BRENDA BREWER: Welcome to the SSR2 plenary call number 112 on the 3rd of June 2020 at 14:00 UTC. I would like to do attendance. We have Ram Krishna, Russ, Alain, Danko, Kaveh, Laurin, Norm, and Scott. Apologies from Eric, Matogoro, Boban, Steve, and Denise. Attending from ICANN Org is Jennifer, and Brenda, and our technical writer, Heather. Today's meeting 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: Okay, thank you. First, I'd like to remind all the sub-team rapporteurs, please update the little bar chart we're keeping of the status of each of the groups. I see that some have been doing it and either some have not been doing it or they have not started yet. I'm hoping it's they haven't been updating this.

So, that's the reminder. From the e-mails in the last day, I've found that the risk grouping and the compliance grouping are not quite ready to report out yet, so we will have to come back to them next week. However, sub-team 27 does have proposed text that was sent out in a Word Document a few minutes before the call. So, I know Brenda has it. Put it up.

ALAIN AINA: So, Russ?

RUSS HOUSLEY: Yes?

ALAIN AINA: Okay. So, after we will look at it, the next step will be to put it in the group document. So, can I do that myself, or what you call it, the technical writer will take care of that?

RUSS HOUSLEY: Let's see what changes the team wants, and if this is acceptable then we can ask Heather to do the moving of the text.

ALAIN AINA: Okay.

RUSS HOUSLEY: So, Alain, would you walk us through the changes?

ALAIN AINA: Okay. So, maybe to remind people, from the comment we got … Basically, one of the comments was that we mention one elliptical and we didn't mention the other algorithms. So we had some comment, also, about the fact that the [funding and rationale] was too prescriptive. And also, there was some comment about the fact that the way we … Recommendation 27 one was drafted according to the recommendation said PTI should change to the DPS to facilitate, and people said no, the DPS does not define how, technically, the algorithm rollover was done. Then, the comment was that we should be more explicit on what are we

saying to facilitate. So then, in light of all these comments, the proposal is that we first, because you can see … So, the whole idea was we're moving from RSA to one of the ECC, the ACC algorithms.

So, what I propose here is that I put the reference to … So, please scroll down. Okay. We put the reference to the other elliptical, digital algorithm like [inaudible] and also put the referral that we are not to say that there is an RFC which set the guidance on how the new algorithm should be used because, the crypto world, things keep moving.

So, that is the RFC from IETF who provide the guidance. So, we put this here to say that it is not this SSR2, this review team is saying use this algorithm, move to this algorithm, but there are some technical documents there who give guidance on how to do that. So, that includes the things people think, that this review team should direct or say exactly what to do or what not to. So, these are the new tests, there.

Okay. Scroll down a little bit. Scroll down again. Again, again, to where the change is. On the quantum things. There. So, with the quantum things, there is no change there. They seem to be … There was no consent. But in the Recommendation 27 one, I said … I changed the word "facilitate" to "allow" because the DPS should allow that the root KSK can change, can work, can change in the algorithm and move from "facilitate" to "allow."

And then, [inaudible] put in … In the previous wording, we put "from RSA to ECC, DSA." So, now we make it more generic, saying that, move to another algorithm that provides the same or greater security and preserves or improves the resilience of the DNS. So before, what we

said … Because the focus was on the ECC, DSA, we said that we should move to the ECC, DSA, which gives the same or greater security but also improves the resilience.

So, we changed the wording to [inaudible]. So, we are not directing or specifying any particular algorithm. So, what we want here is we should move to the algorithm which gives the same or greater security but also improves, whenever possible, the resilience of the DNS to say that some of the algorithm, as we're saying the ECC one, they are using a similar key and the signing period is a bit faster than RSA.

These things can also improve the resiliency, so we changed this to make it more generic and say, if we go, so that if we can have greater security but also improve the resilience, then this would be the way to go. So, let's slow down a bit. Slow down. Sorry, scroll down. Sorry. Scroll down.

RUSS HOUSLEY: No, it's the end.

ALAIN AINA: Sorry. I was enjoying it. Those are the main changes here. This has been reviewed by Russ. You can see the red one is Alain, the blue one is Russ. So, maybe if Russ wants to emphasize it a little bit more or in the things …? But I'm happy with the edits from Russ. Thank you.

RUSS HOUSLEY: So, does anyone on the review team have any concerns with the updated texts?

KC CLAFFY: I just want to make sure that the spreadsheet reflects what we did in our response to the comments, and I don't see it in the spreadsheet.

RUSS HOUSLEY: Oh, the spreadsheet has not been updated yet.

KC CLAFFY: Okay.

RUSS HOUSLEY: You are correct.

KC CLAFFY: And then, the other question I have is, did we check …? Because I think SSAC published something on this topic in the last six months. Did somebody check that? I might be wrong. I know they talked about quantum stuff. I'll go check, but I just wonder if anybody's aware of it. If not, I'll go check and make sure. Here, a comment. Oh, never mind. I guess it was a comment to NIST. Here, I'll send it. Put it in the chat. I don't have any other comments.

RUSS HOUSLEY: I found something that led to SSAC comments on ours. Report has something to do with quantum in it. And I found SAC109, which I don't know it thinks it's part of quantum, but that was the DoH and DoT stuff.

KC CLAFFY: Right. Well, there's 107, which was a comment to NIST on quantum crypto algorithms. I think it's only obliquely related but I want to make sure that one of you guys looks at it because I haven't looked at this in detail. Just be aware of that one.

RUSS HOUSLEY: I will take the action to look at 107.

KC CLAFFY: And then, sorry, also 108. SSAC comments on the IANA proposal for future KSK rollovers. I just want to make sure we're not making a recommendation that SSAC and ICANN are likely already going to do.

RUSS HOUSLEY: Well, or if we do we point out—

KC CLAFFY: Yes.

RUSS HOUSLEY: Yeah, sure. I'll look at those.

KC CLAFFY: Thanks.

RUSS HOUSLEY: It's quite possible that they came out after we did this initial work.

KC CLAFFY: Right. 108 was January.

RUSS HOUSLEY: Yeah, this was certainly done before that.

KC CLAFFY: Right.

RUSS HOUSLEY: Okay. So, any other comments on the proposed changes? All right. We'll bring this back next week with a report on whether 107 or 108 has additional changes, and we'll … Alain, would you take the action to put the responses into the public comment spreadsheet?

ALAIN AINA: To put what? The response, or to update the text?

RUSS HOUSLEY: So, what it says in the spreadsheet, all the public comments are there, and which sub-team is working on them. And then there is, over on the right-hand side, how the document was changed. It's a summary of the change.

ALAIN AINA: Okay.

RUSS HOUSLEY: So just “how was the comment handled” has to be added in the spreadsheet.

ALAIN AINA: Okay. Now it is clear. Okay. I will do that.

RUSS HOUSLEY: Thank you. Okay. I'm unaware of any other sub-teams that are ready to report out. At least, it didn’t get an e-mail from the rapporteur. Is there any sub-team that is ready that I didn’t know about? Okay. Right before this call, Boban sent a note to the team list suggesting that we might make more progress, instead of working in these sub-teams, if we did it on a big call.

My experience earlier when we tried to do that with the team comments was it was very slow-going and long silences. The hope was that the sub-teams working in parallel would be faster. What do others think?

KC CLAFFY: I'm hesitating because I'm not sure what to say, because everything seems slow-going no matter what we do. I think people are just quite not motivated, or many other things competing with their time. I maybe had some of both, myself. I finished … The ATRT thing, which was sucking my

time, is now done. So, I will definitely have more time for this now. I don't know if that's going to help with my motivation when I see nobody else doing anything.

I will say I went through, finally, the public comments for Recommendation 13, which I got assigned to my sub-team, and I found a few things I don't understand in the comments. But I assume that's something I should be handling with the sub-team?

RUSS HOUSLEY: Yes, that was my hope, those kinds of things, even if we said "don't understand the comment" as the team's response.

KC CLAFFY: Yeah. I'll go ahead and send it by e-mail. I actually thought today was a sub-team call. So now, I guess, does the sub-team call wait until next week?

RUSS HOUSLEY: No, sub-team any time you want it.

KC CLAFFY: Yeah, okay.

RUSS HOUSLEY: yeah. But that was the whole point: only the sub-team's calendar should effect when you can be …

KC CLAFFY: And I'm not seeing my sub-team on this except for [Brian]. Laurin.

LAURIN WEISSINGER: Hi, everyone. Yeah. So, abuse team needs a call. We haven't scheduled one yet. I can speak to the rest, though. So, essentially, we went through all the comments. We decided on actions and edits. Some of the edits have already been made. I think we're looking at Friday to come together, discuss text. So, we should definitely have a good chunk next week. It looks like right now, so that is fine.

With the abuse stuff, as I've said before, and that KC can surely confirm, it's just an insane amount of work. So, we have broken things up. Some comments in the table have been [inaudible] for the next team call but we do have to do that. With risk, I'm pretty confident there will be something.

KC CLAFFY: I mean, I don't know about you, Laurin, but I would be in favor of some deadlines, some forcing function from the leadership. Because I didn't look carefully at the blog entry that said, "Now, we're not due until October," but October seems far away to me and I don't know if I can keep doing this until October.

RUSS HOUSLEY: Hey, I'm fine if you finish early.

KC CLAFFY: Yes, exactly. But it's really … And again, I know this isn't the first time this has come up, but this is not working as far as I can tell. And I know I'm part of the problem, so as of today I will be less part of the problem. But I should bring your attention to the fact that the ATRT report has come out, now, and their most prominent recommendation is to, basically, kill all of these reviews.

Although I objected to that recommendation, I am sympathetic to it because I just think this three-plus-year review episode is not, I think, what anybody had in mind, including us. But I think we need to do a little bit of self-reflection, here, if we're going to continue to be part of this problem or try to be part of the solution by moving on from this dysfunctional episode. So, anyway, enough whining. I'll do what I can.

RUSS HOUSLEY: What I'm not getting from what you're saying, KC, is whether you think working in parallel in sub-teams is better or having a big, marathon, dedicated day and just go through them is going to be more productive.

KC CLAFFY: Well, the reason I'm not giving you an answer is that I think you've tried both and they have both failed.

RUSS HOUSLEY: Yes. Thank you.

KC CLAFFY: Yes. Again, I'm sympathetic to it, now. We could try what ATRT did, and it had its strengths and weaknesses. They did do the marathon. They did, in fact, about four hours a week. They had two two-hour phone calls every week for months, after the pandemic started, to try to bring closure to this.

Now, again, they were on a deadline. They were, by bylaws, required to be finished in a year. I think it was a year. And it took them a little longer. They didn't make that deadline because of the pandemic. But they had a very aggressive schedule and, still, they had to sacrifice a lot of topics in order to get done with that schedule. But I think it suggests—and especially given the diffuse nature of many of these recommendations—we're not going to finish unless we have a schedule that forces it.

I would also say I personally think some of these recommendations … Since I'm maybe of a mind more than most to get rid of many of these recommendations in order to make the document shorter … And again, I'll draw your attention to the ATRT, which ended up with five recommendations.

Now, there are sub-parts to those recommendations but they were very much motivated to try to not be part of the 300-plus unattended recommendations in the community. So, I'm in favor of if Russ would put a deadline, and if we don't have feedback or revision by that deadline we drop the recommendation, because people just don't care enough about it to do the work. So, there. I gave you a path forward, Russ.

RUSS HOUSLEY: Oh, okay.

KC CLAFFY: You pushed me and I gave it to you.

RUSS HOUSLEY: I did push you. And now, I'd like to hear what other people think about your proposal.

LAURIN WEISSINGER: Yeah. So, from my perspective, there is just so much you can do. I'm currently half-focused strongly on risk stuff and I cannot do all of this at the same time. I do have other work to do and I think that is what affects most people.

As I said, with risk, I'm pretty confident we will have something to talk about next week. But I do also see KC's point in that we need to create deadlines. What I could see is maybe that we do staggered deadlines. So we say, "Okay, by then in the table you have to have reviewed and responded to all the comments. By that deadline, you should have draft text. By that deadline, we should discuss draft text," something like that.

Also, to keep in mind that, at least the teams I see, there is progress. It's just sometimes difficult to keep going because things are just part of schedule, or there is no time in that week, or whatever else.

RUSS HOUSLEY: Anyone else? Not seeing any hands. Okay. I guess, Jennifer, would you put this on the agenda for the leadership call on Monday?

JENNIFER BRYCE: Yes, I will.

RUSS HOUSLEY: We'll bring a recommendation back to the whole team next week.

JENNIFER BRYCE: Sure.

KC CLAFFY: Russ, can you send the recommendation out in e-mail? I'm nervous about the number of people on this call.

RUSS HOUSLEY: Me too.

KC CLAFFY: Although compared to ATRT, it's a higher percentage of the team. It's still under 50%, maybe.

RUSS HOUSLEY: I understand and I will send your recommendation out and ask for comments on it.

KC CLAFFY: If … Okay. Never mind. I'll take it to the SubPro.

RUSS HOUSLEY: No, the idea is to … What I would like to do is get those comments before the leadership call on Monday so that we have that input to consider for the people who aren't here. Okay? All right. Is there anything else we need to talk about today?

KC CLAFFY: I guess I'll just ask one question that I should ask on the sub-team, but I'm afraid that the sub-team won't know, and then I'll have to come back here, because it has to do with Europe. It was a comment by the WIPO on UDRP cases. Here. I'm going to actually put it in the chat because it's too long to read. But it references, "Please have the SSR2 go look at what EU and Denmark are doing."

Hold on. I can't find the damn window that I'm supposed to paste in. Here we go. And so, I bet somebody on this call knows, and I do not, what they're talking about. I actually didn't understand half of this comment.

"The continued availability of the UDRP as operated by WIPO on a non-profit basis benefits contracted parties by keeping them out of dispute. So, the fact that WIPO is seeing record-breaking numbers of UDRP cases illustrates the root issue of cybersquatting as not being addressed."

I didn't even know that we're seeing record-breaking numbers of UDRP. Can somebody who knows more about this than I do … Or are those

people not on the call? And then it says, “Look at programs in the .EU and .DK [domain spaces].” I need someone to find out what those are for me. Maybe Heather, if nobody else knows and we have to actually have to go dig around.

LAURIN WEISSINGER: I don't know about this myself but I do know a number of tech law and IT people. So, if you send me the text, I can try to reach out to these academics, see what they have on that, if that’s of interest.

KC CLAFFY: Okay. Yes. Okay. And then, one more, which is for ICANN Org, so maybe Jennifer could take this back, is that … Whoops. Did I just send that? Oh, God. I just sent that to somebody privately. What the hell? I didn’t mean to send that to you. Sorry, Norm. Here, let me send this. Clearly, I don’t even know how to use Zoom yet.

Okay, that’s the one. And then, here’s the one from … So, ICANN Org responded to one of these recommendations about DAAR with this comment saying, “Well, we’re already doing stuff. Can you tell us what you’re trying to get us to do beyond what we’re doing? Give us details.”

And so, I would like details from ICANN Org on what it is that they’re doing and, actually, how they’re measuring the effectiveness of what they’re doing. Because I think part of the comments and what we got from the … I'm sorry. I'm going into sub-team space, now, but what the hell? I’ve got time.

The comments that we've seen from the community are, "Yes, we agree with you." So, I think it is incumbent upon us to say something but I certainly do want to be aware of what ICANN Org is already doing. It has been long enough, and I actually found it vague enough when we got a report from ICANN Org to not understand how far what they're doing is going to go toward what we're recommending. Okay. So, that was …

RUSS HOUSLEY: With that one, KC, I think Steve can help you connect, but he could not make the call today.

KC CLAFFY: Yes. Okay, fine. Okay. I'll take that to him.

STEVE CONTE: Ha, surprise! Here I am.

KC CLAFFY: Yay.

STEVE CONTE: I literally joined about five minutes ago. Thanks for that.

RUSS HOUSLEY: You told me you couldn't make it.

STEVE CONTE: Yeah, and then my other call ended sooner than I thought so I decided that I was going to spend the morning with you guys.

RUSS HOUSLEY: Well, thank you.

STEVE CONTE: KC, we're happy to talk about it. I had offered out to the review team a number of times that John Crain is more than willing to come and discuss with the review team, or the sub-team, or whatever. Because I do recognize that, when we did our first presentation on DAAR, that was four years ago, now—three-and-a-half years ago—and it was in its infancy. It was just starting out. And now, we've had some real-time running of it. So, if you or that specific sub-team would like to have that conversation, I do encourage it. I could certainly work with John and make that happen.

KC CLAFFY: Yeah. Although, I think it would be better to have something written that we can point to. But maybe both would be good because I think we should cite it in the report, what we're aware of that's already happening. Okay. The rest of my issues, I'll just take to the review team. Thanks, Steve.

Oh, one more thing. What is PPSIA? Does anybody know? That had to do with Recommendation 14. Okay, nobody knows. I'll go look it up. It was in response to this pricing recommendation, number 14.

"Part of any meaningful look at pricing would look at data accuracy under the 'know your customer' norms, which would call for a tiny resolution of PPSIA independent of ePDP work." I didn't know that acronym. Okay.

And then, there's one last thing, that a couple of these comments, as I was going through them, refer to … Especially in the registry side, they basically say, "CCT also recommended that SSR2 …" They're talking to SSR2. "SSR2 made a recommendation. We echoed CCT." And the comment says, "We already said that was a bad idea when CCT recommended it. We still think it was a bad idea. Please go see our comments from that."

It would help if Heather or somebody could go dig out those comments because, if indeed we are making them knowing that CCT made them, industry objected, ICANN sort of deferred to industry and said, "This has to go through PDP," then we have to acknowledge why we are making them again and why we would expect anything different to happen now. So, it would help to know exactly what their objections were. That's it.

RUSS HOUSLEY: Jennifer, would it be possible for you to pull the pointer to the CCT comment?

JENNIFER BRYCE: Yeah, sure. And I can see what other information I can find on that that might be helpful.

RUSS HOUSLEY: Okay, thank you. Okay. I'm not hearing anyone else. I don’t see any other hands. All right. Thank you. We’ll talk to you next week. Bye-bye.

LAURIN WEISSINGER: Thank you, all.

JENNIFER BRYCE: Thank you.

[END OF TRANSCRIPTION]