FRED BAKER: Okay. Good morning, good evening, wherever you are.

Ozan, I don't know if you've seen your e-mail, but Andrew would like to add an AOB item. I suppose we start out with the roll call. Okay. Oh, these are in alphabetical order, okay.

Cogent? Is Paul or Brad here? Brad Belanger? I guess not.

DISA? Kevin or Ryan?

ICANN?

MATT LARSON: Matt Larson is here.

FRED BAKER: Okay.

TERRY MANDERSON: Terry Manderson is here.

FRED BAKER: Thank you. ISC? I'm here and I believe Jeff is.

JEFF OSBORN: Jeff is here.

FRED BAKER: Okay. NASA? Keith or Tom? Okay.

Netnod? Liman, I know you're here.

LARS-JOHAN LIMAN: Yes, I'm here. I don't expect Patrick to be here.

FRED BAKER: Okay. RIPE? Kaveh or Ram? Okay.

UMD? Karl or Gerry?

KARL REUSS: Karl is here.

FRED BAKER: USC? ARL?

HOWARD KASH: Howard is here.

FRED BAKER: WIDE? Hiro, you're here, right?

HIRO HOTTA: Yes. Hiro is here. Thank you.

FRED BAKER: Okay. So, 1, 2, 3, 4, 5, 6, 7, 8.

HIRO HOTTA: And Paul is here as well.

FRED BAKER: Oh, good morning or evening.

UNIDENTIFIED MALE: You skipped Verisign.

FRED BAKER: I’m sorry. Verisign.

BRAD VERD: Brad’s here.

MATT WEINBERG: Matt Weinberg as well.

FRED BAKER: Okay. Cool. Kaveh, you’re here as the liaison of the Board as well and, Liman, you’re here as liaison to the CSC. Brad is here for the RZERC. Russ is on the phone from SSAC.

Daniel sent apologies.

IANA Functions Operator?

NAELA SARRAS: Naela is here.

FRED BAKER: Root Zone Maintainer?

DUANE WESSELS: Duane is here.

FRED BAKER: Okay. And we're ably supported by staff. Okay. I guess that's [all]. Agenda – you're looking at it.

TOM MIGLIN: Hey, Fred. I apologize for being late. This is Tom Miglin from NASA. I'm on.

FRED BAKER: Hi there. Okay. But I'll read the agenda since Russ is on the phone. So what we've got is a little administrivia, approving the minutes, Caucus Committee update, and then a discussion of supported traveler funding for ICANN66 and the future. Or no, that's actually for IETF, I believe, and the future. We're going to talk about an edit to the ICANN Bylaws supporting the direction we're talking about going. Terry asked to talk about the impact of RPKI, to talk a little bit about the workshop – Ozan, I'll ask you to do it. We have work items from two work parties and then a number of reports from the Chairs, from the Board, from the CSC, from RZERC, RSSAC, IAB, IANA, and the RZM.

AOB, we have the next meeting and we have an e-mail that came to ask RSSAC from David [Song] and Andrew would like to know what we want staff to do with that. Do we have any changes to the agenda?

ANDREW MCCONACHIE: Fred, this is Andrew. My AOB item is actually for the admin call but I can definitely discuss it on this call if you want. But if we ran out of time, please skip me.

FRED BAKER: Okay, that'll be fine. Then we'll un-AOB that I guess. So, Ozan, do you want to go into the administrivia?

OZAN SAHIN: Thank you, Fred. And hi, everyone, this is Ozan for the record. Three weeks ago on the 11th of July, I circulated the draft minutes from 26th of June meeting in Marrakech. Regarding the action items from this meeting, we have only one pending item which is sharing your [inaudible] goals with RSSAC members and this is pending because the goals haven't been shared and made public yet, so other than that, all action items have been completed. If you have any questions or comments, please direct them to support staff. Thank you. Over back to you, Fred.

FRED BAKER: Yeah. Once again I'm talking to my Mute button. Matt, do you want to talk about the caucus?

MATT LARSON: Yes.

OZAN SAHIN: Fred, sorry for interrupting, this is Ozan. The draft minutes was a voting item, so if you want to call –

FRED BAKER: Excuse me. Yes. Okay. Is anyone opposed to the current minutes? Anyone abstaining? Okay. So, I'll consider them passed or accepted or whatever that is. And now, Matt, over to you.

MATT LARSON: Thank you. Okay. So, first of all, we have two new Statements of Interest that came in. Their SOIs are included in the agenda. The first one is for Michael Casadevall. The Membership Committee did meet in advance for this. We reviewed both our recommendation is to approve both. I can talk a little bit about each.

The first one Michael, I believe, was actually at the Marrakech meeting in the audience. I know he's very involved in the DNS community and his Statement of Interest was probably the most complete Statement of Interest I have seen since I've been on the Membership Committee. So, it would seem like he would be a good recommendation to move forward.

The other candidate is with NASA. In fact, NASA can speak to him but of course we'd recommend moving forward with him as well.

So, I'm happy to entertain any questions. But the recommendation is to move forward on both candidates.

LARS-JOHAN LIMAN: Any candidate who writes his application we take is a welcome one.

FRED BAKER: Okay.

BRAD VERD: Fred, I move that we approve the candidates or I motion.

FRED BAKER: You move. Okay. Do we have a second for that?

LARS-JOHAN LIMAN: Second by Liman.

FRED BAKER: Okay. Anyone opposed? Anyone abstaining? Okay, we'll consider that approved.

MATT LARSON: Okay. There's one other thing I'd like to talk about briefly. It's something that I have discussed in the past as well. It's something that the Membership Committee is looking at, and that is looking at the entire caucus, the list of the members, and doing a review of participation from those members over the years. Carlos, you got help on this as well, I believe. I want to make sure you get proper credit whoever helped you. But the bottom line is that there was work done to look at the amount of participation from all RSSAC members dating back to 2014. The way that they broke it up is they classified people who've gone to RSSAC meetings, who participated in work parties, who participated in publications, and then we basically summated the total of participation for everyone in the caucus.

As a reminder, right now there's currently 88 caucus members. Out of that, there are 14 caucus members who've never done anything, never attended a meeting, participated in the publication, been on the call, nothing. And there's another 19 members who've only done one single thing in those three categories. So, approximately one-third of the caucus has basically never done anything.

So, what we want to do is – I wanted to have it done for this meeting and I apologize for not having it already but hopefully in time for the next meeting – really I'd like to in advance send out basically a draft of e-mails that we want to send to caucus members who've not participated, to confirm whether they (1) are still interested and (2) if they are interested, the expectation is that they participate. So, there'll be more information about that and I'm happy to take any questions about the approach as well.

Okay. Well, there'll be more information coming here but the idea here is really to once and for all do a little spring cleaning on the caucus list. I know for a fact that some of the people on the caucus no longer work for the organizations that they originally applied with or are no longer involved in the community. So we just need to do some cleaning up of some kind.

BRAD VERD: Matt, this is Brad. Is the Membership Committee going to make a recommendation for how to move forward?

MATT LARSON: Yes. The Membership Committee will make a recommendation which will probably be discussed in the forthcoming year. Once the RSSAC At-Large agrees with the approach then we'll actually take action. We will not take any action until we get agreement amongst the RSSAC.

BRAD VERD: Great. Thank you.

MATT LARSON: But this is coming.

FRED BAKER: Okay. And I think it's timely. I feel a little bit embarrassed, frankly, when we say we have over 100 members of our caucus and then I go to a work party meeting – Liman knows this well – and nobody shows up or only the Chair of the thing, so I think it'd be nice to get it done to people that are actually willing to work. So, does that complete the membership review?

MATT LARSON: Yes, it does. Thank you.

FRED BAKER: Okay, Steve, do you want to talk about funding guidelines?

STEVE SHENG: Sure. Thank you. The RSSAC caucus has funding slots for the even member IETF meetings where there's an RSSAC caucus meeting. In the past, what we've done is a first come, first served and a lottery process where people just indicate they're interested and then if we have more people than the number of allotted slots, we do a lottery. This has generated some criticism. One is it's unclear whether the funded members actually participate in the RSSAC caucus activities. And the second, there seems to be a desire for a priority in terms of funding. So, with that as a background, staff in working with the Admin Committee developed/proposed some kind of funding guidelines for IETF travel.

Very high-level, the purpose of providing the fund is for the RSSAC caucus members to participate in caucus-related discussions, meetings, working groups, as well as root server system and DNS-related protocol development activities at IETF. We're proposing three priorities. Priority one goes to RSSAC co-Chairs and caucus work party leaders. Priority two goes to active work party members determined by the work party leader and the RSSAC Admin Committee. And if out of those two priorities, if we still have slots left, those who goes to caucus members who expresses the desire to engage more work of the RSSAC. The application process, the caucus members needs to fill out a form so it will be more formalized and the decisions will also be shared publicly on the RSSAC mailing list and the wiki.

One additional requirement we've added is some lightweight reporting that for the funded travelers to really summarize the sessions they attended, the meeting held and their assessment of the experience. So, this is a lightweight process of how a proposal for supported IETF travelers funding guidelines. Any questions? Any thoughts?

BRAD VERD: I hope everybody takes a look at this. We spend a lot of time on this and I know staff has helped quite a bit trying to figure out an unbiased approach that encourages engagement, which goes back to the membership thing that we just talked about.

WES HARDAKER: This is Wes Hardaker. I do have concerns about subjective versus objective measurements and the ability to select people. That's hard to do, prioritization-wise and not have personal bias get in the way of each of us.

BRAD VERD: Yeah. I agree, Wes, but there is as we've learned even with the lottery, there is not perfect solution here.

WES HARDAKER: Yeah. I agree [to go].

RUSS MUNDY: Hi, this is Russ. One quick comment if I could. One of the questions that I have and a comment is I think I heard Steve say that the work party Chairs/co-Chairs would nominate people? Is that correct or was that the RSSAC co-Chairs?

STEVE SHENG: Russ, I think it's whoever applies. It's really there's the application and then we receive the application. Then probably the Admin Committee will check with the co-Chairs, whether the person who will be applying for the funding [inaudible]. The other way around is to apply and then we'll check. The work party will check.

FRED BAKER: And Russ, you're on the phone, you're not reading this so let me read it to you. First priority, it lists the RSSAC co-Chairs and the RSSAC caucus work party leaders. [Inaudible] and the Chair of the work party. Second priority is active work party members. The next question of course is what does active mean? That question is put to the work party leader and the RSSAC Administrative Committee. Now, who do you see actually doing something? Who is commenting [inaudible]? And then third priority, if we still have some funding available and people will want it, the Administrative Committee can respond to that.

Steve, did I get that right?

STEVE SHENG: Yes, that’s correct. Thanks.

RUSS MUNDY: Okay. Thank you. But the intent is that people would apply and then after the application cut-off date then these would be the criteria and that would be used. Did I get that correct?

STEVE SHENG: Right. The guidelines will be announced ahead of time. It will be announced to the caucus first, so everybody knows about it when they apply for the next IETF.

RUSS MUNDY: Right. Okay, thanks. Yeah. I look forward to reviewing this. It’s a challenging problem and I really do appreciate the effort that’s gone into make it a more effective use of the funding. Thanks.

FRED BAKER: Okay. Could we go back to the agenda please? Okay. So, we've had some commentary on the funding guidelines. Ozan, you're going to post those or no? Steve, you're going to post those on the RSSAC list and let people comment there? Okay. At what point should we close that? Could it be reasonable to give it a week, two weeks?

STEVE SHENG: Yeah. Would a week be okay? Because I think, if possible, we want to apply this guideline for the next IETF meeting in Singapore. So I'll say a week, and then a week of comments, and then for a week for the document to be in stable stage, maybe a vote via the mailing list.

FRED BAKER: Okay. And then we can just follow the mailing list guidelines. Okay. Then we'll do that. Please post it. We'll see how the comments go, and then we'll take a vote. So, moving on then.

Carlos, do you want to talk about Article 12?

CARLOS REYES: Thanks, Fred. Hi, everyone, this is Carlos. In Marrakech, you'll recall we had a discussion at one of the work sessions about the NomCom review and Recommendation 9 that came out of that, which was to give the RSSAC liaison voting privileges which would make that position a delegate on the NomCom. And in response, we would have to modify Sections 2 Article 12 of the Bylaws, which is the RSSAC Charter.

I've been meeting with Legal and I think what we're going to do is we're taking our cue from the NomCom Review. So as they move forward with those edits that are coming out of their review to the Bylaws – because this isn't the only edit of course – they're going to do them all as a package. So, nothing at this point now for RSSAC. Once Legal puts together the package of various edits to the ICANN Bylaws, obviously will come back to the RSSAC for your sign up on the RSSAC Charter in Article 12. But right now, there is no action and we'll just keep you posted.

One quick update related to the Bylaws, you'll recall that by adopting the Chair/Vice-Chair model in the RSSAC Operational Procedures that prompted another Bylaw change earlier this year, the public comment closed on that yesterday – last week, last week – and there were only two comments received. They were both supportive so the expectation is that the Board will now go ahead and make those changes to the Bylaws probably at their upcoming workshop. So, that's all on track.

I'll pause here to see if there are any questions. Fred, back to you.

FRED BAKER: Liman, you have your hand up.

LARS-JOHAN LIMAN: I have a small question. That's whether this has been discussed between SSAC as well, if there's any pushback from them for SSAC to become voting?

BRAD VERD: Russ, I think that’s a question for you.

RUSS MUNDY: Thanks. Please unmute. I have not looked carefully in the last short bit, but my recollection is SSAC is taking a voting position consistent with this recommendation and a two-year limitation on service and so forth.

LARS-JOHAN LIMAN: Okay. Thank you.

FRED BAKER: Ryan, you have your hand up.

RYAN STEPHENSON: Yeah. And this is just a little bit of education I guess, and I apologize for not tracking this. But in row 6 of that spreadsheet, it says RSSAC agreed with [signing] especially since NomCom now appoints directors to PTI. Does NomCom appoint also selects the ICANN Board and as well as Directors to PTI, or is it just Directors to PTI? Just a little bit of clarification on that, sorry.

CARLOS REYES: Thanks, Ryan. Yes, the NomCom appoints members of the ICANN Board and members of the ccNSO Council and I think the GNSO Council and At-Large Advisory Committee. So, the NomCom appoints those groups previously to the transition, the IANA sort of transition. And since the transition, it also appoints Directors to the PTI Board.

RYAN STEPHENSON: Excellent. Thank you very much.

RUSS MUNDY: If I could clarify just a little bit there, they do not appoint all of the Board members. The NomCom appoints approximately half of the ICANN Board members. The rest are appointed by the groups themselves.

FRED BAKER: For example, we send Kaveh to the Board, correct?

LARS-JOHAN LIMAN: That’s not how it works. Kaveh is a liaison. We’re talking about voting Board members here. As Russ said, roughly while half of the voting Board members are appointed by the NomCom and then the various supporting organizations being the ASO, the ccNSO, the GNSO, and possibly also ALAC, actually appoint voting members directly which is a separate process entirely.

FRED BAKER: Shows how much I know about ICANN. Okay. Thank you much. So, we have no particular action on this yet. When do you expect that we will need to take action? Would that be on the next call?

CARLOS REYES: Hi, Fred, this is Carlos. Potentially, it really just depends on how the NomCom proceeds with implementing their recommendations. To the extent possible, we'll make sure that the timeline aligns with the deadlines for voting items within RSSAC, but it's really driven by the NomCom organizational review.

I'm posting a link in the chat that explains the composition of the NomCom.

FRED BAKER: What I'm wondering is does this mean that we're going to eventually take a vote on the call, that there's no vote involved that I'm going to need to send an e-mail or Brad, send an e-mail announcing a vote? What's the game plan?

CARLOS REYES: There would e a vote because it requires changes to the RSSAC Charter in the ICANN Bylaws. How that vote happens, it really just depends on timing. If it aligns with one of the monthly teleconferences then we can do a vote during the teleconference and we'll do that. If it requires an online vote, we'll just make sure to sequence it.

FRED BAKER: Okay. That seems reasonable. But let me ask now, if this was put in front of you guys today, is there anyone that would be opposed or would be abstaining to it? Are there any comments we should be discussing? I don't see any hands going up. So, okay, we'll let this one go and we'll deal with it when it comes.

Terry, I believe you wanted to talk about RPKI?

BRAD VERD: Can I ask a quick question? I'm sorry, maybe I should know the answer to this one, but is there a reason not to vote on this now and just put it on the shelf? Or is it possible that it's going to change, Carlos, between now and a potential vote?

CARLOS REYES: Thanks, Brad. In Marrakech, we created a red line version of the Bylaws for Legal. Ultimately, the red line would come from Legal. So, I don't expect many changes from what RSSAC is suggesting, but I don't think we should vote until it's been vetted by ICANN Legal and all the other ducks are in a row.

BRAD VERD: I got it. Okay. Thanks.

CARLOS REYES: Yup.

FRED BAKER: Okay. I thought Legal had already seen it.

CARLOS REYES: They have but the Board has to approve it to go for public comment. So, we just want to make sure that the RSSAC votes on the same content that the Board is approving rather than what we suggested to ICANN Org and Legal. Does that make sense?

FRED BAKER: Yeah, that makes sense. Liman, you have your hand up.

LARS-JOHAN LIMAN: Yes. In addition, this isn't marked as a voting item on the agenda, so people who have read the agenda and are unable to attend wouldn't know that we're voting on it. Thanks.

FRED BAKER: That's fair. Thank you.

CARLOS REYES: Yes, this is not a voting item today.

FRED BAKER: Okay. Well, we'll see where that goes then. Terry, you wanted to talk about RPKI.

TERRY MANDERSON: Yes. Thank you, Fred. I hope you all had an opportunity to read the e-mail that I sent out. I found it a little bit I guess concerning. Oh, that's right. I also sent some slides off to Ozan. Thank you very much. I found it a little bit concerning that RPKI is hitting almost an inflection point, I guess, or a change point where a number of organizations are actually going to start validating their routing announcements or what they receive in routing announcements against the RPKI. That's a significant change to what we've observed so far. I've put some time thinking to what would be the impact to the root server system. I've harbored some concerns about the RPKI for some time but it hasn't been at any level that I have thought it problematic. Next slide please.

I've just included some terms about RPKI if you're not aware of it. RPKI is the Resource Public Key Infrastructure. It's covered in RFC 6810. We talk about a certificate authority which is an X.509 concept spoken about in RFC 5280, Route Origin Authorization or ROA which is covered in RFC 6482. That's essentially where an organization makes [inaudible] station that their prefix is going to be announced by a particular autonomous system number. Then we talk about RPKI validation. There's a number of RFCs that cover RPKI validation and how RPKI validation works, from 6709, 7115, and 8360. Next slide please.

I looked at this from a principle point of view and we have some base facts. We have 12 RSOs, we have 5 RIRs. And out of the RSOs, IPv6 and IPv4 resources come from only 3 RIRs. By virtue of the way RPKI is intended to work is that those resources would have their RPKI certificates based in those 3 RIRs. That means 9 letters, resources are allocated by ARIN, 2 letters, resources are allocated by the RIPE NCC, and 1 letter, resources are allocated by APNIC. Each RIR runs their own RPKI.

A year or so ago or some months ago, I guess, each RIR now asserts they own all of 0/0 and ::/0 in RPKI. That's not a perfect hierarchy. That means each individual RIR says they own all of the address space. ARIN says they own all of it. RIPE NCC says they own all of it, etc. And there's an [IP] statement that agrees with that direction. Next slide please.

We have a couple of principles in place. Firstly, we have the independence and diversity of operations covered in RSSAC042 and RSSAC038. We also have a statement out that says the failure of one RSO is not critical and that's in RSSAC021. When we talk about independence and diversity of operations, what's diverse enough? Is three diverse enough? Is one organization that impacts nine root server operators diverse enough? When we talk about the failure of one RSO, I read that as, okay, if APNIC have an issue and that impacted the M-Root operations, would that be in the same space as ARIN having an issue impacting nine letters? Next slide please.

We do know that some friends of providers have stated that they'll commence filtering their routes by RPKI in 2020. I believe I saw one note from someone else that NTT has actually already started. There's certainly a very strong push for adoption from the RIRs, both APNIC and RIPE, LACNIC, all RIRs are pushing for adoption. ISOC has their manners activity which is promoting good routing security. A part of that includes you should do RPKI. Next slide please.

These are the issues that I thought about. Hang on. I saw a chat message. I'll just quickly answer that. "Would it be possible for an organization to run their own CA and not using the RIR CA? Also, would it be possible to get a copy of the slides presented?"

Yes. Please, Ozan, share the slides.

"Would it be possible for an organization to run their own CA?" Not in the way that the architecture is structured for RPKI because you get your resource certificate from an RIR. I hope that answered your question, Ryan.

In the scenarios I've put together here, the first one is that an RIR is compromised and the ROAs of the RSOs in that RIR CA structure results in an invalid state. That essentially means if an organization who's doing RPKI validation sees a route from that RSO, it will drop the route. That route will not be propagated. That really means that there is no fault of the RSO and there's absolutely no fallback or mitigation to this at present. Next slide please.

In terms of that scenario, that would mean if the RIR is ARIN, that would mean nine RSOs could be impacted and it would be currently 87% of the root server system that would just basically go off the net because the routes would not be propagated. The potential here is, and what I'm basing this on is that at some point, most T1s, T2s will do RPKI validation. At that point, it would impact routing quite significantly across the Internet. Next slide please.

If that RIR is the RIPE NCC, two RSOs would be impacted and it would be 11% or almost 12% of the RSS. Next slide please.

Again, if the RIR is APNIC, one RSO would be impacted and there are currently nine instances or just under 1% of the RSS. Next slide please.

The second one is in scenario 2. Based on the fact that all RIRs are in fact authoritative RPKI, 0/0 and ::/0. If an RSO does not do an RPKI, let's say an RSO is being averse to RPKI – risk averse, whatever you may want to call it, or legally averse because some RIRs do require a number of contracts to be agreed to – and any one of the RIRs is compromised and a ROA is created against an originating ASN other than what is used, then the RSO's routes will be deemed invalid. Let's take the point of view from ICANN. If we decide not to do RPKI and we don't have an active ROA, AFRINIC could be compromised – let's hypothetically say they are – and a ROA is created underneath AFRINIC that disagrees with my routing announcement, then all of my routes will be deemed invalid and I would be taken off the net. That could then happen to any other organization that is not doing RPKI as an RSO.

Again, it is no fault of the RSO except for being cautious of RPKI, given the scariness of scenario 1. There is no mitigation or fallback to this. Currently, last time I looked, all but K would be impacted. So that's 94%.

I see a question from Liman, "What happens if two RIRs announce conflicting ROAs?"

Those are one of the questions I asked a number of people. Generally, it's a race condition to the point of who wins. So it might impact or it might not. It depends on RPKI validators. I'm not exactly clear on what RPKI validated code is currently doing. The RFCs actually say that the idea is you look for validity. You don't look for failure. So if there's one announcement that is valid, it should win. But again, I can't be sure of that. I think some investigation would need to happen. Next slide please.

In scenario 3, all RIRs are authoritative RPKI. If an RSO does do RPKI in any of the RIRs is compromised and a ROA is created then one or more

RSS routing announcements may become temporarily unstable and it's again to be validated. I think that answers Liman's question. Again, it's no fault of the RSO. Next slide please.

So the questions I have and before I get into my questions, let me just quickly check Fred asked, coming back to Ryan's question, "Is there a way that Aaron could co-sign the DoD certificate and announce it? Could the RSOs get the other RIRs to similarly co-sign certificates and announce them?"

Fred, possibly, I don't know. It would depend on what would be palatable for the RIRs. They are the ones in the driver's seat of this space.

So the questions I have, are all the RPKI CA operations constructed in the same old bit of fashion as the root zone KSK which has built-in protections? Are the allocation of IP resources and RPK operations suitably compartmentalized and separated such as the root zone administrator and maintainer separation? Are there suitable controls in place to stop IP resources existing in multiple RPKI CAs since RIRs, along with the IAB have walked away from a single global and consistent RPKI CA, keeping in mind that the original plan for the RPKI was that the RPKI would've been seated at the IANA and because it would've been a complete hierarchy it would from RPKI allocation state and certificate issuance, you could not have a situation such as scenario 2 where an RSO could be impacted by multiple RIRs. Are there any mechanisms in existence such that the operations of the RSOs can be impervious to RPKI values by RPKI issuing entities? What can we do as RSOs to mitigate this risk? Does this mean our diversity of organizations is now actually 5 per number of RIRs or 3 given where the RIR resources allocated from and not 12? And is that actually okay for the root server system?

I think that was my last slide. I think with that, I'd like to ask, are there next steps for us here? And are there any other questions?

FRED BAKER: Well, I don't see any hands, so I'll chime in here. Thank you for that. It seems like the obvious place to discuss this is actually going to be on the SIDR Ops list in IETF. Basically, not talking about RSOs per se but talking about entities that would like to have redundancy. Imagine that a Certificate of Authority goes south, what's the backup plan? And it may require an Internet draft we could probably cobble up among ourselves, describing a potential solution. Is that how you would approach this?

TERRY MANDERSON: I took the opportunity at IETF to raise my concerns actually at SIDR Ops. I've got a lot of shaking of heads and one comment at the microphone is, "I don't care if you're an RSO." Tough. I don't think I'm a snowflake in any way, shape, or form, but the sentiment really was from the SIDR Ops meeting was that, "This is not our problem. This is your problem somehow. I'm not too sure how it's my problem." They don't see a problem with the architecture.

FRED BAKER: Okay. I see a problem with the architecture but Wes wants to get in. Wes?

WES HARDAKER: Yeah. A couple of things. I actually would think that Russ should have comments too because he is much more integrated into the development of the RPKI in the first place. The RPKI was designed to help things, not hurt things. Now, of course, with any security mechanism, you can end up hurting things too. I value the analysis done and I think we should definitely do things like spread out across our RIRs and stuff and in fact even though B recently renumbered, we'd even be willing to renumber something to LACNIC or assign the address space or something like that. We likely will be issuing RALOs for our space sometime in the near future.

But the important thing to remember is that the RPKI was designed to prevent a form of attack which we have traditionally not worried about much, and that is hostile takeover of routing space in the first place. So we know for a fact that there are people that are answering for root server address spaces with their own service. We see that in – if you go look through the RIPE ATLAS data, you'll see instances of your servers that are identified by other NSIDs and things like that. That's just the ones that are actually willing to lie about it and actually say it publicly. We have no idea frequently how many routing blocks are being advertised by malicious actors that we don't know about.

I guess my last point is, remember that the purpose of this is good and to be able to [inaudible] a technical solution to another problem and looking at the mitigations and the risks of that technical solution that's important. The other thing to know is that the root servers are not unique. The up and the downsides of the RPKI system and its validation affects every net blocks, not just ours. Now, we're interesting because we want the independence and the lack of hostile takeover a single entity and things like that, but I would argue that there's probably a lot of other organizations that are in the exact same boat, everything from corporations like Facebook to do the RIRs themselves for that matter. Thank you.

RUSS MUNDY: Fred, I do have some comments.

FRED BAKER: Go ahead.

RUSS MUNDY: Thanks. I did send a message to the list last night. I apologize that it was so close to the meeting but I listed a number of points. I also got some feedback from your presentation at the SIDR Ops meeting, Terry. The impression that I had was, to an extent, there was at least what was contained in what you said did not evenly address the benefits and shortcomings that are associated with the RPKI and doings, putting security in the routing space itself.

As Wes said, it was created to counter route hijacks. Now, they happen all the time and nobody I don't think has any real valid statistics on how extensive route hijacks are. They range from small events to some really large massive events. To the best of my knowledge, there's only been limited amount of this malicious activity explicitly against the root server system or the individual RSOs. But some of them have been involved, who has pointed out one place where this can be observed. And having the set of structures that was created through the IETF process, it did in fact, it was a long effort and there was a lot of discussion about some of the problems that could result. And as you noted since all five of the RIRs have issued essentially a certification for themselves that say they can be the owner of all the address space, that facilitates the transfer of IP space and AS between the RIRs but also does open up to the type of problem you noted where one RIR could cause problems for holders of space in other RIRs. But similarly, if the problem that you note where one that could cause a problem like that, another RIR could in fact issue a certification for that address space under their full address space ownership.

So, as people heard and listened to some of the points that you made, I think some of the skepticism and perhaps some of the shaking of heads reflected not so much that you were sort of taken “we’re special, we’re a nameserver” as it wasn’t really I think an evenly approached recognition of the problem that it was supposed to be solving, examination of the likelihood of that problem because any route hijack has to be solved by the operation’s activities involved. There wasn’t any acknowledgment that RSOs, especially since going to Anycast are very vulnerable to route hijacks. We haven’t really seen one and a malicious one against the RSOs could occur, and that is in fact the type of thing that the RPKI was created to prevent.

With respect to security of the RIRs, each one has decided what’s in a security itself. Kaveh did offer on the list to provide more insight and details into the operation, and this is certainly something that I think is legitimate to examine. But my general point I was trying to make in the e-mail that I sent last night was that I think a fairly thorough risk-benefit analysis should be conducted with respect to these issues that you identified because I agree there certainly are potential problems. But are there solutions? And when you said there aren't mitigations, I think that's one of the things that caused people to say, "Well, we're not sure that this is sort of a balanced presentation about RPKI."

I'll stop with that and if there's other comments or questions for me, I'm happy to respond. Thanks.

TERRY MANDERSON: Russ, if I may just very quickly respond. There were absolutely shaking of heads and my observation was they didn't actually offer any answers to any of these concerns. That's why I've walked away with there are no mitigations. I don't know of any and they didn't offer any.

RUSS MUNDY: So, I think it was your scenario 2 where another RIR caused the problem for someone whose IP space came from a different RIR than the one that was problematic since everyone has in fact issued the "I own everything" certificate. A solution to that is for a different RIR to issue a valid certificate for that particular space.

Also if there is a compromise of an entire RIR, there would be a large and very intense bit of attention applied to that I think. Now, whether or not people had thought through some of these things, I did have a little bit of the advantage of reading your e-mail and having thought about it a little bit, I'm happy to do more dialogue on it and more back-

and-forth analysis because one of the hard things to know about route hijacks is they are totally unpredictable. And when they occur, the corrective action at this state and time, if you're not doing RPKI, requires positive coordination with multiple operators. If the group that originally caused the problem was a group with malicious intent, you could not depend on that group correcting the problem that they had induced that resulted in the route hijack. You'd have to go to further up the chain in the routing hierarchy groups to get correction. So, trying to develop how high a risk one has of having the route hijack is very difficult and I think it would present in some ways the hardest part of doing a thorough risk assessment, risk analysis.

Terry, have you had a chance to take a quick read through the message I sent last night?

TERRY MANDERSON: No, I haven't. I'm sorry.

RUSS MUNDY: Okay. Perhaps it would be useful if we did some dialogue on the list so everybody can see the back and forth of what's going on.

I think that's all that I wanted to just raise at this point. Thanks.

FRED BAKER: Okay. Wes put a comment in the chat. I won't read it to you but look in the chat to see Wes's comment.

What I wonder, would it make sense for some variation on us – "us" might be Terry and Russ – would it make sense to file an Internet draft for SIDR Ops that's driving the problem in proposing a solution? That's the question.

TERRY MANDERSON: I don't know. Actually, I don't know whether that would help or not.

FRED BAKER: Russ, you have your hand up. Is that an old hand?

RUSS MUNDY: No. That is a new one, Fred. I did manage to get to a place where I can get to the Zoom. Yes. I think it would be good for us as a group to at least come up with an approach for improving the robustness of the routing protection for the RSOs now. The SIDR Ops, I agree, sounds like a reasonable place to present this. We as a group know enough people around the community that we could in fact discuss it informally with people before we took it to SIDR Ops and get the open IETF Working Group feedback and see if people saw it as a plausible solution.

I think Wes's suggestion off the top of his head is one possibility that if there's the IP assignment, the challenge is in fact a hard challenge. I know that at least some, if not a large portion of the RSO IP space is like a C space, and I think Kaveh did offer a potential solution there.

I think discussing it further and coming up with a plausible approach, that would have some balance to it because I have to say what I saw from the slides some of the informal feedback I heard. No one said this but it almost sounded like at least from Terry's perspective that the RPKI was more of a problem for the RSOs than it was a solution. When you approach a working group whose job is to look at this technology and how it's used and have someone come in and say, "This is more of a problem than it is a solution," I suspect that was also some of the headshaking that was going on. Thanks.

TERRY MANDERSON: If I may very quickly respond, Russ.

RUSS MUNDY: Sure.

TERRY MANDERSON: That's exactly what it is from my perspective. It is absolutely more of a problem than it is a solution. The impact for protecting against route hijacking for me is exceptionally low. It is very low. I have 170 instances out there. Others have more. So if someone hijacks in one little area, it's only one little area. It is not across the board. At this point in time and I'll pick on AFRINIC just as a name out of the hat, if they are compromised right now and the ROA is issued right now, for all intents and purposes, I would be RPKI invalid and my routes will be dropped.

So, yes, Russ. I absolutely see this as more of a problem than it is a solution right now. And no one could tell me otherwise. No one. I think that's a very hard message for SIDR Ops to hear because they are very in amid with their solution and that's okay. But that doesn't help me get to a position where I'm responsible for the operation of a root server. And every organization essentially represented here is responsible for the operation of a root server.

So, those are the concerning things. I'm perfectly happy to continue the dialogue and I'm probably thinking here and now is not the right place. But I'm absolutely perfectly happy to continue with the dialogue. What I'm really looking for is, "Terry, your assertions are invalid," and I don't believe they're invalid and no one has told me otherwise at this point. Additionally, "Terry, your risk profile is incorrect," and no one has suggested that either. So those are the two things I'm looking for and I haven't heard on this call so far. So, yes, I'd be looking to continue the discussion.

RUSS MUNDY: One thing I hadn't mentioned, Terry – and I think you may or may not know this – one of the differences in the specification that came out the IETF for the RPKI versus DNSSEC, to be compliant with the specification for DNSSEC, if you're saying you're doing DNSSEC in validation, you must do validation and you must not return and answer to the query and resolver. In the RPKI specifications, the control over what happens with an invalid route update is completely left up to the operator themselves. Now, given that people don't like this sort of manually override, but what has occurred in the DNSSEC world was the creation of the negative trust anchor and the processing of that. But what as far as that aspect of the RPKI, local operators can be completely within the specification, and as I understand it, most all the implementation have the knobs set so that the local operator is not forced to trash the answer. They can take the update if they believe that it is in their best operational process.

That’s one of the subtle differences in terms of what happens with validation in RPKI versus DNSSEC. You still have to have people and you still have to have operators involved if something like that is the situation.

The other thing in terms of the route hijack, although you say you're spread in a hundred locations, you're still using a very small number of IP space and such a routing hijack such as what happened with the Pakistan YouTube hijack a few years ago where it was intended to be contained only within a geographic area, it escaped, got into the routing system and was promulgated worldwide. So even though you're in many locations with your Anycast node, your IP space can be hijacked from a small or a single entity once it gets into its promulgation state across the network. That is one of the other considerations in terms of the risk that’s faced by the nodes with a large number of Anycast instances.

Thanks for letting me comment on this and I’ll stop there.

BRAD VERD: I want to thank Terry for sharing this. I think this conversation is maybe … I know, Terry, you're sharing this conversation with [inaudible] Ops, so this conversation could continue there. I guess my question is as the conversation continues, when something comes up that if people believe that RSSAC should be commenting on something then clearly bring it back here so that we can do that. But I believe like any further discussion on specific route hijack and whatnot maybe this is not the best use of our time right here.

FRED BAKER: I would agree with that. It seems like it should be e-mailed for the moment but I do think there's a place for a solution. I'm thinking about Ryan's concern that he uses the different certificate authority. There needs to be a way to deal with that and I'd suspect that comes out of SIDR Ops. Okay, time to move on.

The next topic is the workshop planning. Ozan, do you want to talk about that?

OZAN SAHIN: Thank you, Fred. At ICANN65 in Marrakech, RSSAC asked for staff to circulate a Doodle poll to determine the location and timing of the next RSSAC workshop, and that's what we did. The first week of October in Washington, D.C. area stood out based on the results. Then staff got in touch with various departments, especially ICANN Meetings Department to get the estimate cost. And then finally last week, a certain note to RSSAC list indicating the workshop would be held in Reston from the 1st of October to the 3rd of October.

I also shared a link to a form where RSSAC members could complete if they are interested in travel support. Please make sure to fill in this form by this Friday, 9th of August for planning purposes and then staff will submit the list of travelers to ICANN Travel Team. For your [inaudible], I’m pasting the link to this form here in the chat. Please let me know if you have questions. Back to you, Fred.

BRAD VERD: Fred, this is Brad. May I comment?

FRED BAKER: Go for it.

BRAD VERD: Just for everybody’s edification, this workshop in October will be in the Verisign facility at the Hyatt like we had last time. Just so everybody is aware of that.

FRED BAKER: Okay. So we’re walking down to the Verisign facility, correct?

BRAD VERD: Yeah. It was described as if it would be in Reston. The last one it wasn’t Reston. I just wanted to set expectations that it was not at the Hyatt. That’s all.

FRED BAKER: Okay. That’s cool. So, Ozan, are we done with that?

OZAN SAHIN: Yes, Fred.

FRED BAKER: Okay. Cool. Then moving on, Duane and Russ, do you want to talk about the Metrics Work Party?

DUANE WESSELS: Yeah, sure. This is Duane. The work party – we had a meeting in Montreal a couple of weeks ago. I feel like we've made some good progress on a couple of things. First of all, we agreed to focus metrics on service level aspects only. So, [Inaudible] taking is out of scope using these kinds of metrics for some research purposes and other purposes that are not related to service levels.

We also agreed to not have [self-supported] metrics and probes operated by the operators, which essentially also means that we won't have what we were calling near probes, I believe, so focusing now just on farther away probes.

Current work is to document these decisions in the work party document and rearranging some of the text in certain sections. We have a call this Thursday and following that, we'll have standing bi-weekly calls every other Thursday for this work party.

Anything to add, Russ?

RUSS MUNDY: No. That's good. Thanks, Duane.

DUANE WESSELS: Okay.

FRED BAKER: I'm actually on next for the Resolver Work Party. I'm having a discussion with Paul, with my co-Chair – or whatever you call him, the work party leader. Practically speaking, he is the work party. We have had zero contributions from anybody else or there's one that we very specifically wanted to have – that was Jeff Houston – that hasn't happened. The work party is largely a conversation between myself and Paul.

Paul is stuck right now on using IPv6 in his simulation basically because he doesn't have IPv6 in the lab that he's working in, wherever that is, which seems surprising to me, but that's what he reports to be the case. So what he's thinking is that he's going to wind up allocating the ULA or something within the simulation and then placing a network address translator between that and the outside world, which wearing one hat, I know that my community is going to cry when they hear that. On the other hand, speaking very practically, frankly I don't see a problem with it. It allows him to test the mechanics wherever the address came from. He and I are having that conversation.

We haven't got a next meeting planned. I would like to have that happen in August. I'm going away for three weeks in September. So, I want to have that happen before I disappear.

Ozan, has Paul been talking with you about scheduling a meeting?

OZAN SAHIN: Hi, Fred. Yes, the last time he talked about it, he mentioned that the next meeting wouldn't be before August, so I should reach out to him again and ask when the next meeting would be.

FRED BAKER: Okay. So I would like to have that meeting before August 27. Very personally, I'm going to disappear on the 27th, so I really don't care when but between now and the 27th.

OZAN SAHIN: Understood. Thanks.

FRED BAKER: That's pretty much what I have to report. So, I'll move on. We have reports from co-Chairs and I'm on the hook to deliver that. I'm not aware of anything we need to report. Brad, do you want to chime in?

BRAD VERD: Yeah. Nothing to share since the last call that I can think of that hasn't already been talked about.

FRED BAKER: Okay. Kaveh, what's happening on the Board? Kaveh?

LARS-JOHAN LIMAN: This is Liman. I was thrown out and back in again. So maybe the same thing happened to Kaveh.

KAVEH RANJBAR: Can you hear me now? Can you hear me? Sorry, I was on mute. Nothing has happened. There will be a workshop start of September but we are still waiting. Nothing coming off from the Board side. So, basically, no update.

FRED BAKER: Okay. Liman?

LARS-JOHAN LIMAN: There's actually nothing to report from the CSC either because there was no meeting in July that the committee decided to cancel July meeting. The only notable news item from the CSC is that Byron Holland, who is the ccNSO and also the CEO of CIRA, has decided to not send reelection to the CSC, so we are looking at having a new Chair next year. But he will remain in his seat until his term ends. Thank you.

FRED BAKER: Thank you. Brad?

BRAD VERD: Nothing to report from RZERC. There's been no meeting. I think right now we're in the process of trying to schedule. So, maybe next time.

FRED BAKER: Okay. Russ, SSAC?

RUSS MUNDY: From SSAC, there will be comments provided in response to the request for public comments in the four documents, RSSAC037 and the other associated documents. They're pretty well put together at this point and I had not made any offer to let RSSAC have a preview, but I can ask for that prior to publication if you folks desire, but I had not asked for that so far.

FRED BAKER: Okay. Daniel isn't here who sent his regret. So, Naela, what's happening with the IANA?

NAELA SARRAS: Only one quick news item. We mentioned this during the Marrakech meeting. Kim Davies is holding a webinar with community members to consult about the budget consultation for PTI. He has a webinar happening on the 13th of August and he's I think extended an invitation to the SO/AC Chairs, so if anyone is interested to contribute to informing IANA and has the right priorities, help us in other priorities, he's welcoming that feedback during the webinar. That's it for me.

FRED BAKER: Okay. Duane, RPM?

DUANE WESSELS: Nothing to report there. Thanks.

FRED BAKER: Okay. Liman, you dropped a note in the chat. Let me respond to that verbally. The October workshop is happening the 1st through 3rd of October in Reston at the Verisign facility. Ozan sent out an e-mail a couple of days ago. You might check your e-mail. If you don't see that there, drop a note to me or to Ozan and you should be able to get that.

Okay, we have now arrived at AOB. Next meeting is Tuesday, the 3rd of September. Brad will be running that meeting. Do we have anything else we need to discuss today? Hearing none, then do I hear motion to adjourn?

LARS-JOHAN LIMAN: I so move.

FRED BAKER: Okay, then we stand adjourned. Thank you.

LARS-JOHAN LIMAN: Thank you all.

UNIDENTIFIED MALE: Thanks. See you soon.

[END OF TRANSCRIPTION]