of that, the accreditation is going -- is ranked down, will it be affected for their operation daily or something like that? What is the effect of this -- that accreditation? Thank you.

STEVE METALITZ: Yes. Thank you for that question.

Let me just clarify something. This is not really -- this doesn't go directly to the issue of whether the service provider would respond to the law enforcement organization by providing the information. This question of the confidentiality is whether they tell their customer that this request has been made. That's, I think, the issue that we're focusing on here.

So I just wanted to clarify that.

I think the whole idea of having accreditation of these providers is that once the accreditation framework is in place and has been implemented, then registrars will only be able to deal with those providers who are accredited and they won't be able to accept proxy registrations or privacy registrations from unaccredited providers.

So in the case --

For example, if there were a local law in place that said that these requests from law enforcement have to be held in confidence and a provider systematically abused that and did -- and did disclose to the customer when the law said they shouldn't, that could be the basis for removing the accreditation of the service provider.

And if that were to occur, then all the accredited registrars could no longer accept registration -- proxy registrations from that service provider.

I know this is a bit complicated because we have two -- we will, once this is in place, have two accreditation systems, one for registrars that we've had for many years within ICANN, and the other for these service providers. Graeme?

GRAEME BUNTON: Thank you. I think what I hear your question getting at is what happens during a de-accreditation of a privacy service provider and the domain names that were previously protected.

And there is no immediate answer to that, and I think what your question highlights is the complexity that's going to be involved in the implementation of this -- of the output of this PDP, and it's another good reason why we need to move forward on this as quickly as we can because it's going to be a lengthy,

complicated process that requires serious careful thought to address concerns like that. Thank you.

ALICE MUNYUA: Thank you. European Commission?

EUROPEAN COMMISSION: Thank you, Alice.

I just want to briefly react to two of the points that have come up.

First of all, the rule on disclosure, where you rightly say that of course this doesn't prevent the situation where national laws already oblige keeping such requests confident, as do any other rules that we adopt here, because as I said before, we do not impact on the national legal frameworks for any of these rules.

But what you are creating, in essence, is a new default, and while you say that there is a possibility, of course, for registrars and proxy/privacy services to adopt stricter rules, you will be creating the default and any work that proxy/privacy services are willing to do to accommodate law enforcement requests would be additional work that is not laid down in these rules.

I think we have to come back to what we are looking at here. It is basically specific law enforcement requests in individual

criminal investigations asking for information that for other services is already, by default, public, so it is not particularly sensitive information.

But on the other hand, the fact that such requests would automatically be forwarded to the user making use of these proxy/privacy services would endanger the criminal investigation in almost all of the cases.

So by creating this default, you are negating the possibility for law enforcement to use these requests as a useful tool for their investigations and I think that is a very important point to consider.

I also do not see that the current rules in the registration -- in the registry accreditation -- registrar accreditation agreement of 2013 would in any way pose an obstacle to the types of rules that we are suggesting you put in place here because they deal with the default situation of the public WHOIS. They do not have any specific requirements for this situation. And they also do not prevent us from adopting rules that are appropriate for the specific case that we are dealing with here.

And I want to remind everybody again that this is a very specific case. We're not dealing with general access by just anybody to the type of information that is held by proxy/privacy services but by accredited, authorized law enforcement agencies who are

making these requests in individual criminal investigations, and we're also not talking about mass surveillance, and I think that point needs to be remembered in this discussion.

So on those two points, I really do not see that there is any legal obstacle to accommodating the requests that the public safety working group is proposing for the GAC to make.

Thank you.

STEVE METALITZ: Thank you very much for that comment.

Yes, I would agree with you that these rules that are proposed in the recommendations of the working group do not require the service providers to maintain confidentiality where that's not a requirement of the applicable law. Where it is, they are required to, and you're absolutely right, we can't change that law or affect it.

I think the effect of that would be that if they violate that law, they can also lose their accreditation, which is, you know, commercially valuable to them, presumably. So that is certainly some incentive to do it.

And I think -- if I heard you correctly, I don't think we're providing organizations with an incentive to violate

confidentiality in a case where there is no legal requirement for them to maintain confidentiality. I think what's spelled out in the report is actually the opposite, which is that there's some encouragement for them to do that when they receive that request. But you are right, that's not a requirement in the rules as they come out from this working group.

On the jurisdictional question, I would just say that I don't -- I think you're correct. It's not a legal impediment. I -- we viewed it as a practical impediment. That this is where the issue came to rest in the RAA discussion, and it is a difficult question as to, as you referred to, an accredited law enforcement request from outside the jurisdiction, and my sense is -- there are obviously a lot of people in this room that are far more knowledgeable about this than I am, but my sense is that that label can be very difficult to apply in some cases, and when a service provider in Jurisdiction X receives what appears to be a law enforcement request from Jurisdiction Y, it's not always clear on its face that this is from any type of accredited law enforcement provider. So -- law enforcement agency.

So that's a bigger question which I think does need a resolution. The working group just felt it was beyond its practical capabilities to achieve that resolution, and that's why we, in effect, defaulted to what is already in the RAA.

GRAEME BUNTON: Thanks, Steve. Yeah, I think that's an interesting point, that solving the jurisdiction issue is a very big question. It's an interesting opportunity for the community to look at how to do so, but that needs to be in a -- in a larger forum than this particular working group.

And I do think, on the disclosure piece, that we worked quite hard for quite a long time to try and balance civil society interests, business interests, and intellectual property interests, and as mentioned, there was perhaps not enough law enforcement involvement in the working group to really balance those interests as well, but I do think there was a reasonable job done there, and so I'll -- your concerns are interesting and we can take those on board.

ALICE MUNYUA: Thank you. Spain?

SPAIN: Sorry. From what I'm hearing, correct me if I'm wrong, but I see little room and, above all, little will to take GAC concerns into account and do something during the implementation phase to address them properly.

So I would like to ask you: What are the reasons the GAC should have to give its approval to the report by the working group and leave -- and trust that our GAC concerns can be dealt with in the implementation phase?

I would like to hear the reasons that you would present to us to endorse the recommendation as it is and trust that our concerns that are very legitimate can be addressed in a future stage.

I would like to remind that the hurdles law enforcement authorities find in implementing and overseeing the enforcement of laws results many times in Internet fragmentation, because sometimes we have to regard to blocking because we are not able to trace back the person responsible for -- to determine -- for certain content, and in the end, we have to take recourse through those kinds of measures, which are very undesirable but we are left with no other recourse. Okay.

GRAEME BUNTON: Thank you for the question.

This is Graeme, for the transcript.

I think one of the reasons that we should move forward, as has been mentioned already, and that's that the interim spec expires at the end of this year, and so as of Jan 1, 2017, there will

be no rules for privacy and proxy service providers, and so that should serve as reasonable impetus to make sure that we're moving forward with some sort of process to make sure we have some rules in the immediate future.

STEVE METALITZ: Yeah. This is Steve Metalitz.

If I could just build on that. I think, yeah, it was mentioned by several of the previous speakers from the GAC in the earlier session.

The current environment is not really sustainable. It's a completely unregulated, if you will, environment, and now I like to say that if .PROXY were its own generic top-level domain, it would be the second largest in the world. It's about one-fifth of all registrations. Literally tens of millions. And there really aren't any rules that apply to when -- you know, to who can use it, to when it would -- what are the procedures for finding out this information when it's needed, for example, as you reference in the intellectual property area, as well as others.

So I think the justification, if you will, for moving this process -- for the GAC to allow the process to move forward is to try to take at least a first step in bringing a certain degree of order and

predictability and consistency to what is currently an unpredictable and inconsistent environment.

And the path that ICANN has chosen to try to do this is through an accreditation process. And this would set at least the basic -- the basic rules for that.

Thank you.

ALICE MUNYUA: Thank you.

Any other questions or comments?

Okay. If there are no comments, I thank GAC chair for way forward.

CHAIR SCHNEIDER: Thank you. First of all, thank you, in particular the two of you, also for coming here. We see how important this exchange is that people can ask questions, that you understand where these questions come from. You can explain your rationale, not just in paper but orally to people, which is very helpful for us in turn, and I think we have to continue, as you say, this dialogue and be much more present.

The only problem from the government side is that we normally get more tasks but less resources to do this, which is something

we're learning to cope with. But I think that the will is definitely there to build on this interaction, which is extremely helpful, I think, for both sides and should foster all together coming up with solutions that are progresses rather than steps backwards. And I think this is a good example of, I think, we have achieved or we will achieve a lot of progress. And let's hope that during the implementation, we will get to a point where we get the best out of it that is a good balance for all concerns involved. So I would really like to thank you very much for coming here. And also, those board members who have listening carefully, not saying anything but listening carefully, of course I think that's been noted.

And we have some time for one more comment from you or from anybody else, if you wish.

STEVE METALITZ: Thank you very much, Mr. Chairman. I would just thank you again for this opportunity. I endorse everything that you said. And I think, again, in response to the last question, there's a trust component but there's also a participation component. We need the input from the law enforcement community to do a better job on implementation.

So I hope that when -- if this moves forward and when the IRT, the Implementation Review Team, is set up, that there will be a way to have active participation from law enforcement.

Thank you.

CHAIR SCHNEIDER: We'll try to make sure that you will get one person per all of the 168 countries of the GAC to participate in your work.

No. Thank you. I think this request is noted or invitation is noted, and we hope -- we'll do all our best to be present in this.

So thank you very much. So we close this session for now and can actually move on to the next one.

[END OF TRANSCRIPTION]