ICANN75 | AGM – RSSAC Caucus Meeting
Tuesday, September 20, 2022 – 13:15 to 14:30 KUL

OZAN SAHIN:

Hello and welcome to the RSSAC Caucus Meeting. My name is Ozan Sahin, and I will be the remote participation manager for the session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior.

During this session, questions or comments submitted in chat will only be read aloud if put in the proper form, as noted in the chat. I will read questions and comments aloud during the time set by the chair or moderator of the session.

If you would like to ask your question or make your comments verbally, please raise your hand. When called upon, kindly unmute your microphone and take the floor. Please state your name for the record and speak clearly at a reasonable pace. Mute your microphone when you're done speaking.

This session includes automated real-time transcription. Please note that this transcript is not official or authoritative. To read the real-time transcription, click on the Closed Caption button in the Zoom toolbar.

To ensure transparency of participation in the ICANN Org multistakeholder model, we ask that you sign into Zoom sessions

using your full name. For example, the first name and last name or surname. You may be removed from the session if you do not sign in using your full name.

With that, I will hand the floor over to Ken Renard.

KEN RENARD: Thank you, Ozan. Welcome to the Caucus meeting. There's only a few of us here in the room now, so online folks please feel free to speak up and ask questions and participate. So we have an interesting agenda here, and we'll take a look at that now and ask if anyone has any updates to the agenda. We're going to talk about the Caucus engagement. There are some interesting results there, as well as the work parties.

I don't see Brad here to see about getting a GPG update. We'll see if he can join us. And then we'll go on to AOB. Is there anybody that has any suggestions or additions or changes to the agenda? All right. Hearing none, we'll go ahead with the Caucus engagement information, and that's to Jeff Osborn.

JEFF OSBORN: Thanks very much. We have done the annual Caucus Membership Survey, and the data is available here. We've put together a couple of slides. There's no shocking information, but it's all fairly interesting. The geographic distribution of the membership is

nearly fully half out of North America and about another third Asian Pacific. And those are not surprising numbers. Next slide.

We've gotten good responses. This is about what we expected. There are currently 110 members. So 35 out of that, I felt, was … It's a good number. It's an improvement over last year, in fact. Next.

Not surprising, given COVID, we've had a reduced number of live participation in Caucus meetings. I was kind of surprised that we did so well in 2021, but it's a trend you would sort of expect. Next.

It seems like the frequency is acceptable. I thought it was interesting, though, that as you pass through the years more and more people wanted to meet more frequently. I think having been cramped up with my own lovely family for a whole year, that's probably a matter of cabin fever as much as anything. I don't think this is any compelling call, though, that we need to change the frequency of the Caucus meetings. Next slide.

Similarly, I think the current venue seems to be the most popular choice. And again, I can only think that people wanting to add places that we meet has to do with the desire to sort of get out and meet face to face again. Though, nothing compelling. Next slide.

Participation in work party. There's a slight drop and I don't know whether it's statistically significant, but we did say for 2022 that

lack of participation in a work party was no longer grounds for questioning whether you wanted to be a part of the Caucus and sort of being asked to either attend more frequently or not be a member. We've extended that through …

What did we say about next year? We had a policy previously where we really tried to keep track of how much attendance and participation members had, and we suspended that for the existence of COVID. I don't remember exactly when that ends, but it's at least through the remainder of 2022. And I think it's been a reasonable policy and we haven't had a big fall off in participation, so I'm not concerned. Hopefully, this is all over by next summer, knock on wood. Next slide.

Contributions to the work party. This isn't a big surprise, either. I think most people participate in discussions. The text review section was larger than I expected, and seeing it increasing to nearly 90% seems very strong.

This, I thought there's one interesting piece where somehow it became less easy and more neutral to contribute to the to the working group and its product. And again, I'm not sure how much this has to do with COVID, but it's data so we're presenting it. Next.

This is always a nice wrap up. This looks like a Soviet election result. Basically, nobody wants to leave which I think is sort of a ringing endorsement that things are gone well.

So just to review real quickly. The Caucus questionnaire, we do a fair amount of thinking about it and deciding whether we want to change pieces of it. Everybody here took part in it. The quality of the longitudinal data, I think, is best if we don't change it much. So we're probably going to not really change much again. I think it will be interesting next year to see whether the ability to meet in public changes any of the numbers, but I don't feel like there's any call to action in this data that says we need to change something in a dramatic way. If somebody disagrees, please, please let me know.

Any questions or commentary? Ah, the freeform text. Now this I thought was amazing. This first one … Somebody should feel very proud of themselves for what they're doing because … I'm going to read this out loud.

"The RSSAC Caucus is one of the most welcoming environments among communities in the ICANN space." I just thought that was really a very positive piece of feedback, and it speaks very well to the workgroup leaders and ICANN staff who make this a nice environment in which to work.

The second comment I also thought was interesting where self-nomination is a valuable thing, but setting an entry bar might be an interesting thing to do. This comes up in the membership committee discussions all of the time where we would love to have new involvement, but we got applications from people who really have basically no DNS experience whatsoever. And we usually send them back to look at the requirements list.

So I don't know how much this actively matters. We don't have that many work party leadership positions. But again, this is the open forum feedback, which is often the most interesting part of the surveys. Next page.

These are all interesting. You can all read, so I'll leave that there. The first one of those, we're actually actively talking about ... There are a few people who were talking about trying to fund a tool that would allow you to track what the root server latency was from sort of anywhere in the world, maybe on an iOS platform or something like that. And that's an ongoing discussion this week. If that ends up coming to fruition, we'll talk about it more.

And that's it. Thank you for your time. And thanks for the great work product, Ozan, always.

KEN RENARD: All right. Thanks, Jeff. Next is on to the current work parties and work products, and I think Duane might be up next. Yes, Duane. On to RSSAC001.

DUANE WESSELS: All right, do you have a next slide that's specific to RSSAC001? Okay. This is probably not really news to anybody because a lot of the same people were just in the room. We had a meeting on RSSAC001 Version 2 prior to lunch. So that was our first sort of real meeting of the work party.

And in case someone is not familiar with this, RSSAC001 is a document that describes service expectations for root server operators. It's an old document. It's been seven years, and so it really needs some attention with respect to its currency. We are looking at changing the phrasing of the language of "expectation" versus "requirements." We're looking at changing maybe some of the specific expectations, or adding some or deleting some. And already there's a good amount of comments in the Draft Version 2 document.

Still TBD is the extent to which we would need to update the companion RFC. That's likely to be a topic for our next meeting which will be in the timeframe of two weeks from now. And that's where we are with that work party.

KEN RENARD:	All right. Thanks, Duane. The next work party, I think Andrew is going to discuss. And that's RSSAC002 updates.
ANDREW MCCONOCHIE:	Yeah. My name is Andrew McConaughy. I work for ICANN support staff. Ray Bellis is the work party leader for the RSSAC002v5 work party, but this is a really bad time for him time zone wise.
	Do we have this slide for the RSSAC002v5 as well? If not, that's fine.
[OZAN SAHIN]:	We don't. No.
ANDREW MCCONACHIE:	Okay, that's cool. So this document is obviously an update from v4. If you're not familiar with RSSAC002, it's the metrics measurements that the root server operators collect and then publish. And this work party, to update it to v5 has really just gotten going. I think we've only had three meetings.
	Our meeting yesterday, we made some kind of preliminary decisions. There's nothing really set in stone yet. There was some discussion about whether or not label count would go into RSSAC002v5. It's looking like there's a weak consensus to not include label count, but that's still ... I think that discussion is still

ongoing. The work party will also ... It decided that it will be meeting every two weeks, so the next meeting of that work party would be in, I guess, two weeks from now.

And another thing is, there a couple Caucus members—Anupam and Abdulkarim—who are going to be looking at the existing metrics in v4 and seeing if those require any updating. Just giving a kind of Holistic Review of the metrics in v4 and seeing if there's anything that might need to change for V5.

So we're just getting going there. And if that interests you, I encourage you to join the work party.

KEN RENARD: Thanks, Andrew. Next one, which is not actually a work party yet, I will talk about cyber incident oversight and disclosure. Go to the next slide.

So just a little bit of background. RSSAC058 was the success criteria for a governance structure, and it states that ... You can read that. So an important note that RSOs have been doing incident disclosure or incident response since inception. So this is not something that's missing. It's really a matter of formalizing the process as the RSS governance becomes formalized as well.

So this kind of stems back to NIS 2 that proposed some incident reporting requirements. At the time we speculated that NIS 2

would not be the last. It was not the last. And this is a way of maybe us getting out ahead of the game and trying to define NIS ourselves. Next slide, please.

Again, this is a potential work party. The work right now within the RSSAC is to try to develop a Statement of Work. And the scoping of that work is probably the biggest challenge there. There is no deadline. In fact, there's really no obligation to pursue the …

The purpose of this work party would be to provide a recommendation or some document to the RSS governance structure to say, "This is what we think the cyber incident oversight and disclosure could look like." There's no guarantee that the governance structure would take that up. It's just a recommendation to that structure.

We've done stuff like that in the past with other things like metrics, like defining a rogue operator, things like that. So it's just kind of getting a little bit ahead of the game and providing input to that body for them to consider.

Some of the issues with this. RSOs are independent and autonomous. With cyber incident disclosure, each organization is going to have their own policies with that. The current set of questions there, you can see those. What role should the governance structure have in this oversight as maybe an

aggregation point or as a central point for regulators, governments, any interested party to go to see information about cyber incident disclosure?

But this is going to be a difficult, complex issue to tackle, and transparency, autonomy, security are all things that need to be very carefully balanced.

I see, Fred, that you have your hand up. Go ahead.

FRED BAKER: Well, I'm thinking about the conversation we had with the government [access] people—Elena Plexida and Jamie—I forget his last name. This would interact with that conversation. Would it not?

KEN RENARD: Yeah. And they seem to think that this type of work would be very valuable. It may answer questions that regulators might have. It might help them understand certainly what's there rather than opening without something, an incident disclosure mechanism in place. They may open-ended to try to regulate more than they should or more than is in our scope. So having this in place, they seem to think could alleviate a lot of concerns from some of these parties that might try to regulate. Thanks, Fred.

FRED BAKER: Okay. Would it be worthwhile asking them what is the minimum profile of this that they would hope for?

KEN RENARD: Liman.

LARS-JOHAN LIMAN: Lars Liman from Netnod here. Fred, I fear that out of 200 various people giving opinions on that, we will get roughly 800 opinions. So while I have thoughts in that direction as well, I kind of put a cap on myself and say that I'm not sure that's a good idea.

But that said, I understand where you're coming from and we probably need to find some way to deal with that problem. Thanks.

KEN RENARD: Jeff.

JEFF OSBORN: Jeff Osborn, ISC. I can't imagine we wouldn't prefer to be the ones proposing what we report rather than waiting to be told what to support. Because we can get asked for squirrels per hour or furlongs per fortnight if we let somebody else choose.

KEN RENARD: Right. And that's one of the motivations behind this, is to kind of get out in front. And this is what we think ... It's not just that this is what we're willing to disclose, but what's the right things to disclose. Liman?

LARS-JOHAN LIMAN: And that gives us a chance to give a motivation for why we choose to publish the various types of data we publish so that we give an underpinning. Whereas if we only get [inaudible] requests for data, it may not always be the case that it has a sound underpinning. Thanks.

KEN RENARD: Robert.

ROB CAROLINA: Rob Carolina, IOC. Since the subject has come up, I thought I would just make the observation that in terms of what types of things would be included within disclosure obligations, personally my suggested framework for thinking about this is what does the emerging body of regulations around the world that are addressed to the security of critical national infrastructure, what sorts of things are regulators asking for routinely?

ICANN|75
KUALA LUMPUR

So if NIS 2 had been applied to us, we know what sorts of information they were asking for. There's a whole body of regulations coming out of different aspects in the U.S. federal system in different vertical regulated segments about what types of information they're asking for. If you just substitute, as a framework, the Root Server System governance structure and assume that it is trying to fulfill the role of what those regulators are doing, then I would start with that as a framework and then figure what makes sense to include and what makes sense to exclude from that.

Because ultimately, the success of the system will be whether or not the Root Server System governance structure is able to fulfill the function of persuading the various regulators around the world that they are fulfilling the function that we don't want the states to intervene in. If I'm making any sense. I apologize.

KEN RENARD: That makes sense to me. I guess listening to politicians and—oh. Just joking. Yeah, I think looking at this from sort of both angles, what would those regulators want to see? And I think, based on what we got from the Government Engagement Team was, if you sum it up, they're asking us to tell them when to worry. When should they hit a big red button?

I imagine there's other political motivations underneath there, but then from the bottom up I'm thinking this is a security person. What types of things should people care about—data integrity, data availability? But that's applying logic to the problem, and may not be the best ... Somewhere in the middle between those two approaches. My thoughts.

ROB CAROLINA: Just to follow up on that. I agree with that completely. I think that the trick then becomes to tell those kinds of things to whatever the Root Server System governance structure becomes because we're hoping to build a two-stage system where we're dumping more information on our own ... I don't usually want to use the word "regulator," but building a governance structure is kind of like building a regulatory system.

So we're trying to figure out what would that regulator want to know. And the people in this room and the people in the Caucus are the kinds of people most likely to be able to come up with that.

KEN RENARD: All right. Well, one big DEFCON or RSSCON number. Are any other thoughts from the room, from online about any of the work parties? Come on. That's the last piece of the agenda here. This will be a very short meeting. If nothing else, we're going to put up

that comment about the welcoming environment and just display that for a while.

UNIDENTIFIED MALE: T-shirts.

KEN RENARD: Yeah, we can make T shirts. Caucus T shirts.

ERUM WELLING: Hi, Ken.

KEN RENARD: Hi, Erum. Yes, go ahead.

ERUM WELLING: Thanks. Since we have a little bit of time, for this third potential working party, is there already some kind of draft? How can we volunteer to assist you or others with the development of the Statement of Work?

KEN RENARD: So at this point, generally the Statements of Work are done inside the RSSAC, not necessarily with the Caucus. Part of me thinks that … You know, there's a lot of good discussion that's been

happening and what if we opened up just the Caucus mail list to talk about various things, throw out ideas towards this topic to collect it.

Because I think this is going to take some brainstorming and then then try and make some sense out of where this could go. And then we kind of scope out that Statement of Work, though. If you have any thoughts on the topic itself, I ask you to send it to the Caucus mail list just to keep the discussion going. And within RSSAC, we'll continue to pursue that Statement of Work and see if this goes as a work party.

ERUM WELLING: So may I continue a couple words about that?

KEN RENARD: Please.

ERUM WELLING: Thank you. So the Statement of Work would only cover what needs to be done. Right? And it would be the Caucus that would come up with suggestions as to what the framework would be or some of the ideas or answers that we can come up with to the Statement of Work. So I just want to make sure I understand that RSSAC would only be coming up with what needs to be done

because some of the discussion we just got into in this room started to define what could potentially be the answers.

And I just wanted to make sure that when the Statement of Work comes out that it's an open book. That the people in the RSSAC Caucus would be allowed to develop the framework as opposed to being given the framework?

KEN RENARD: Yes, I agree with that. The problems that we're having with scoping of the Statement of Work, I think it helps to brainstorm if you dive into some of these details and then come back and abstract all of these details that are being discussed now on the list will be brought through to input to the Caucus work party if it if it goes forward. So yeah, I definitely agree that it should still remain mostly open ended as far as the content but kind of the guardrails of what the Statement of Work. You know, stay within these bounds is what we're trying to put together.

ERUM WELLING: Thank you.

KEN RENARD: All right, I don't see any other hands. If anybody else has any closing remarks? If not, we can adjourn.

OZAN SAHIN: Thank you, all. Please stop the recording.

[END OF TRANSCRIPTION]