
DANIELLE RUTHERFORD: Welcome, everyone. Thank you for joining. This is the as the virtual RSSAC Caucus meeting held during IETF 114 on the 24th of July 2022 at 19:30 UTC. Attendance for this meeting will be taken through Zoom, and so we won't go through the full roll call.

Fred, I'll turn it over to you.

PAUL HOFFMAN: Can someone do a sound check so we know whether audio is working?

DANIELLE RUTHERFORD: Yes, Paul.

FRED BAKER: I can hear you, Paul. Can you hear me?

PAUL HOFFMAN: I can now. Thank you, Fred.

FRED BAKER: Okay, thank you.

DANIELLE RUTHERFORD: Also speaking today, we'll have Jeff Osborn and Robert Carolina. If you two would like to do a soundcheck?

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

JEFF OSBORN: Test, test. This is Jeff.

DANIELLE RUTHERFORD: Thank you, Jeff.

ROB CAROLINA: Hi. This is Rob Carolina.

DANIELLE RUTHERFORD: Beautiful. Loud and clear. And we've done soundchecks for other people. Fred, over to you.

FRED BAKER: Okay, great. So you're looking at the agenda for today. Before I dive into it, does anybody have any changes that they would like to make to the agenda?

PAUL HOFFMAN: Fred, this is Paul. It looks like Duane will not be on time. He seems to still be in the air. And so if that continues to be true, I will do the RSSAC001v2 discussion.

FRED BAKER: Okay, sounds good. Okay, we'll go ahead and use this agenda with that modification. Jeff, do you want to talk about the Caucus?

JEFF OSBORN:

Sure. Thanks, Fred. We actually have something of a multimedia presentation here, and with Ozan absent from doing his fabulous coordination, I'm hoping we get this right. We have multiple speakers for different slides. So if nobody else is going to open this, I'll go through them. But I believe starting at about the third slide, other people are supposed to step in. And I don't have the entire cast list in front of me. Next slide. There we go.

Andrew, this was yours.

ANDREW MCCONACHIE:

Yeah, I think I'm the first person stepping in here. So my name is Andrew McConachie. I work for ICANN Support Staff. Also on the call with me today is Danielle Rutherford. Ozan and Steve Sheng could not make it today. So, these are the four people that support the RSSAC and the RSSAC Caucus.

I'm based in Rotterdam in the Netherlands, and I help out a lot with some of the writing that the RSSAC and the RSSAC Caucus does. Danielle is based in California, and I believe you've already heard her voice. And Ozan is based in Izmir, Turkey. And they both help out with a lot of the administrative tasks. And they keep us on time and on schedule, and on point. And then finally, Steve Sheng is our boss. And he also helps out with the writing a fair bit. And he is based in Pittsburgh, Pennsylvania.

So back over to you, Jeff. Thanks.

JEFF OSBORN: Thanks, Andrew. Next slide. The membership date is an interesting thing for us. I'm the chairman of the Caucus Membership Committee, and we primarily deal with people who are self-nominating and apply to be members of the Caucus. Our current membership is more diverse than it has been in the past.

Historically, we had a predominance of North American and European presence. The current North American component is fully 45%, but that's down from previous years. European at 13%. We have a lot of Asian, Australian, South Asian, and Pacific membership as well at 28%. And then Africa at 8% and then Latin America at about 6%.

So this is an improving piece of data that I think looks best as a trend line rather than a pie chart, but that's what we had. Any questions on that? And I believe the next slide is ...

[KEN RENARD]: Why didn't you do it as a trend line, Jeff?

JEFF OSBORN: Because Ozan does all of the pretty stuff and when I do it, it looks like chickens walked in mud.

[KEN RENARD]: That's a pretty good excuse.

JEFF OSBORN:

It's the truth. Oh, hey, highlights. I actually get the next one, too. The Caucus membership is basically ... As I said, it's self-nominating, and people apply to it themselves. And we go through and keep track of things like the level of involvement that people have had. A couple of years ago, there was a concern that there were people who had signed up for a membership and then hadn't either attended a meeting or had any meaningful work produced.

We've gotten to a level where most of the people who are in the group are actively attending meetings, have attended workshops, and are producing helpful content. In March, though, last year, we realized that we really needed to add some leniency because the pandemic was, you know, besides just being the great excuse for everything not quite working right, it really legitimately was knocking some people out of the ability to certainly show up in person, but in other ways contribute.

So we decided to pause our monitoring activity and are sort of strictly requiring people to attend most of the meetings. And we further had decided to extend that throughout the rest of 2022. So for the time being, we are not tracking attendance and sort of getting at people and saying, "Where have you been." But, Inshallah, good God willing, by next summer maybe the pandemic won't be as big of an issue anymore. We'll see what happens. Next slide.

Ken. If Ken's not there, I can certainly wing this one. One of the other things we had intended to do as a part of the membership is try to broaden the areas of expertise that would benefit the work of the Caucus. We've tried to have a fairly deep requirement that people have had sort of hands-on DNS root server or implementation experience.

And we got a phenomenal amount of it. We got some really incredible depth from some of the applicants.

But we got some who are sort of hobbyists who, you know, maybe can configured DNS on their own machine. And they mean well, but we sort of send them back and say, “Here are some things you could do that would be that would be more helpful.” We're trying to broaden that. And instead of requiring people to have complete and deep experience across broad areas, to look for people who maybe have more depth in areas that we're not covering as well.

Certainly, the technical area we're very good at, but areas like Internet governance and actual community experience in some of the outlying areas, there are things that we're looking more broadly for experience. The Internet governance experience was actually added to the requirements in the ICANN document that specifies what it takes to become a member. Next slide.

Oh, okay. Is this coming and going or is it me? There it is. This one I've really ... It's too bad that Ozan isn't able to do it because he's very familiar with the way these processes work.

The Membership Committee has been working with the Admin Committee to identify Caucus members and recommend them for special recognition and basing it on considerations like the material contributions, leadership roles in Caucus work parties, and representative or liaison roles that people have carried out. So for 2021, we would like to recognize three members in 2021—Abdulkarim, Kazunori, and Paul. So thank you all very much, and congratulations.

KEN RENARD: Check, check. Can you hear me?

JEFF OSBORN: Yes. Hi Ken.

KEN RENARD: Sorry, my audio went out. But thanks for covering that, Jeff. Just briefly on the widening the expert areas of expertise for the Caucus, the purpose there was to increase engagement of the Caucus, especially as we move into some policy issues, things like that. So of increasing the membership breadth and trying not to scare people away by thinking you need to be an expert in these 17,000 different categories.

So the takeaway, if anyone here knows people that are interested in being a part of the root server community and Caucus and can contribute, please pass these changes on, and the Membership Committees welcomes applicants and the Caucus welcome engagement in different areas.

JEFF OSBORN: Thanks, Ken. So I guess we're two slides forward now. One more.

DANIELLE RUTHERFORD: Next step is the overview of recent RSSAC publications, and I believe Rob will be speaking to RSSAC058 and RSSAC059 first.

JEFF OSBORN: Excellent. Dr. Carolina.

ROB CAROLINA: Thank you very much. As most of you will know, RSSAC adopted RSACC058 and RSSAC059 in November of last year. And RSSAC058 presents a series of success criteria that can be used to analyze any proposal for an RSS governance structure. The success criteria are perhaps ...

I want to pause on that for a moment because if you have a chance to look at them—and I would encourage everybody to do so because this is a very current topic, given the work of so many people to try to develop the next generation of RSS governance—the success criteria should not be viewed as simple sort of binary success or failure-type criteria. Particularly the Section A criteria, substantive criteria for a for a Root Server System governance structure.

So as discussions are held and as people around the Internet community assess various proposals for a governance structure or elements of a governance structure, there are going to be a series of balances that have to be drawn. So there's probably no single governance structure out there that will produce absolutely complete compliance with every single substantive idea in the document. Instead, it's going to be like any governance structure. There's going to have to be a bit of give and take and a bit of figuring out how responsibilities and how authority is apportioned.

So of course, RSSAC058 walks through a number of criteria, whereas RSSAC059 was a very specific recommendation to the ICANN Board of Directors. In the same way that RSSAC037 has a very long description of principles and elements that need to be in a governance structure, and RSSAC038 was a recommendation, RSSAC059 is a recommendation.

And I have to assume that it was reasonably successful because less than 48 hours after the publication of RSSAC058 and RSSAC059, the ICANN Board of Directors held a special session in which they embraced the recommendations in RSSAC059 and embraced the structure put out in RSSAC058 and transmitted that to GWG for further consideration.

So that's where things stand at the moment. Happy to answer any questions.

DANIELLE RUTHERFORD: All right. I'm not seeing any questions. Thank you so much, Rob. Next up will be Anupam to speak to RSSAC047v2.

ANUPAM AGRAWAL: Yes, thank you. So RSSAC047 is an advisory document on metrics for the DNS root servers and the Root Server System. The first document was released in the year 2020. RSSAC047 initially presented a set of measurements, metrics, and thresholds for the DNS root servers. So when we say measurements, metrics, thresholds, it was about the root server operators, what they need to do to provide a minimum level of performance.

And these thresholds were essentially based on the technical metrics designed to assess the performance and availability. As an OCTO was essentially implementing the measurement system and trying to find out what are the issues and what are the cases which were not covered as part of RSSAC047 which led to this work party to create the Version 2 two of the document.

And the work party was given a very clear-cut mandate to correct whatever technical errors which could be corrected as part of this document, and also make sure that there is an additional review period of two years or three years, whatever is required.

So the work met for a period of three or four months and then it addressed the various issues and provided the clarification where it was felt that RSSAC047 is not correct or it is a little ambiguous. To that extent, there were certain sections on reporting which were modified. Section 5.3 on RSI correctness was a section which essentially was modified. And the work party also attempted to clarify the publication latency in Section 5.4 of the document.

So, overall, at the end recommendation was also added based on the charter of the work party to add a period of review which was essentially two to three years. And there was a small number of grammatical changes which was done.

And thanks to all of the members of the work party—Paul and Warren contributed. And thanks to Duane.

And just my last point that, as part of this conversation, we could also figure out what are the additional things which can be included in this

RSSAC047. But since the charter was very precise, we have not attempted to do that. But that list of things which could be looked at by the future work party is available with the staff. So it is recommended that the next set of conversation starts from what was discussed as part of v2.

Thank you. This was all I had to update.

FRED BAKER:

Okay, thank you. Now show me the agenda, please. Here we go. Okay, so now, Paul, you wanted to talk about our second one.

PAUL HOFFMAN:

Hi. Actually, Duane wanted to be speaking about it, but flights got funny. So I am stepping in for Duane here. This is a Statement of Work for potential new work for the Caucus. And basically, RSSAC001 has been around for five or six years and has not been touched since then. RSSAC001 has a bunch of service expectations on the RSOs. It has requirements and recommendations about what they are supposed to do with the service expectations, and it just hasn't been touched in a long time.

Duane and I, when we were chatting one day, notice that some of it seems a little bit out of date and we just thought, okay, maybe we should do a round of touching it to see. So if you scroll down to the scope of the proposed work, basically we're suggesting, just in the same way on Anupam talked about how we did RSSAC007v2, we're looking at doing a v2 RSSAC001. And there are a bunch of things that are potential,

and I'll go through them here with the hope that if RSSAC if RSSAC picks this up and Caucus members are interested, that various Caucus members might find one or two things on this list that they would want to help contribute to the work party.

So right now, RSSAC001v1 has a bunch of requirements and expectations on root server operators and it would be good now that it's six or seven years later and now that RSSAC037 has been out, so people have been thinking a little bit more about what are our root server operators supposed to be doing.

We should look at what RSSAC001 says and see whether any of those things are out of date, whether there are obvious new ones, and such like that. And since RSSAC001 is about a bunch of expectations, are the RSOs meeting those expectations. And if they're not, maybe that shows that the expectation is wrong. Or maybe it's something that we can nudge the RSOs on.

So no one has done, really, an evaluation of all of the expectations in RSSAC001 and said, "Is [RSO2] doing this? Is [RSO2] doing this?" So, you know, we can evaluate those. That's fairly easy to do.

And one of the things especially that nudged Duane and I was it would be good to have some clarifications on setting the expectations, recommendations, requirements. The wording in RSSAC001 sort of jumps around between "musts" and "shoulds" and "are expected" and such like that. It would be good to tighten that up and make them all parallel.

So some of that is really just wording, but some of it's also about expectations. Do we want to say “must” about certain things? And if we don't want to say “must” ... Those six of us sitting at the IETF meeting are aware—and many of the IETF active folks who aren't here—are aware that when you say “should,” “should” usually means should except for these very limited cases, and such like that.

So maybe we want to do that in RSSAC001v2 as well. And then again look if any of the service expectations should be revised. Are there new ones that should be added? Have we thought of new service expectations that should be added? And of course, should any of them be removed? So all of that, plus just normal terminology. We've now done a lexicon since RSSAC001 was out. Can we freshen it up this way?

So if this is adopted, we hope that Caucus members will find one or a few or maybe all of these things interesting and would want to contribute to the v2 document.

And then just as a note, when RSSAC001 was originally published, there was a companion document that was published by the IAB, RFC 7720, which was definitely not the same as RSSAC001. They were parallel documents. So if we do a V2 of RSSAC001, then we either want the IETF to maybe be involved or to be involved in the same way they were with V1 which was after we were pretty much done with v1, then the IETF got involved. And then we did the two things. We published the two things pretty much in parallel.

So there will be definitely some paperwork dance between us in the IETF or the IAB on this. So we hope people are interested. Are there

questions or anything that I can help answer since Duane probably is still either in the air or in a taxi?

FRED BAKER: Well, Paul, I have a question. If you want the IETF to get involved—which, of course, they're welcome to do—what group within the IETF would you kick that to? Is that DNSOP? Is that IAB? Who would that be?

PAUL HOFFMAN: I don't know. That would actually be something I would kick back [inaudible] because that would be something that would come from the RSSAC leadership, possibly through the IETF liaisons. You know, we have an IAB liaison to RSSAC. That would need to be discussed. You know, I'm not absolutely sure. I'm going to sit here and go away from the screen for a second and ... I just am looking up RFC 7720, and that was ...

FRED BAKER: IAB.

PAUL HOFFMAN: It was IAB. Thank you. So I would say the polite thing to do would be to have it be ... So we would go to the IAB. And we do have a liaison through the IAB. That certainly doesn't prevent us from asking for other help, or mentioning to folks, like you said, Fred, in DNSOPs and such that this work is going on. But I think it would be clear that the work should be happening in the RSSAC Caucus, maybe getting additional

input from outside people. I don't know. Again, that's more of a question for the RSSAC leadership, so I would kick it back to you.

FRED BAKER: Okay. Gee, thanks. Benno, you wanted to get a word in edgewise.

LARS-JOHAN LIMAN: This is actually Liman, sharing a computer with the Benno in a hotel room here. But I was one of the co-authors for the 7720 RFC, and I maintain that this is an IAB thing that should be doing through the IAB because it pertains to operations rather than to protocol specification. And I think the IAB is in a better position to give a concise statement on that thing. Now, of course, I expect the IAB to interact with the IETF community regarding this, but the statement should be from the IAB. That's my personal opinion. Thank you.

PAUL HOFFMAN: Thank you, Liman.

FRED BAKER: Okay. Thank you, Liman.

PAUL HOFFMAN: Yeah. And again, that's not something that we're gated on in order to start the work on RSSAC001v2. It is something that we need to be aware of because of the earlier interaction. But I think we have plenty of time to figure out who are the right people to work with and whether they

even care. It may be that RFC 7720 is good enough on its own and doesn't need to be updated. But we'll certainly bring it to the IAB and see if they care about it.

FRED BAKER: Okay.

PAUL HOFFMAN: Okay, I think that's it on this. So Fred, we're waiting to hear from RSSAC about whether that Statement of Work was adopted. Is that correct?

FRED BAKER: That's correct.

PAUL HOFFMAN: Okay. Great.

FRED BAKER: And we'll discuss that, I think, next Tuesday.

PAUL HOFFMAN: Very good.

FRED BAKER: Okay, so the next thing on the agenda is RSSAC2. Andrew, did you want to talk about that?

ANDREW MCCONACHIE: Yeah. Sure, Fred. Thanks. So this is about RSSAC002v5. The current version of RSSAC002 is v4, and there's a recommendation in there that the measurements that the RSS gathers should be reviewed every two years in case there are new technology developments and that kind of thing.

And RSSAC002v4 was published in 2020, I think March 2020. So it's been a little bit more than two years and there were a couple of ideas of things to add to RSSAC002. So this is a Statement of Work for updating v4 and making v5. If you could scroll down a little bit, Danielle.

And there's really just two things. Besides the standard look-at-everything-and-make-sure-that-it-still-makes-sense, there are two kinds of specific things that are called out here. One of them is a discussion about whether RSSAC002 could contain label counts—so the number of labels in DNS query that reach root servers—and whether that should become a publishable metric maybe to help in tracking the deployment of QNAME minimization or maybe to help in seeing how many prime inquiries there are. So that's one item that's going to be up for discussion in the work party.

The second item that's up for discussion in the work party is probably a bit more basic, a bit more mundane. It's just around clarifications of the load time metric. There were some RSOs. I don't remember precisely how many or how often it's reported, but there were some that were reporting load times of zeros. And it's unclear what a load time of zero means, so there will be a discussion about that. And that's really it.

And this is in the same position as what Paul just talked about. So this SOW is now stable and it will be discussed, I believe, next Tuesday at the RSSAC August meeting.

Are there any questions about that? About this Statement of Work and upcoming potential work party. It doesn't seem like it. Okay, back to you, Fred. Oh, is that [inaudible]. Did you have something to say?

UNIDENTIFIED MALE:

Yes, I was slow finding the buttons. I mean, obviously, we'll discuss this during the working group, but I'd like to reiterate my position that the RSSAC2 [inaudible] should not be used for research-type questions. They shouldn't be used for operational questions. I think the question of QNAME minimization deployment can be very easily answered by looking at DITL data.

ANDREW MCCONACHIE:

Okay, noted. Thank you.

FRED BAKER:

Okay, thank you. Is that all of the you have, then?

ANDREW MCCONACHIE:

Yes. Back over to you, Fred.

FRED BAKER:

Okay. Ken, I think it's your turn.

KEN RENARD: Thanks. Quick audio check. Can you hear me?

FRED BAKER: Yes.

KEN RENARD: All right, good. So the next topic is on cyber incident oversight and disclosure obligations. Just a frame of reference on this. The previous two work topics are ... The Statements of Work are stable and should be voted on by the RSSAC this next meeting, next week, I believe.

But this one, the Statement of Work is not stable yet. There's still some work to do on it, so this would probably fall out in another month or so. But I just wanted to bring this up and introduce the topic here to the Caucus, something that might be coming down the road soon.

So in RSSAC058, which was discussed earlier, the success criteria stated that "The RSS governance structure must include provision for cyber incident oversight and disclosure obligations, and codify security threat and vulnerability information sharing ..." And you can read that.

Note first of all that the RSOs have been doing this, albeit informally, since the inception of DNS. So this does exist. But as we formalize the governance of the Root Server System and we're formalizing the governance structure, we should formalize this piece as well.

This kind of came out of NIS 2 which proposed incident reporting requirements for DNS operators which, at least at the beginning, did include the Root Server System. And at the time, we speculated that the NIS 2 would be the first of several reporting requirements from various jurisdictions. So we saw this coming as an issue, possibly from many fronts. Next slide, please.

So going back to the broader context here, where RSSAC has published supporting documents towards Root Server System governance, including the RSSAC047, the metrics document, and the further definition of rogue operators. So these documents have sort of further defined things that were in RSSAC037 or make recommendations to the Governance Working Group or the governance structure when that's in place.

So this topic has not been discussed in depth, either by RSSAC or the Governance Working Group. But we know that some formal requirements will be defined at some point, whether it's the GWG or part of that governance structure. So we, the RSSAC Caucus, could take the opportunity now to make that recommendation, make some recommendations, make some maybe clarifying or defining what was meant or what should happen here.

So from a broad perspective, cyber incident and oversight disclosure needs to balance at least these three things: transparency ... Really to kind of establish community trust and Root Server System, we should be disclosing, "Hey, this is what's happening." Give people the confidence that the Root Server System is able to withstand the attacks that we do see, and things like that.

We need to balance that with autonomy of each RSO as well as security. You obviously don't want to disclose too much information that might be advantageous to an additional attacker. So there may be more pieces that may come into that that balance. So next slide, please.

So these are just some of the topics that we're proposing for this work party. And again, autonomy and independence of RSOs. Things that are specific to the security architecture of individual RSOs. Maybe try to define a clear boundary of what's in scope and out of scope for incident oversight disclosure. So we should be talking about things like the RSO service infrastructure. Not the HR department of the company organization.

I think Paul Hoffman put it well. I'm going to paraphrase Paul. We should be confined to things that have a material impact on the Root Server System. So if it doesn't impact the service levels, then it's generally out of scope. Defining that material impact is difficult, but I think that really sets us in the right direction.

We see the purpose of incident oversight as, again, to maybe have some lessons learned among RSOs which, again, has been ongoing for years. But things that can lead to potential architecture changes if necessary, things like that. Again, these are just ideas to kind of spur the work party and get discussion going and allow the work party to make recommendations.

So, information sharing outside of the Root Server System or outside of RSOs. What kind of things could or should be disclosed to the public? If that's definable or not, we don't know. Let's have the work party try to

figure that out. I think it was Duane who suggested maybe just having a mechanism for disclosing vulnerabilities to the public versus defining exactly what specific types of incidents could or should be disclosed.

With all of these things, the level of detail, level of granularity that would be documented by this work party is really up to what the work party thinks is appropriate. We don't have to get down into the fine details of any particular incident. It's more about defining what we think is right at the level of detail that we can define and kind of going from there. Next slide.

So part of this is maybe setting expectations for external organizations like an NIS 2. "This is how we disclose information. This is what we disclose" such that we don't end up with lots of requests for or requirements for "Thou shalt do this ... thou shalt do this" on the Root Server System and have a mechanism for creating this transparency to the Internet community.

Some other details here. Discloser. We don't want it to be onerous for the RSOs. We don't want it to be too much work for RSOs to provide tons of documentation and things like that. But obviously, sufficient information to maintain that trust and the reliability and resiliency of the Root Server System. And obviously, not leaking unnecessary information and being respectful of organizational policies.

So I believe that's the last slide on this topic. That's what is being discussed as far as the refinement of the Statement of Work. And if this continues and goes through and then is approved by the RSSAC, this would spin up another work party in the Caucus.

So if you do have any thoughts on that, on the topics or anything like that, I don't think we'd want to discuss nitty gritty details today. But if there's any broad thoughts on this, please, I invite you to discuss them now or send them via the Caucus mail list, again, in support of creating the Statement of Work.

And I see a hand from Erum.

ERUM WELLING: Hello. Can you hear me okay? Is it okay if I take the turn now?

KEN RENARD: Yes, please.

ERUM WELLING: Okay, thank you. So my question is about just working parties in general, being a new member of the Caucus. And maybe you covered this earlier and I missed it. But I'm just trying to get understanding of, if I wanted to see ... Is it like a repository of all work parties? So I can say, okay, here are the five current work parties. And it sounds like these work parties are kind of like task forces, that they perhaps might have a start date and an end date associated with them. Can you explain a little bit about how they're organized, where we can find out what is out there, and how can we sign up, and that type of stuff? Thank you very much.

KEN RENARD: Sure, Erum. Thanks for the question. So right now there is a Caucus webpage. And if anybody can find that and post it in the chat, I'd appreciate that. Right now there are no active work parties, so that list is null. We see that there are the two work parties coming up on the revisions to RSSAC001 and RSSAC002. So assuming that the RSSAC approves those work parties—and the same with the security incident disclosure—if the RSSAC approves those, a message will go out to the Caucus, “Here's the formal Statement of Work.” And schedules will be made for meetings and open that up for Caucus members to participate in the calls.

Yes, they do have start dates and usually, you know, expected end dates. Usually about a year for a work party, but it could be less for simpler work parties. So look for those announcements coming up to the Caucus list, probably after next week. Anybody else have any ...

ERUM WELLING: So, could I ask a little bit of follow-up to that, please?

KEN RENARD: Sure.

ERUM WELLING: Thank you. So, is there any way we can establish some kind of regularity on notification of these, I think, just to balance out other things that are going on? For example, can e-mails relating to the work parties be sent out on a Wednesday? Just something that we can predict instead of, “Hey, you know, I check this e-mail account once every few days and,

oh, I missed it three days ago.” So if there's some kind of rhythm we can get familiar with, it would really be helpful. Just a suggestion. Thank you very much.

KEN RENARD:

Yeah, the traffic on work parties in general is to the Caucus mail list, not to a specific mail list for a work party itself anymore. That way we can keep all Caucus members involved and abreast of what's happening. In theory, a work party starts up and people join the work party. But the reality is, people can join at any time and hopefully contribute a good bit to the working documents.

Paul.

ERUM WELLING:

Thank you. That answers it. Thank you.

KEN RENARD:

Thanks. Paul.

PAUL MUCHENE:

Thank you, Ken. So I just wanted some clarity on perhaps the target for this work party. Is the outcome of that party going to target the RSS or the RSOs? Just a clarity on the distinction.

KEN RENARD:

For the disclosure? Security incident and disclosure?

PAUL MUCHENE: Yes.

KEN RENARD: So, the target audience would really be either the Governance Working Group or the governance structure when it's implemented, as these are recommendations of what the RSSAC Caucus or Root Server System community thinks security incident disclosure should look like. We, as the Caucus, have no real authority over strictly defining what it is, but this document would really be intended for that governance structure as input to their thought processes.

In a sense, you could think of it as we are maybe doing some of the legwork in defining this or saying this is what it should be for that governance structure. Or just, "We are providing our thoughts as of now. This is what we think. Take this and use this however you see fit."

PAUL MUCHENE: Okay. Thank you.

KEN RENARD: Paul.

PAUL HOFFMAN: Hi. So to follow up on your response, Ken, and to go back to what I was talking about a little bit ago about RSSAC001, there are in fact some security disclosure discussions in the current version of RSSAC001. It is

one of the places where it is weak in my mind, and I think purposely so, because of the issue of leaking information.

But I would prefer that if RSSAC does do RSSAC001v2, that it not get too tied up into this discussion if we are also going to be having this discussion in parallel. Because I think that this discussion could take much longer than a year, especially when we get other security experts involved. But I think that it will inform RSSAC001v2, possibly to take out any discussion of the security implications and then put it in a v3, for example, once this is all finished. But like I say, it does in fact impact the RSSAC001v2 work because it's already part of RSSAC001v1. Thank you.

KEN RENARD:

Okay. So maybe the outcome, assuming that both of those work are kicked off, the changes to RSSAC001v2 could be a, "Look. Referenced this other document for further information." Okay, thanks. Thanks, Paul.

That's all I had on the topic of the cyber incident and disclosure. Thanks for the input, everyone. Back to you, Fred.

FRED BAKER:

Okay, thank you. Did Brad file any slides?

DANIELLE RUTHERFORD:

He did not.

FRED BAKER:

He did not. Okay. Well, what I think he wanted to talk about was the current discussions that are going on in the GWG, which there a recent change to the GWG. Originally, the charter that came from the ICANN Board said that there would be three RSPs represented on it. And since the RSOs don't speak for each other, there were problems there.

So basically, we have changed the charter of the GWG to include a representative from each of the RSOs. That happened, what, a month ago? Something like that. And what we've been discussing since then is basically RSSAC058. How do we understand that? How do we interpret that? Is there anything obvious that we should change in the way the GWG works or in the things that it has produced? And I'm not sure that we have any particular changes that we want to make, but there's that conversation going on.

So we have 12 RSOs on this call. Does anybody want to add to what I've just said? Hearing nothing. Oh, Erum, go ahead.

ERUM WELLING:

Sorry to raise my hand again. Just a quick question. So in regards to the documents that were covered earlier by Robert Carolina, RSSAC058 and RSSAC059. Since they're not directly part of some working party, how can the RSSAC Caucus provide input? Or is appropriate for them to provide input? Thank you.

RED BAKER:

Well, I think if you have comments on the documents, putting that on the SSAC Caucus list would be appropriate. And, I don't know, we might

go back and update the document if that consensus develops. But right now they're considered pretty much final.

Ken, did you want to respond to that?

KEN RENARD:

Thanks, Fred. This is on something else for the Caucus with respect to the GWG. The GWG decided to open their sessions to observers. I don't know the proper channel for requesting that access. I don't know if anybody any of the ICANN staff might be able to weigh in on that. But also, the GWG met for the first time in person since it started right at the beginning of the pandemic, at ICANN74, and there were some good sessions there. And I think we've kind of shifted gears and we're really kind of ramping up and going to make a lot of progress here in the near term. Thanks.

FRED BAKER:

Okay. I think the obvious way to go about if people want to join the GWG Call would be to contact Carlos Reyes. I'll put his e-mail address in the chat. So if you want to listen in on a GWG call, please contact Carlos. Now understand that in that context, you're a fly on the wall. If you have a comment to make, it would probably be worthwhile to have a chat session with the chair, which is Brad Verd, about whatever you want to talk about.

So with that, I think we've pretty much covered the GWG, or at least the recent conversations of the GWG. Let me move on to AOB. We have a

meeting coming up in September. Okay. Thank you, Danielle. We have a meeting coming up in Kuala Lumpur. You're welcome to go there.

Now, a comment on that meeting and this from the SO/AC call the other day. If you were in The Hague or if you followed the conversations about the Hague, you heard an awful lot about health and safety. They will be following essentially the same set of guidelines in Kuala Lumpur that they were following in The Hague, and they have the force of law behind that.

When you're out on the street, you're supposed to wear your mask. And it'll be hot and humid. And sorry, but you get to wear a mask in that because Malaysian government has said that it is so. So be prepared for health and safety concerns.

Abdulkarim, did you want to get a word in?

ABDULKARIM OLOYEDE: Yes. Well, it's not on this topic. It's probably on something else I just wanted to find out. Can I go now?

FRED BAKER: Go ahead. What's your question?

ABDULKARIM OLOYEDE: Okay. I just wanted to find out why is the RSSAC not participating in the EPDP on IDNs?

FRED BAKER: I'm sorry.

ABDULKARIM OLOYEDE: I said I wanted to find out why is the RSSAC not participating formally in the EPDP on IDN?

FRED BAKER: Well, I'm not sure we have an awful lot to say about that topic. We distribute the information that is in the root zone as delivered from the IANA. And if the IDNs are included in that, and some of them are, then obviously that will be among the things that we deliver. But RSSAC has not found anything in that particular EPDP that it wants to comment on.

So, are you saying that you would like to have RSSAC commentary on the EPDP?

ABDULKARIM OLOYEDE: Yeah, I think so because I think, in the sense of the RZ, I think there are some things that would probably ... RSSAC will probably be in the best position to answer some of these questions. Especially, I believe some of these technical questions that have to do with the root zone. And I'm thinking ... I really don't know why, so that's why I'm asking why it was decided that RSSAC was not going to participate formally.

FRED BAKER: Well, right now the RSSAC doesn't intend to participate formally. Maybe you could ask the chair of the EPDP to send a note to me and we can discuss that in the RSSAC.

ABDULKARIM OLOYEDE: Okay, thank you.

FRED BAKER: Okay. Now, do we have any other comments? Any other things that people would like to address? Failing that, I think we're at the close of the agenda and the close of the meeting, so I'll adjourn us.

[END OF TRANSCRIPTION]