JENNIFER BRYCE: Pamela or Yvette, would you mind doing a roll call, please?

YVETTE GUIGNEAUX: Sure, Jennifer. I'll go ahead and do that. Hi, everyone. This is Yvette in the room. Welcome to the SSR2 Plenary call on March 18th, 14:00 UTC. We'd like to remind you this meeting is being recorded so please state your name before you do your comments. Joining us for today's call from SSR2 is Eric, Alain, Danko, Kaveh, Laurin, Russ, and I believe somebody else just joined us.

JENNIFER BRYCE: KC.

YVETTE GUIGNEAUX: Hi, welcome. From ICANN Org staff we have Pamela, Jennifer, Steve Conte, and myself, Yvette. We also have our [inaudible] provider, Heather, as well. And welcome, Zirko from SSR2. He just joined us, as well. If anybody has any questions on the expected standards for behavior or anti-harassment policy we can post those in the chat, as well. I believe that's it from me. We don't have any observers or anything else so I think that's it from me. Russ, I will go ahead and turn the call back over to you.

RUSS HOUSLEY: Okay. Thank you. I wanted to make sure that everyone saw the cancellation of the face-to-face meeting in April. I don't think it's coming

as a surprise to anyone given all the travel restrictions and other things going on. We did not pick an alternate date to Doodle for. We want to see when travel for all of us will be safe and when we start getting a window where that might be true we will set up a Doodle to pick a time to do the face-to-face.

In the meantime, we thought we would continue to go through the document and resolve as many of the comments that we have. Next on deck is the public comment will close toward the end of this month, and then we will start dealing with those. Hopefully, we will be able to do that in a more expeditious way than we have been dealing with these. We'll just to see what those comments bring.

So, thank you to Naveed. I don't think he's actually on the call but, on the call last time, he took the action to rewrite the findings related to recommendation four and he did that and he put it in the document. I know I had some comments on it. Maybe others did, too, but I think that's probably the place to start to resolve that open issue from last time. So, I'm trying to find what page it's on.

JENNIFER BRYCE: 27.

RUSS HOUSLEY: Yes. That begins at the top of page 27. So, if we could put that up in the Zoom screen. Others don't have it up on their own screens. So, I think deleting the text that was there does resolve a bunch of the comments but let's take a look at this new text. Please let us know if there are any

concerns. Laurin, was your comment in there about the original text or the new text?

LAURIN WEISSINGER: Hi, Russ. I believe old text. I cannot see the comment right now.

[JENNIFER BRYCE:] It was the old text. Laurin made his comment on February 24th. The new text was added March 10th.

RUSS HOUSLEY: Okay. Thank you. Then I guess my comment which was, “Can we combine section 4.4 or the part of the recommendation 4.4 and 4.5?” They seem to overlap quite a bit.

HEATHER FORREST: Russ, I'm unclear as to what you want to merge because what you just said doesn't quite match what your comment said.

RUSS HOUSLEY: Okay. There are so many comments here, finding which ones line up is so hard.

HEATHER FORREST: Yeah, right. If you click on what’s highlighted the comment will move to be next to it.

RUSS HOUSLEY: Ah, okay. We merge.

HEATHER FORREST: Can we merge 4.4. with 4.2?

RUSS HOUSLEY: Yeah.

HEATHER FORREST: And then with 4.5 it's, can you merge that with 4.3? So, I don't think you wanted to merge 4.4 and 4.5, I think you wanted to merge those up into the other recommendations.

RUSS HOUSLEY: Yes, I did.

HEATHER FORREST: Okay.

RUSS HOUSLEY: There just seems to be quite a bit of overlap, there.

HEATHER FORREST: If there are no objections, I can take it as an action item to do that.

RUSS HOUSLEY: I'm not hearing any objections but Naveed isn't here either. Could you do that in suggest mode so that we could put it back if when he sees it he has a concern?

HEATHER FORREST: Of course.

RUSS HOUSLEY: All right, thank you. But there are a bunch of comments here that can be marked as resolved. Okay. Moving on. I think that brings us to Work Stream 2. I can't remember how far we got into this.

HEATHER FORREST: I think since we stopped at SSR2 recommendation four on the three-hour call, I think that we're actually at recommendation five, with the first comment being from Laurin, who wondered about the impact of this recommendation. There is also a long-term action item about potentially merging this into the Work Stream 2 recommendation on risk management, and that was assigned to Boban.

RUSS HOUSLEY: So, Laurin, can you talk to …? It seems to me the team was pretty strong on there being a C-level position here. I do understand the reason for the merging because we want the C-level person to be responsible for the risk management and the other activities we talk about in section six.

LAURIN WEISSINGER: Yes. Going back to this, we do have a lot of work on risk. Essentially, there is this one, rec five, which relates to SSR1 recommendation 27 where, essentially, I was thinking about, "Well, is this better served in moving where all this other stuff is?" and just make a note here to say, "Yes, we took this in. We'll talk about it later, just from a structure and logic perspective."

The other issue I see is, going back to my comment from February 24th, that we actually said the 15/16 was okay. So, right now this is so high-level that I'm not sure what I would do with it, right? Essentially, risk management framework should present like a strategic comment. Okay, that sounds good. You could argue that is already happening. The articulation, I think KC has mentioned that: "Well, to what extent is this actually possible and should be done?" is a good question.

Essentially, my feeling with this one is this all sounds good, if nothing wrong with it, but we're lacking what needs to change materially. Really, what is wrong with it? What do they need to fix? That doesn't come out of this text, at least not for me. This is where my comment is stemming from, and I think KC had another one on February 3rd where she also said, "Yeah, what is missing? What are we saying needs to really, fundamentally change?"

RUSS HOUSLEY: So, Laurin, I'm just trying to understand. Are you saying that we say all of that later when we talk about it in Work Stream 2, and therefore this should just be merged, or are you saying something else?

LAURIN WEISSINGER: So, I'm saying what is in here should be merged, in my opinion, yes, And number two is that, essentially, I feel like it's a bit too wishy-washy. The thing is, if I was to take this, I am now on staff and I get this recommendation to implement, what do I do? It is in no way smart to come back to my typical criticism. I don't know what I should do.

KC CLAFFY: Especially since the last paragraph of this recommendation seems to contradict it. It says, "Risk management activities including the framework and the SSR report as assessed by the team where comprehensive and appropriate." If that's the case, why is there anything in here?

LAURIN WEISSINGER: Yeah. So this is exactly … Sorry, KC. I hope you were done.

KC CLAFFY: No, go. Yeah.

LAURIN WEISSINGER: I said in the beginning as well, we said 15/16 was okay, so what's our problem?

RUSS HOUSLEY: So, what I hear KC arguing is we should even have said that recommendation 27 was fully implemented.

KC CLAFFY: You know, this does leak into where Russ had just started with Work Stream 2 because in Work Stream 2 we say we need a C-suite, and that's more or less centralizing something about security, which is what we say here, that risk management should be centralized and strategically coordinated, which I don't think I disagree with. But to the extent that there is a rationale for that recommendation, it is down below in Work Stream 2, where Russ alluded to, that maybe we should be folding this in.

I think when we get to that in a few minutes, hopefully, we have the same issue, really, which is we hadn't concretely identified the problem. Well, we have sort of identified the problem that we're trying to solve there. We have said that there is some aspect of security that's managed on this side of the org and there is some aspect that's managed on this side, and centralization would be good, we should say. It's hard to do all this in a decentralized manner.

But we haven't really pointed to a problem. Maybe that's hard because maybe some of us learned it under NDA or something, but we haven't really pointed out a harm that is happening because ICANN has chosen to do it another way.

So, I think that is the same issue with here. What is the harm that has happened? What is the problem that we're trying to address by saying the risk management framework should be centralized? If it's part of the same reason we're saying there needs to be a C-suite/a CSO, yes, fold it

in. Whether that means the SSR1 wasn't done enough, I'd have to go back and look at the spreadsheet someone filled in to say, "What is the gap between now and what we would consider being done?" But yeah, it's definitely not clear from this text.

RUSS HOUSLEY: Yeah. KC, the spreadsheet says "see recommendation five."

KC CLAFFY: Yeah. Okay, great.

RUSS HOUSLEY: Sorry. I just didn't want you to waste your time.

KC CLAFFY: Thanks for saving me time, Russ.

RUSS HOUSLEY: Yeah.

ERIC OSTERWEIL: Down below, the same references look at our discussion on SSR1 recommendation 27. I'll note that that begins on page 118. What the discussion there seems to outline is that something is in place, but to meet implementation, the recommendation, there is a lack of specificity or something like that.

So, I think maybe this conversation should dovetail around that description makes sense, and then whether it does or it doesn't this discussion up above should be updated to match what's down below. Because down below, basically, yeah, it's done, but it says, "Specific guidance regarding the additional action, blah, blah, blah."

The review is still relevant but it was difficult to assess whether this recommendation has been fully implemented, basically because of language. So, I think if we want to try and find harmony in what we were trying to get at, it's probably important to look down at page 118.

LAURIN WEISSINGER: Thanks, Eric. So, this is what I did, as well, scrolled down. And as you said, it's a lot about, "Okay, look. There is no proper definition from SSR1," etc., etc. So, my proposal would be fold this into the CISO and say, "This is the person who should be responsible for this and who should, as we do in this space, develop a proper system, a framework, and centralize it," because I think that is actionable in that, hire this person, and put risk management for security under this person, and then implement it according to appropriate practices, standards, etc.

So, I think that would be much better than this really long, unclear recommendation because that can be put in a sentence. That's what I would say we do.

RUSS HOUSLEY: So, Laurin has proposed, essentially, merging recommendation five and six. It's unclear to me what you're proposing we say about SSR1 recommendation 27 in that. Go ahead.

LAURIN WEISSINGER: I would just say we just make a note of some sort where we say, "We identified a problem here. We addressed this problem elsewhere," something along those lines.

RUSS HOUSLEY: What I've tried to do here is to make sure we don't have that kind of fuzziness because the table now says either, "What needs to be done to go from where we are to fully implemented?" or it says, "It's subsumed by one of the SSR2 recommendations." And so, I'm looking for one of those two things.

LAURIN WEISSINGER: It would be subsumed, I would say.

RUSS HOUSLEY: Okay. So, you would basically say, "SSR1 recommendation 27 is subsumed by the merger of five and six"?

LAURIN WEISSINGER: I think yes. I think that is what I'm saying. Let me see. What is six? Six is the CISO, right?

RUSS HOUSLEY: Yep.

LAURIN WEISSINGER: Yeah, exactly. Done! That's what I would say.

KC CLAFFY: Yeah, I would agree with that. Again, the more recommendations we can merge into something that gets outsourced to some security firm that does this sort of security/strategic planning for ICANN. And we want to say, "Metrics of success of that exercise would include, we believe, centralization of CISO, strategic plan with actual metrics, timeline," but get it out of that it's something that is SSR2's responsibility to fully flesh-out, because we can't.

RUSS HOUSLEY: Yeah. Okay. Does anyone have concerns with the approach that has just been articulated by Laurin?

KERRY-ANN BARRETT: Hi, I have just one. Just to caution that with the mergers and shifting the logic flow of how the recommendations were [reformed] would shift a little bit.

RUSS HOUSLEY: Yes, it would.

KERRY-ANN BARRETT: I just want to make sure that in doing this shift, if we're going to do a second pass-over to make sure that, logically, the recommendations now flow [on in together] or if we want to now think about what is connected between the merges that we've done because the preamble would change, the context would change, and it would affect the other recommendations that had SSR1 linkages.

If we do this kind of change to the logic, when someone reads the entire document it would be shifted as well. So, my caution would be that while we're trying to consolidate just keep in mind the overall frame that we came up with in making sure that persons understand that we address SSR1. We have some linkages with SSR2. We have a table that tells you how to complete SSR1.

These are further recommendations just to strengthen the positions that we found lacking based on our own assessment. So, just try to ensure that as we shift, and merge, and try to consolidate, that that is captured, and whoever is doing that, just to make sure that we have assigned someone, a groups of someone's, to make sure that's done.

RUSS HOUSLEY: I think that is an important thing to remember. It really is about readability but I think we have to get the content down, and then if we end up reorganizing to deliver that content, so be it. Although, Heather will pull all her hair out, at any rate. Laurin, are you willing to write the merger?

LAURIN WEISSINGER: Yes.

RUSS HOUSLEY: Okay. Jennifer, that's the first big action item.

JENNNIFER BRYCE: Got it. Thank you, Russ.

RUSS HOUSLEY: Yep. So, I believe, then, we skip down to recommendation seven, since Laurin just took an action that will involve rewriting six. So, I believe we're now on page 33. So, I see a bunch of adds and deletes from Kerry—I think those were just to make it more readable—and that we get to a comment from Laurin, "Why not contracted parties?" I can't quite figure out what text he's pointing to. [cross talk] Oh, that's back in six.

HEATHER FORREST: Hi. Russ, you really should just click on the word that's highlighted. Just don't try and track the comments along the sidebar, just click on the word so that the comment you want is right there.

RUSS HOUSLEY: Okay. So, we are then at KC's comment, "Which objectives?" which is part of 7.1, "Align strategically against the requirements and objectives of the organization." I think we have a table, now, that answers that question

but I think the recommendation is actually broader than that, to say that this activity is supposed to be aligned with the strategic plan. As it changes over time, this security risk framework should be revisited to make sure it's aligned with that. Am I wrong?

[YVETTE GUIGNEAUX:] KC's still waiting for the table. Where is the table that says "what objectives"?

RUSS HOUSLEY: Oh, that's in a different Google Doc, of course.

[YVETTE GUIGNEAUX:] What problem are we trying to solve, here?

RUSS HOUSLEY: This one, if you had the readers digest it, it's we want the risk management to be done in accordance with ISO 31000 and externally audited.

[YVETTE GUIGNEAUX:] Then why do we need …

RUSS HOUSLEY: I mean, that's, to me, the high level. There are a lot of words, here.

[YVETTE GUIGNEAUX:] Yeah. I don't understand why this isn't also folded into 5.6 because five was about risk management framework, wasn't it?

RUSS HOUSLEY: It was.

[YVETTE GUIGNEAUX:] And six would be one thing that might come out of a risk management framework if you went and asked somebody else for advice on how to do it, so why can't this whole thing be "go get a real risk management framework developed by professionals"? And do we need all the sub-pieces of it? Do we not believe that a professional would recommend all of these sub-pieces? And if we do, then let's just outsource this to a professional.

ERIC OSTERWEIL: There are a whole bunch of meta-comments in here and this is one of those things that we had talked about off the recording a couple of times and I just want to maybe use it as a poster child or a strawman for why iterative consolidation loses signal. Yeah, we could fold this in under the thing that we're talking about reporting, and we can fold that in under C-suite because that would make sense, and then we could fold the risk management under the C-suite and say, "Anybody who is any good should just figure this out."

But I think, sort of paraphrasing what KC just said, the motivation that prompted this was a very specific instance in which things weren't being handled properly by "professionals," and so we very much wanted to

recommend something very specific because there was a problem that we found and it was a really big one.

But as we continually fold things into each other, the recommendations become more and more diffuse. I just want to, again, be true to form and say I think combining recommendations is something we should do very judiciously because while we could say, "Yeah, at a high enough level everything's SSR. Why don't we just have their recommendations? S, S, and R." That kind of would defeat the purpose and I worry that, while that sounds really good, we're getting closer and closer to that.

So, this particular recommendation was talking about things that need to happen because we observed that they are not happening this way and that we observed an actual, real, serious problem as a result. So, I'm more than happy to expound further on that, but hopefully I put that down for everyone to think about.

LAURIN WEISSINGER: My proposal would be the following. If we take number five, get rid of that one, then we put the risk management under the CSO, CISO, whatever-person, then essentially … Oops. Wait. I have to scroll back up, sorry. Then "position responsible for strategical and tactical security," that would move into five, so it would be a function of the centralized security person. They can hire someone else and can do it themselves. I don't think that is our problem. That this person should be qualified, that would go without saying. In the above, I'm happy to also put these two or three words in there.

6.3 would be kind of … So, what I'm trying to say is, why don't we put the responsibility for risk into the CISO and then we just use the next recommendation to be clarifying what this person should do. So, that would be …

RUSS HOUSLEY: Laurin, I think we already do that. If you read 7.3.3—

LAURIN WEISSINGER: Yes. To some extent, yes.

RUSS HOUSLEY: Right. We already say this risk needs to be managed differently than it is.

LAURIN WEISSINGER: Yes.

RUSS HOUSLEY: And it needs to report to that C-suite position but it needs to follow ISO 31000 and it needs to feed the business continuity and a faster recovery, which come later, and the information security management system needs to take advantage of the …

LAURIN WEISSINGER: Yes.

RUSS HOUSLEY: And so, it's those linkages that we're trying to make recommendations about here.

LAURIN WEISSINGER: Yeah. No. So, Russ, what I'm trying to talk about is a bit more … I think we just need to pull those together and rethink this story. I think there are a lot of superfluous facts there, at the moment. This is what I'm trying to say.

RUSS HOUSLEY: All mystery novels have superfluous facts. So, how do we get from where we are to the recommendation seven that marries well with what you're rewriting for 5.6? I think we have to see what you write before we can have somebody write this one.

LAURIN WEISSINGER: Yeah. So, I think, essentially, I made a quick note in there so that I don't forget it. We would want a CISO, CSO, whatever, to be in charge of this kind of function. This should report to this person in some way, shape, or form.

And then, I think we can just say, "Okay. 7.1 can stay," and then, essentially, we can cull two considerably. I think 7.3.1 is fine. 7.3.2 is essentially a result of doing 7.3.1. And then, 7.3.3. I'm not sure if that is relevant because it's like, do they have to appoint a dedicated person? No. They could, essentially, contract this out to someone and that gets reported to the CSO. So, I'm not sure if that one is actually that useful, because it limits what they can do.

RUSS HOUSLEY: Well, I think what matters is that the C-suite position has the overall responsibility—

LAURIN WEISSINGER: Yes.

RUSS HOUSLEY: —For risk management, business continuity, and disaster recovery—

LAURIN WEISSINGER: Yes, exactly.

RUSS HOUSLEY: —Who is responsible for implementing the ISMS.

LAURIN WEISSINGER: Exactly.

RUSS HOUSLEY: So as long as we say those things, I'm comfortable.

LAURIN WEISSINGER: And then I'm thinking, can this [call back]? Yes, okay. So, what I can offer is, let me try to do this. I will take in seven and so a bit of fiddling around

with that one as well. I'll just put it in suggests that we can discuss next week.

RUSS HOUSLEY: Okay, Jennifer. Laurin's going to rewrite seven, as well.

JENNIFER BRYCE: Thank you.

RUSS HOUSLEY: Laurin, make sure the findings chime with what you come up with.

LAURIN WEISSINGER: Oh, no. It is mainly cutting and rearranging text, I think.

RUSS HOUSLEY: I understand. I'm just saying, let's not [let this get to] the situation where we have a recommendation and findings that are about something else.

LAURIN WEISSINGER: Yeah.

RUSS HOUSLEY: Okay.

JENNIFER BRYCE: Russ, Steve has his hand up.

RUSS HOUSLEY: I'm sorry. I can't see both screens at the same time. Go ahead, Steve.

STEVE CONTE: Thanks, Russ. I think the conversation is healthy and I think that it's good to work this out. I just want to bring to light to the team that we are currently in a global crisis and we are flexing and managing ICANN's risk and ICANN's business continuity. We're on a full travel ban. We're entirely remote at this moment, and yet business is operating as usual.

So, as you rewrite I ask that you utilize—God, I hate to say it this way—the opportunity that is taking place right now to observe how ICANN is managing risk and is conducting business as usual, and everything else, and please take that into consideration as you rewrite this because we're actually in an operational phase and not a theoretical phase at this point, and I think it's worth noting. Thank you.

[YVETTE GUIGNEAUX:] Good point.

RUSS HOUSLEY: I agree that we are in one kind of crisis and it is being managed. Canceling the meeting was absolutely prudent, and so on. A different kind of crisis also needs to be part of the business continuity, risk management, the faster recovery. I mean, a natural disaster that takes out one of the

DNSSEC roots or something, one of the two facilities where the key is stored, those kinds of things.

So, yes, I totally appreciate what you're saying but we're in one vector of a kind of a crisis and hopefully we won't see more than one vector executed at the same time. But you're certainly correct, we ought to say something when we're on the end. Heather, could you put a place in the findings regarding the business continuity part, where we could say, "Make some observations about the Coid-19 handling?"

HEATHER FORREST: Of course.

RUSS HOUSLEY: Hopefully, we'll be able to write that in hindsight.

HEATHER FORREST: Might be nice.

RUSS HOUSLEY: Okay. Anything else regarding seven? Yes, it looks like Boban had a question regarding 7.2, regarding who assesses the success of these measures. In the way we're asking this to be externally audited, is that it, or is it …? The answer should not be SSR3, right? Laurin, do you have an answer for this that would be affected by your rewrite?

LAURIN WEISSINGER: Not really. Maybe.

RUSS HOUSLEY: I'm just concerned about the silence.

ERIC OSTERWEIL: I just want to say again that I'm very apprehensive about rewriting this recommendation, considering the hefty amount of subtext that went into crafting what's there.

RUSS HOUSLEY: Who do you think should assess whether the measures regarding the risk management are successful or not and how these measures are assessed? If we ever wrote anything about that, I don't recall it.

ERIC OSTERWEIL: So, 7.2. This is what we're talking about, right?

RUSS HOUSLEY: Correct.

ERIC OSTERWEIL: So, I might be misreading it but it says, "ICANN Org should describe relevant measures of success and how these measures are to be assessed." In other words, I think what this is saying is ICANN Org should say, "This is what we think is important and this is how we think it should be assessed." I might be misunderstanding but if I read that sentence

correctly it's saying, "There need to be stated intentions [at this whole] thing. We're going to do this and this is how we're going to measure it."

RUSS HOUSLEY: Okay. So, you're saying we are recommending self-assessment?

ERIC OSTERWEIL: Published policy about what will be assessed. In other words, we're saying, "You should tell us what you're going to do and how you're going to verify you've done it." I think that's what it's saying.

So, no, I'm not saying they would be self-assessed. They might say we're going to be audited, but they're saying, "We're going to do great justice, and the way we'll define justice is this thing, and the way we'll find out if we're done good justice is we'll ask Judge Judy."

It's sort of like someone can say that sounds like shenanigans but at least it's a stated policy on what's going to happen. So, I think that's all this is saying. I could be wrong. I'm just reading it real-time but that's what it looks like to me.

RUSS HOUSLEY: So, your point is that the result of the assessment, however it's performed, needs to be public? That's your point?

ERIC OSTERWEIL: Okay, what I'm saying is sort of like we are going to follow the following audit framework. We are going to follow the following risk management

framework. In order to ensure that we followed it correctly, we're going to contract with one of the big four auditing firms. That would fulfill that.

Someone else could say, "We are going to come up with our own custom way of evaluating whether we've done a good job or not and we're going to ask a friend of ours to tell us if we did a good job." That would also accomplish this.

But the fact that they've stated what they're planning to do, then someone could say, "I want to make a public comment. I want to raise a flag," but they've had to state, "This is what is going to happen and this is how we're going to verify we did a good job." This is not telling them how to do it, it's telling them they have to tell us, the community, how they're going to do it.

I think this recommendation is specifying that you can't just say, "We're doing a good job. Don't look over here." You have to tell us what you think a good job is and how you're going to verify that you accomplished your good job. You have to tell us, the community. That's what I think this recommendation is saying.

LAURIN WEISSINGER: I think I agree with Eric on this one, as well, where it's, yes, we essentially need some form of—I don't know how to call them—methodology baselines. There needs to be some kind of report on this. All of this makes sense. We might be able to make this a little bit clearer and more succinct but I think the point is, there, we just might have to edit the text a little to make clear what we mean here.

But we put the burden on Org here completely to say, “Well, define this, tell people what you’re doing, and then figure out how you measure against these objectives.”

RUSS HOUSLEY: Okay. The next comment comes from KC. She says, “Why is this not part of SSR1 recommendation nine? I don’t see a clear difference,” which is the one that calls for information security management systems and security certifications. I didn’t think these were the ones to be merged. I thought the ISMS-related one came later.

KC CLAFFY: In all cases, it’s not clear to me what is the problem that we’re trying to solve, and what is it that ICANN is not doing, specifically, that we want them to do? I feel like all of this, if we really think there are unprofessional things going on from a security perspective inside ICANN, we should say we’ll get professional guidance on how to do this and not pretend that we, as a bunch of volunteers, can fix the problem.

LAURIN WEISSINGER: This is really very high-level. I'm not sure if this is actually a solution, I just want to throw it out there. We seem to have a lot of problems with our SSR1 follow-up to our own recommendations. So I am wondering, do the negatives here actually outweigh the benefits? What I'm saying is, it might make sense to look at these again, define the issue areas, then we reorganize the text alongside these issue areas in a logical manner, one

after the other, and then we put the “this is an SSR1 follow-up” somewhere as a note, instead of trying to rip this apart.

Because I think half of what we’re discussing at least is, essentially, this duplication of us trying to have these follow-up recommendations, and then making new ones about the same issues. I think this is one big reason why this is disjointed and why we have all of these discussions, because the stuff that is logically connected is not in the same spot because we’re trying to have these two extra parts. I'm not sure if we can change this, if we should change this. I'm just saying I feel this is our key problem right now.

KC CLAFFY: Do I hear you, Laurin, saying you want to remove all reference to SSR2 recommendations in our set of recommendations?

LAURIN WEISSINGER: No, that’s not what I'm trying to say. What I'm trying to say is we have an SSR1 follow-up on the stuff that has to do with risk, for example. And then, we have our own recommendation that relates to risk.

What I'm saying is not to remove and of the points but to change the structure in which we present this, to say, “Oh, okay. We don’t do SSR1 risk, then we do something else SSR1, and then we do something on risk SSR2,” but we essentially reorganize this so that it flows logically, and we don’t go with the current structure where we do SSR1 first completely as the recommendations and then we build on top, but instead we put it in one.

Because I think a lot of our problems are currently that there is this duplication and this logical disjoint because we are talking about X, then we're talking about Y, and then we're talking about X again.

HEATHER FORREST: I wonder if it would be helpful if, perhaps, Laurin, you and I had a separate call and just came up with an example outline of what this would look like so that people could see it and react to it.

LAURIN WEISSINGER: Yeah, and I'm more than happy to do that.

HEATHER FORREST: Okay.

LAURIN WEISSINGER: I mean, I'm working from home now.

HEATHER FORREST: Who isn't?

LAURIN WEISSINGER: Yeah.

HEATHER FORREST: All right. I'll coordinate with you.

LAURIN WEISSINGER: Yeah. Thank you. All I'm trying to say is, maybe if we fix this we might be able to get rid of a lot of the discussions we're having because they're all about structure and linking stuff up.

KC CLAFFY: I have been asking for that for two-and-a-half months so I'm very happy someone else—

LAURIN WEISSINGER: I'm aware.

KC CLAFFY: And then it suddenly becomes a good idea because someone else asked for it? That's fantastic as far as I'm concerned! So yes, please go off and do that. Too, though, I wouldn't say that's our main … I think it would do a huge amount to address the incoherence that I currently find in this document but the other big problem here is the smart thing that Laurin keeps harping on, that every single one of these recommendations needs to, identify the problem that it's trying to solve, and if we cannot talk about the problem because of some sensitivity of security information we have to come clean about the fact that there is a problem that we cannot talk about.

I don't think that's the case. I think we ought to be real careful if that's the case, and if so, then really outsource it to a professional security

organization. But if it's not the case, then we should identify, what is the problem that we're trying to solve? We often do not do that.

And that's separate from what I think is another big problem with the document, the fact that we just duplicate things everywhere between SSR1 assessments and SSR2. So, I'm fully in favor of Heather's suggestion.

ERIC OSTERWEIL: KC, in the spirit of what Heath and Laurin just said, I'm happy to have a private conversation with you and explain the substance behind a lot of this recommendation. And in fact, the footnote at the bottom makes reference to the meeting that spawned this. Like I said, I'm happy to have that conversation with you. We can have it later today if you'd like.

Basically, the directions in these recommendations are saying, "It's not us saying what you should do. It's us saying that you should do something different than what you've done before. You should do these things, which we happen to note is different than what has been done before, because we saw something that was a real big problem." So, maybe they don't do a good job but I'd like to at least give you full context, so I'm happy to have that separate conversation.

RUSS HOUSLEY: Thanks, Eric.

KC CLAFFY: Just remember SSR3, if such a thing exists because ATRT is voting to kill all SSR reviews until further notice, but if SSR3 ever exists they have to

not only figure out, was this recommendation implemented, but was it effective?

And so, we need to say, “What is the problem that it is trying to solve?” so they can decide, did it solve that problem? And then, we also need the metric of … Maybe not a metric, but at least some identification of, how do we know the recommendation was implemented in the first place, much less effective?

LAURIN WEISSINGER: Yeah. Thank you, Eric. Just to reiterate what I was talking about last for two minutes, I'm not talking about taking anything of substance out. What I'm talking about is, move this stuff around so it’s logically coherent. And then, if there is stuff where we can remove unnecessary duplication, we can do that. This had nothing to do with substance or the specific recommendation. I came to saying this again because I really feel it is becoming very obvious that we have this problem.

RUSS HOUSLEY: Okay. We only have five minutes left. Given this discussion, I find it hard to believe we can get through eight in that amount of time. I will ask, is there any other business?

[YVETTE GUIGNEAUX:] But Russ, we could delegate eight to Laurin and Heather.

RUSS HOUSLEY: We delegated the whole outline to see if they could come up with a better one. That seems like enough.

[YVETTE GUIGNEAUX:] We got through a lot this call.

RUSS HOUSLEY: We did. So, is there any other business? All right. Then I think we'll give you five minutes back.

UNIDENTIFIED MALE: Thank you all.

RUSS HOUSLEY: Be safe.

UNIDENTIFIED MALE: [cross talk]. Be safe, yeah.

[END OF TRANSCRIPTION]