BRENDA BREWER: Good day, everyone. Welcome to the SSR2 plenary number 114 on the 17th of June 2020 at 14:00 UTC.

Attending the call today are Alain, Ramkrisha, Kaveh, Russ, Kerry Ann, Scott and Eric.

Apologies from Danko.

Attending from ICANN Org is Jennifer, Steve, and Brenda, and technical writer Heather.

Today’s call is being recorded. Please state your name before speaking for the record. Russ, I'll turn the call over to you. Thank you.

RUSS HOUSLEY: Thanks. The first thing is we’re trying to figure out when to hold the conference call regarding DAAR. A Doodle poll was sent out Monday I think. But some people have not yet responded. We need to close this soon so that we can get input. But right now, it’s looking very much like it'll be in lieu of the plenary call next week. But not many countries have been heard from here yet, so if people could fill that in during the call, we can maybe make a decision at the end. Thank you.

So in addition, there was a Doodle poll about the number of people who would be able to participate in a plenary call next week, given that that is going to overlap with the ICANN virtual meeting. So if you could show those Doodle results. It looks like a fair number of people could attend, but let’s hold off on making an absolute decision based on whether that is the slot we have to use for making the DAAR call.

Okay, the next thing is to report out on subteam 27. Alain sent a document earlier today to me and I passed it along to Jennifer for display. So Alain, I turn it over to you to take us through that.

ALAIN AINA: Yes, I have to apologize for the delay. I sent the document two hours ago [and before that to Russ] who is with me on the subteam 27 and didn't have time to look at it. So my suggestion is that I will go through it but I don’t think we should try to approve it [at the group] but then maybe wait for Russ to review it.

I also did add the comment document. I don't know if you can also show the feedback document quickly. Jennifer, can you show the feedback document?

RUSS HOUSLEY: There it is.

ALAIN AINA: Scroll to the right side. I want to show the colon E to colon 7. Okay, so if you just scroll down to section 27 where recommendation 27, okay, as you can see, I did that and I put a suggestion for our response to the comment and also the changes with—so basically, we address this comment by saying that, yes, we add the text to cover the other ECC algorithm so as to [inaudible].

[And again, there is more on that, so scroll down.] I was wondering if we could maybe extract only the section 27, but if you keep scrolling, I think there's a section where we'll see the SSAC response. Yes, this is another example. I think this is one of the comments from SSAC saying that yes, the fact that referral to the [NSA] recommendation on this thing, etc. So we accepted the comment and then said that we would remove the reference to that recommendation to go for RSA 3072.

And there's also another one here saying that—it's on recommendation 27.1, this is another recommendation from SSAC saying that we should make the recommendations more generic in nature. Okay, we agree that we should do that. [inaudible]. So then I said we accepted this and the new proposal [inaudible] as I showed last week or two weeks ago, then we totally remove the reference to specific algorithm and we just say that we should move from RSA to another algorithm so we are no longer mentioning ECDSA or quantum, post-quantum algorithm.

So now please scroll down more. This covered the SSAC I think there were a couple of comment on 27 from ICANN Org. Yeah, please scroll up a bit. And then I covered this. There were two recommendations or comments from ICANN Org following these two.

Okay, apparently [then I think I added] I also added some comment—there were two comments from ICANN Org. Something seems to have happened. Okay, so basically, if you can go to the ICANN Org. Yeah, right here.

So ICANN Org comment saying that the DPS does not provide the plan for algorithm rollover, so [inaudible] the team has not intended to provide how the algorithm rollover should be conducted. And then also, the complexity of the rollover has been acknowledged in 27.2. And then I'm pointing to the new [test.]

Then there was another, a second point, again from ICANN Org, saying that they were doing that consultations on the key rollover, but that consultation clearly said that it does not cover algorithm rollover and this team, we supported the separation between normal key rollover and algorithm rollover. That's why in our report, we have different sections dealing with KSK rollover and we have a different section on covering algorithm rollover.

So this is what I put then pending review from Russ and the team. Can you now go back to the other document? Okay, so basically, this document is the base of what I just presented over there. As you saw, most of the concern, especially from SSAC, is being so prescriptive on EC, etc. so the idea here is to make the discussion on the DNS cryptographic more generic [inaudible] even those we continue to mention ECC, we continue to [inaudible] ECC and cover the other [inaudible] ECDSA which was also one of the comments.

And then if you scroll down a little bit, this reference to the US security agency recommendations, I think we said that we should remove it. and what I also did is to put now also the finding on the DPS after—

RUSS HOUSLEY: Did we lose Alain? Oh no.

KERRY-ANN BARRETT: It still says he's connected but his mic is ...

ALAIN AINA: Hello.

RUSS HOUSLEY: Yes.

ALAIN AINA: Yeah, can you scroll down to this? Okay. Scroll down after the description. So then the section on the finding that the DPS is quiet on the key rollover has been put after the description of the algorithm here, and then you have the new version of the recommendation 27.1 where the key changes here is that the previous one said PTI operations will update the DPS to facilitate, and [this facilitate has generated] the two comments we saw from the organization saying then no, the DPS does not provide a plan, which is normal, so now we changed facilitate, we replaced by just to allow. And then we also addressed the issue of people complaining that yes, key rollover does not necessarily improve [inaudible]. We changed the wording. Then it is the new 7.1. Then 7.2 remained the same.

And as I said, this has not been reviewed by Russ, my team member, so I think we can discuss it and if there are comments, objections ... So I'm done.

RUSS HOUSLEY: So I sent the document and the pointer to the public comment response to the mailing list, so everybody should have that. I suggest we send any comments that you might have to the mailing list. If there are minor word changings, if there are direction issues, let's talk about them now. So, are there any direction issues?

Okay. Hearing none, please wordsmith to the list. And up next was the Laurin for grouping of subteams that are dealing with the risks part. What do you want displayed, Laurin?

BRENDA BREWER: Russ, Laurin is not on the call.

RUSS HOUSLEY: Oh no. I could swear I heard him. Okay, Laurin's not here. Then we'll skip that for now and move to KC. KC, you wanted to talk about recommendation 22.

KC CLAFFY: Yeah. I'm just not convinced, based on all the comments that I read, that this needs to be in here. If it does—if there are folks who feel strongly that it needs to be in here—and I take the point that RSSAC who is really the constituency who would most benefit from it, I guess, did comment but they comment very tersely of, "Well, we support this." However, a lot of others did not or didn't care or didn't see the problem. In particular, both ICANN Org and SSAC don't understand what problem it is we have identified that we're trying to solve. I rather agree with that, having read all the RSSAC 37 and the whole governments working group stuff.

If somebody feels strongly that we want to keep it, I think we really need to go to RSSAC—and maybe somebody did this and I missed it—and ask them what is the problem you see and what would you like to see SSR2 say specifically in terms of how to measure implementation of such a recommendation, or do you think pretty much ICANN is being responsive when you need something. Which is clearly what ICANN thinks from ICANN Org's public comment to this recommendation. That's basically my position. I wonder what others think. Did anybody talk to RSSAC or know of anybody that talked to RSSAC from SSR2 before writing this?

RUSS HOUSLEY: I don't remember who held the pen for 22. Does the person who did—are they on the call?

KERRY-ANN BARRETT: I'm not the penholder and I can't recall who drafted it, but I just have a question for KC. Would it be remiss of us not to even mention it even if we remove the recommendation? Are you saying that we shouldn't speak to it at all? Because my feeling is that the review team would have—whoever drafted it at the time, because as I said it probably would have been one of the legacy recommendations, that it would have been because of observations from the investigations that we did earlier on that came up. So, do you see room in incorporating it as a comment even if we don't want to give a specific recommendation but then reference the RSSAC recommendations and at least say that this is an observation that we made, but we decline to make a specific recommendation because blah-blah and then refer them to the more detailed document? I'd prefer that approach than just to remove it.

KC CLAFFY: Well, sure. Look, we have to explain how we are dealing with the public comments, so my assumption is that in that explanation, we would say given that ICANN Org thinks this is already under way, we will not make a specific recommendation but encourage other review process to consider this as it plays out.

KERRY-ANN BARRETT: But should this be part of our findings, not necessarily just in response to a public document? Because it would have been something that we thought is an issue. And as I said, I'm not sure who drafted it, but the fact that it's stayed in all the iterations means that it's something that's important enough to stay there. So, should be, instead of just replying to the public comment, actually have a specific reference to the issue and say that we would defer to give specific recommendations in ours, but probably [ask for] continued monitoring of what ICANN Org is doing.

KC CLAFFY: That would be fine with me. I think we should still ask, and I can reach out to somebody on RSSAC. We don't have an RSSAC rep on this. I guess Eric was the closest we had to an RSSAC rep, but I would ask [inaudible]

KAVEH RANJBAR: Yes, if I can speak [inaudible]. If you need to link with RSSAC—because I'm also on RSSAC, but not here in RSSAC capacity. But I can easily link you to the right person. So I would be more than happy to help. Drop me a line.

KC CLAFFY: Well, if you're on RSSAC, I would just be curious of your view of this recommendation and what your take is on whether RSSAC sees there's a problem now that needs to be solved in terms of ICANN’s role in the governance proposals that—I mean, it was over a year ago now that these documents were published, and I don't know what the status is of ICANN’s processing of them. Do you know—

KAVEH RANJBAR: Yes, I know that. I can comment on that but I prefer not to comment on RSSAC’s decision because—I don't think there's a conflict with the board, but I think that’s the right thing to do. But in general, the process on that, RSSAC is following up with the board and actions are happening. Now there is a new work party basically that has been formed which is root server system governance work party which consists of different stakeholders. They have met a few times and they have, I think, reported back to different constituencies. I think they’ve also published a public report, but I'm not sure about that. So that is ongoing and the aim is that phase—which would be phase two as it was planned—will end this year, hopefully. That’s the last I've heard. And then there would be a framework and then next step would be implementation. So that is ongoing, but I wouldn’t comment on RSSAC but I would be happy to link you to people who'll readily give you the answer.

KC CLAFFY: Okay. Are you aware of that process actually creating any sort of—what's the phrase in here? Key performance indicators for the root servers?

KAVEH RANJBAR: Yes. So they are work—I don't think it's KPIs, but yes, one of the goals that they're going to achieve—and I think it's even specifically mentioned in the charter—is to come up with service level expectations, so that's the track they're following. So yeah.

KAVEH RANJBAR: Okay. My view is that there is not a need to do a recommendation here, that what is happening seems to be what should be happening, and I don't know what the problem is that SSR2 thinks exists that needs to be solved and how you think SSR3 should measure—well, I guess there won't be an SSR3, but whatever, how implementation of this should be measured.

KAVEH RANJBAR: Sorry, one additional input just because I know that the group, GWG is very open to meeting with different players, if you're interested in general, if SSR2 is interest, Ted Hardie is the char and generally, because I know they were looking for people who might have ideas about what they are doing and I know that generally they're open to meeting with interested parties. Just as an information [inaudible].

KC CLAFFY: That would be of interest, to me at least. It sounds like it’s been long enough that maybe touching base with the people who we think were claiming to help would be valuable. That’s all I have though.

RUSS HOUSLEY: Kaveh, KC, are you going to make sure that that RSSAC conversation comes to closure?

KC CLAFFY: Maybe, Kaveh, do you mind syncing me up with Ted, or at least sending me his e-mail?

KAVEH RANJBAR: Yes, I can do that. Just mind you, Ted is chair of GWG which is not RSSAC. RSSAC also has three representatives there, but it consists of different groups. But of course, I will [send you his e-mail.]

KERRY-ANN BARRETT: As we explore this, the only caveat I would have is, like, I would support your thinking and your process, but I would generally just want us to at least include in the report itself before removing in it, just a statement or position on it and what action we thought was necessary and where it felt within our purview or we thought it was better suited onto someone else’s purview as the work continues. I don't know what would come out of the discussions, but at least a mention of our thinking to remove it.

KC CLAFFY: Kerry Ann, I accept that, but then we need some consensus on, one, what the problem is, and two, whether the working plan that ICANN and GWG are taking up right now is addressing the problem, because that would be a finding and then a reason to remove the recommendation. And it looks like that to me, but it would be good to have one other voice say that.

RUSS HOUSLEY: So, what I heard today makes me think that there is something on track that is likely to address it. But I can't tell if it for sure will. And that’s just a reason to have something in the report so that five years later, somebody takes—

KERRY-ANN BARRETT: [inaudible] take it up. And that’s where my thinking is, Russ. As you said, KC, identify the issue, fine. But if we can't make a specific recommendation as you said, because the work that they're doing may address it, is just to actually state that. So the next review team or whatever will come out of our recommendations, for persons to look back if they were implemented or not. In that general findings section where we have like observations, things that we noticed but we didn't comment on because we spoke about doing a section like that before.

We could just say this is one of the things we thought was being addressed [under the] workplan and we just hope that somebody continues to monitor it. Just as a general statement so it doesn't get lost altogether.

KC CLAFFY: Yeah. Okay.

RUSS HOUSLEY: Okay. I notice that Denise is not here. Was somebody else planning to speak to the abuse grouping?

KC CLAFFY: No. There was going to be a call on that yesterday but it got canceled at the last minute.

KERRY-ANN BARRETT: I'm not sure either.

RUSS HOUSLEY: Okay, then we'll hope to hear more at the next call. I'd like to remind rapporteurs that we need status updates put into that spreadsheet so we know where they are, and that we're shooting for July 1st to have all the subteam report outs. Any team that has a report out will talk about next steps. KC had recommended that we drop any recommendation that has not got a report out by the 1st, but we softened that a little bit and said we will talk about any subteam that hasn’t reported out as a group to figure out a way forward.

Let’s go back to the DAAR Doodle poll and see if we have more responses. Okay, I think it’s pretty clear that we’re going to use the call slot next week for the DAAR call then.

JENNIFER BRYCE: Russ, this call is for after—

RUSS HOUSLEY: Oh, it’s an hour off. Sorry. I was assuming it was my time zone. Silly me.

JENNIFER BRYCE: I know, it’s pretty confusing.

RUSS HOUSLEY: Okay, good, so we can actually have both.

SCOTT MCCORMICK: Are you assuming your time zone? Sorry.

RUSS HOUSLEY: Yes, how awful.

KC CLAFFY: So Russ, that means you can't attend?

RUSS HOUSLEY: No, I can't. There's an IETF thing going on at that time. Okay, so we will go for the Wednesday. That must be Brenda's time zone, right?

BRENDA BREWER: Yes, of course. I don't know if I can change it to UTC.

RUSS HOUSLEY: No, that's fine, I just had ... All right, so I will put it on my calendar, but ...

BRENDA BREWER: Tada, UTC.

RUSS HOUSLEY: In case the other thing happens to drop off. Okay, so let's schedule that. Laurin, you seem to have just joined us.

KC CLAFFY: Can I ask a question about that call? Is there going to be a transcript of it?

RUSS HOUSLEY: It'll be recorded, I believe.

KC CLAFFY: And it can be in the normal SSR2 archives so other people who aren't there can go watch it.

RUSS HOUSLEY: Sure. I'll let Jennifer speak to where to find it.

JENNIFER BRYCE: Yeah. We’re going to record it the same as all calls, and we can request a transcript and we’ll post it on the Wiki so you can link back to it in the report.

KC CLAFFY: Great. Thanks.

RUSS HOUSLEY: Okay. Laurin, did you join?

LAURIN WEISSINGER: Yes, I did join. My apologies. I'm moving house so I got the time wrong because I'm doing a million things at the same time.

RUSS HOUSLEY: What a horrible time to be moving.

LAURIN WEISSINGER: Oh yeah. It’s great. But yes, so next week, that call is fine. I realized my answer didn't show up even though I thought I had replied. And I guess you want to know about budget change.

KC CLAFFY: Budget change?

LAURIN WEISSINGER: The change of the budget recommendation.

KC CLAFFY: I have no idea what you're talking about.

LAURIN WEISSINGER: So, I'm not sure, is this what I should talk about?

KC CLAFFY: Well, your name was next to risk.

RUSS HOUSLEY: Yes. Last week when he presented the updates, there was a discussion that led to a discussion of budget. There's two aspects of budget we’re talking about. The first is to be able to identify SSR-related items in the ICANN budget. That’s a spillover from SSR1. And then when we were talking about the c-suite position, we said, hey, that needed to come with adequate budget to do the job. So harmonizing all of that was the task that Laurin took his homework out of last week.

LAURIN WEISSINGER: Yeah, so essentially, if you go to the “relevant to” documents, it’s both in the one that has all changes accepted and the risk background document. Essentially, all I did is I pulled down the analysis that was with budget and extended it. So essentially, the idea is—I'm not sure if it can be shown. Oh yeah, Jennifer just posted a link. Thank you.

So essentially, the idea is all the security minus a few bits and bobs that might not be possible to move would move under this new role. So essentially, the budget recommendation when it comes to transparency, I essentially left what is there, did some level of culling because of how it now works, and then essentially say, okay, move all the relevant security budget under this position because all the security org would move under that position as well so it only makes sense to move that budget and I also kind of made this organizational change clearer. If you look at—

RUSS HOUSLEY: I think we should be looking at recommendation six, Brenda.

LAURIN WEISSINGER: The old recommendation six, and after that, the one following is [inaudible] budget. Here, I don’t have the markup, and it’s a few days, yeah. If you go down a little bit and a bit more, yeah, so this is where it starts. This is essentially where I pulled down the analysis we already had, and then you can see the new 4.1 which is like after this, after position which are either omitted or did it wrong when I accepted the changes. Should be the position of the executive c-suite. Security also has [to be raised,] move all relevant budget item responsibilities under the purview of this new position. That’s essentially the only change, and then there's a small change above where I kind of reiterated on the organizational change that we expect to happen with this position being installed. That’s it.

And apart from that, for the whole risk section, at least I have not heard from anyone outside the drafting team kind of giving ideas or speaking to issues with what we have done. So I'm not sure how much longer we should keep that open, or at what point we should consider that one accepted, essentially.

RUSS HOUSLEY: Well, the text has been in front of people, except for this budget part, for a week. So—

KERRY-ANN BARRETT: Russ, I still owe you the sentence.

RUSS HOUSLEY: Yes, you do. That’s right. I saw that in chat but I wasn’t going to call you out. But thank you. And yes, we need that sentence from your action item from last week. So let’s put this on the agenda for consensus call for a week from today. If people have editorial, please bring it to the list or put in a comment in the Google doc.

LAURIN WEISSINGER: And I will take the action and hopefully not forget it with all the moving that I change the first sentence that it’s the position of the executive c-suite security officer.

RUSS HOUSLEY: Okay, so we noticed that Denise is not here to talk about the abuse. Were you planning to, or do we have to wait until next week?

LAURIN WEISSINGER: Essentially, I think we have to wait until next week. I'm not sure if anyone on the abuse subgroup knows more than me, but all I got was essentially meeting cancelled. I'm not sure why. And yeah, that’s essentially where I stand. I know that some people have done their preparations for the response to the comments. And yeah, we have to agree on text, and I guess we just need a new call. I don't know what happened to yesterday’s.

RUSS HOUSLEY: Okay. So what I think we decided in terms of calls going forward is that the DAAR call will happen next Wednesday and that we are going to have a call—although some people will miss it—next week, and that the DAAR call will be essentially directly after the SSR2 call.

Okay. So rapporteurs, please keep things moving. There's a whole bunch of teams we haven't heard from, and we need to bring this to closure by July 1st. Is there Any Other Business today?

Okay, hearing none, I think we’re done, then, for today. Thank you.

LAURIN WEISSINGER: Thank you all. Bye.

JENNIFER BRYCE: Bye.

LAURIN WEISSINGER: Sorry for joining late.

[END OF TRANSCRIPTION]