BRENDA BREWER: Hi, everyone. Welcome to SSR2 plenary call number 70 face-to-face meeting day two in Brussels on the 18th of May 2019. We're beginning the day at 7:12 UTC.

We'll go around the room again for attendance. Remember to push the mic as you speak, and we'll start with Scott.

SCOTT MCCORMICK: Scott McCormick.

DENISE MICHEL: Denise Michel.

RUSS HOUSLEY: Russ Housley.

LAURIN WEISSINGER: Laurin Weissinger.

ANGIE GRAVES: Angie Graves.

BOBAN KRSIC: Boban Krsic.

NAVEED BIN RAIS: Naveed Bin Rais.

NORM RITCHIE: Norm Ritchie.

JENNIFER BRYCE: Jennifer Bryce, ICANN Org.

BRENDA BREWER: And we have Kerry Ann joining us remotely. We have apologies from Negar and Jabhera. Today's meeting is being recorded. Please state your name for the record, and we'll begin the call. Thank you. Oh, Danko is on remote as well. Thank you.

UNIDENTIFIED MALE: Morning, everyone.

RUSS HOUSLEY: Good morning.

UNIDENTIFIED FEMALE: Morning.

RUSS HOUSLEY: Okay. When we broke up yesterday, Laurin took an action item to turn the ideas that we had discussed into recommendations, and he's going to tell us what he did earlier this morning.

LAURIN WEISSINGER: So the last discussion was turned into what is now recommendation 38 on Compliance. In addition, we have now a kind of – if you look at the title, I have a very short description of what it is about and the related recommendations. They're also in a spreadsheet. That should be in everyone's shared team drive if this worked. I will post the sheet somewhere. You can see it, Jennifer? Okay, then it worked.

RUSS HOUSLEY: So you think this aligns with all five strategic objectives?

LAURIN WEISSINGER: In that case, yes.

RUSS HOUSLEY: Okay. Can you –

LAURIN WEISSINGER: Elaborate?

RUSS HOUSLEY: A little bit.

LAURIN WEISSINGER: This is something we can discuss.

RUSS HOUSLEY: I think we ought to.

LAURIN WEISSINGER: So strategic objective one in terms of security, that should be clear. Effectiveness of multi-stakeholder governance, so this one has strategic goals below that go into this direction of kind of accountability, transparency, etc. Strategic objective three is evolve unique identifier system to continue to serve the needs of global Internet userbase. Again, this all functioning and abusive parties being cut off would probably count as that.

Geopolitical issues could emerge because if ICANN fails to kind of rein in SSR issues, then obviously, challenges geopolitically become more likely, and then obviously number five, this is unclear, but this could have a significant financial impact on ICANN's financial sustainability.

RUSS HOUSLEY: Well, thank you for all that effort to put this in a structure for us. So as we said yesterday, we want to go through each of the topics, get a synopsis of what the team's findings are, look at the related recommendations, and see whether we have achieved consensus [or we need to] make a change.

So which one – can you put the link to the status document in as well? Okay, so I don't know what else to do other than just take these one at a time. So the first one is ICANN SSR1 is perform an assessment of ICANN's information security management system.

Instead of making its own recommendation yesterday when we talked about this, we decided it was better to expand our text on the SSR1 recommendation nine to include the establishment of an ISMS as opposed to have any other separate discussion of it.

So if you go to the recommendations document, you'll find that recommendation number two is the one that is the response to SSR1 recommendation nine, so that paragraph is the one that was edited yesterday to include the information security management system. So basically, the second sentence was added.

So given we had already come to consensus on everything [inaudible] that sentence? Does anyone have any concerns with that approach? Okay, hearing none, we're going to declare that we have consensus on that topic. Alright.

NORM RITCHIE: Is this recommendation saying to implement 27001? Because that's how [inaudible].

RUSS HOUSLEY: So that is where ISMS is defined, and that's what the second sentence is trying to say, implement – we're just trying to define that. And then

later, it gives a list of approaches, pick one and use it. Okay. If it's not clear, please edit.

LAURIN WEISSINGER: So we don't have a directly related recommendation. In some cases, we have two recommendations on the same topic, but in this case, there are multiple related ones, and we should probably in a later editing pass think about if we can merge something here. But I would say let's put a note down and not do this now.

KERRY-ANN BARRETT: Can you hear me?

RUSS HOUSLEY: Yes, we hear you.

KERRY-ANN BARRETT: I think what Erik was asking, [the sentence specifically] said that ICANN should fully implement the [inaudible] implement. I think that's what the question was. [inaudible].

RUSS HOUSLEY: So, can you just add transparent where you think it belongs?

KERRY-ANN BARRETT: [inaudible]. So I want to say that along the lines of [inaudible] concerned measures such as [inaudible] or something like that [inaudible].

RUSS HOUSLEY: Kerry Ann, do those edits – can you see them? Do they resolve your comment?

KERRY-ANN BARRETT: [inaudible].

RUSS HOUSLEY: I couldn't understand her. Did anyone else? We didn't understand that, Kerry Ann. Oh, good. Thank you. Typed in chat that she's fine. Okay, the second topic is ICANN SSR topic one. I'm sorry, topic two, is perform an assessment of ICANN's business continuity management system, and Boban, can you tell us where we are on that?

BOBAN KRSIC: Hi. The only thing that I did yesterday was to add business continuity to recommendation number 11, so we referenced initially to business continuity. There was a statement in the recommendation, and I just added in a second paragraph, an ISO standard that is 22301 how to implement the business continuity management system, and that's it, so you [can address it] with recommendation 11.

RUSS HOUSLEY: Okay. Laurin, I'm confused that recommendation 11 is about security risk management, right? Okay, thank you.

LAURIN WEISSINGER: It's two things. [In] the table, it was correct. Sorry. Yes, this was one of the recommendations I noted we should kind of look at together with certification and the ISMS, and there are a few others where we have to probably look at kind of groups and see to not repeat anything and then have them in like a functional setup.

RUSS HOUSLEY: Can we merge the first two bullets? Norm, use the microphone.

BOBAN KRSIC: Just to add a comment, norm asked me if it's here mentioned in dedicated security risk function, because ICANN has risk management in place, so we add just here in the recommendation alphabet is related to security risk function and [inaudible] risk management system.

RUSS HOUSLEY: Okay, so with those changes, does anyone have any concerns, or have we reached consensus on this? Okay, the next one is related. Laurin's got the lead on this one. Sorry.

KERRY-ANN BARRETT: [inaudible]. Sorry, I was just reading it. I hope you can hear me clearer.

RUSS HOUSLEY: We can hear you. Go ahead.

KERRY-ANN BARRETT: I know that we'll probably refine [inaudible] make a comment. I'm okay with a general [inaudible] but it's not specific [inaudible] doesn't mean anything. So someone who might have to implement it in terms of what we mean by pertinent security [inaudible]. So I'm okay with [inaudible] maybe we can [inaudible] a bit more clear on what we mean [by] pertinent security [contractual terms.] It doesn't give a lot of directive to whoever may need to implement it. So this could be a placeholder, just to fix that part of the sentence.

RUSS HOUSLEY: Do you think you can propose changes to address your concern, or is it ...

KERRY-ANN BARRETT: [inaudible] I would probably want to just clarify what [we intended by pertinent contractual terms] as it relates to what we spoke about yesterday with the Compliance team about [inaudible] or is it pertinent in terms of more stringent measures for security? Is it pertinent in terms of what? Like what do we mean [by defining] pertinent contractual terms? Operational terms – so pertinent is very broad [inaudible] won't help them to [inaudible]. So if anyone wants to talk to me about it and I can [inaudible] language, but I'd rather us [inaudible] what we mean by pertinent. [If we don't want a list,] it's fine, but what aspect of the

contract that we think [inaudible] define what we spoke about [inaudible] just to try to go through what does abuse mean, etc.

So those are the kind of things that we want [inaudible] the broader description of pertinent. I don't mind speaking to someone offline to fix it, but [inaudible].

LAURIN WEISSINGER: Just to reiterate, I had a look at essentially relations or intersections of recommendations. So just for a note, the recommendation 11, which is security risk management, relates or touches on or intersects with recommendation eight, which is also on risk management. Number 12, which is outward-facing risk management, 40 which is on the disaster recovery plan which is mentioned here as well, and again, the disaster recovery, which is also 27. Sorry.

So what I'm trying to say is we should keep that in mind when we look at these, because I feel there needs to be an editing pass to get rid of these kind of problems so that one recommendation does one thing and there are not two or three that relate to the same issue.

RUSS HOUSLEY: So when the group makes that pass, would that resolve your concern, or is that likely to resolve your concern?

KERRY-ANN BARRETT: [inaudible]

RUSS HOUSLEY: Yes, please.

KERRY-ANN BARRETT: It's more than just a correlation. I think as we start to define it, the way I look at the document now, [inaudible] understand what Laurin [inaudible] concerning the correlation between different sections and broader subjects [inaudible] risk management [inaudible]. But when we met with Compliance, [inaudible] the contracts needed to be [inaudible] I know we'll have specific language [inaudible] aspects of the review, so it's just that [inaudible] broad brush [inaudible] pertinent then we're saying it's risk management that needs to be [inaudible]? So the contract SLAs as they are now have a lot of terms defined. So what are we considering as pertinent [inaudible] any subject relating to abuse so that their contracts define areas that address DNS abuse. That's the only concern I had. [It's not a matter of] correlation between the various recommendations, but that that one that we have there is a very critical issue that the Compliance team had raised with us [inaudible] more specific, [inaudible] what they need to do. So just the word "pertinent" is very well-defined for me. [inaudible].

RUSS HOUSLEY: I'm at a loss as to how to address your concern.

KERRY-ANN BARRETT: As I said, we could put a placeholder [inaudible] other recommendations, it's something that could be fixed to be more specific

to all the areas that we have identified that should be addressed in the contract terms. That way, we could tie that to a more specific recommendation into what we're recommending for them to do [inaudible] definition [inaudible] term. So it's more a flag that [inaudible] as is, but whenever we finalize, we should [inaudible].

RUSS HOUSLEY: Okay. So what I'm hearing is we have not reached consensus on this particular recommendation, because at least one person thinks we need to be more specific and measurable here. So I'm hoping –

NAVEED BIN RAIS: Russ?

RUSS HOUSLEY: Go ahead.

NAVEED BIN RAIS: So another thing regarding this measurable is like another point I see here, which is asking ICANN to point or name a dedicated responsible person. So I see two things here in this bullet, one is appointing or naming, and the second is the findings should be fed into the [BCD and ISM.] So these are two things and how measurable that is, like are we asking for recommendations from that person? Is it one single person? Is it like a pool of persons? Is it community-driven? Is it coming from the ICANN? Is it a contractual kind of thing? So again, to be more specific would be better in this case, I think.

RUSS HOUSLEY: So I think you're calling for dividing that into two thoughts. One, the dedicated, responsible person, and the other is how the findings are fit in.

NAVEED BIN RAIS: Yeah.

RUSS HOUSLEY: Norm, should this risk management down here be security risk management, or is this one ...

NORM RITCHIE: I think they all [inaudible].

NAVEED BIN RAIS: To elaborate more, I see a disconnect between appointing somebody and seeking the findings. So there has to be something in-between, like –

RUSS HOUSLEY: [inaudible] how to do that.

NAVEED BIN RAIS: It's a process until reaching a finding. So, what process are we seeking for?

RUSS HOUSLEY: Norm, can you type something in to [pick] your point about organizational [instinct?]

NORM RITCHIE: [inaudible].

RUSS HOUSLEY: Dedicated and responsible person. So this won't be the same person.

NORM RITCHIE: No, the question is [inaudible]

RUSS HOUSLEY: Exactly. And I think that's a separate point and you need to – somehow, I think the bullet four, the security and risk management – maybe that one's also separate and distinct from existing systems or something like that.

Okay, are there any other points to capture here? Because we still need to come back and address being more specific and more measurable.

Okay. Moving to the –

KERRY-ANN BARRETT: [inaudible].

RUSS HOUSLEY: You're pretty quiet there. Okay, moving on to ICANN SSR3, Laurin, this one is about the risk management methodology and framework.

LAURIN WEISSINGER: Essentially, we were just talking about that.

RUSS HOUSLEY: You need to talk to the microphone.

LAURIN WEISSINGER: Essentially, what we were just talking about [inaudible]. So that was integrated.

RUSS HOUSLEY: So it's also recommendation 11?

LAURIN WEISSINGER: Yes, with all its related recommendations.

RUSS HOUSLEY: So if I understand your other table right, that means recommendations two, eight, 11, 27 and 40 all apply here.

LAURIN WEISSINGER: More or less. So essentially, what is happening is what I'm doing [with their] related is if an issue, for example, say, disaster recovery pops up in a rec and then in another one, that's when I said this is related or there is something we should check, if this is doubled or if we can somehow merge, etc.

So this is what's happening now. So for example with the [inaudible] two is on the ISMS, which has language relates to this, eight is on risk management, 11 is on security risk management, 14, 27 are on business continuity, which is also, again, mentioned in definitely 11, probably also two.

NAVEED BIN RAIS: But 12 here is like mapped to eight and 11, but 11 is not mapped to 12. So [inaudible].

LAURIN WEISSINGER: Yes, because that's only risk.

NAVEED BIN RAIS: Okay. So [inaudible]. Like when we say 12, related to eight and 11, when we write 11, we don't see that it is related to 12.

LAURIN WEISSINGER: Okay. 12, I just forgot, because there's so many related.

SCOTT MCCORMICK: By the way, ISMS addresses risk, business continuity, disaster recovery. So I think –

LAURIN WEISSINGER: That is my point, yes. So that is why it's mentioned for all of those. So that's number two, the ISMS. And essentially, my question, again, is, do we need those extra recommendations, or can we fold some of them into one? Because for example ISMS addresses these things.

So might be too much, but then the question is, do we want to group them together or something like that?

NAVEED BIN RAIS: Like one [synopsis] can result into more than one recommendation even they're related, so if there's no overlap, we can keep the – so you're only saying that if there's a duplication, then in that case, we need to merge, right? But not that one sign-up says for one recommendation, right?

SCOTT MCCORMICK: No. So essentially, what I'm just saying is if there's overlap, we have to make sure that this is addressing two points or two issues [and] not the same. All I'm saying is we have to review those where these intersections or overlaps exist to make sure that we do not make the same point multiple times, or if we make additional points, if it makes sense to have this in one place, that's one.

And the second one is if we want to group related recommendations together so that we have, say, one on – I don't know, one on risk and one on business continuity, but we put them on the same page or close to ISMS and each other. So this is just a note, this doesn't mean I think we should necessarily have to do something. It's more like a flag. Keep in mind this is related. That's it.

NAVEED BIN RAIS: Which one are we looking at now? 12?

RUSS HOUSLEY: We're looking at that – at least what I'm doing is there's that list, I'm reading them together to see if I can understand the concepts that we're asking for, and that's what I'm worried about getting consensus on, is those concepts we can organize and wordsmith later.

LAURIN WEISSINGER: Kerry Ann, quick question. I see edits, but in ten, not 11. Kerry Ann, we're slightly confused because we were discussing recommendation 11 and your concern was on recommendation 10. Could you elaborate?

KERRY-ANN BARRETT: Hi. Is the audio any better?

LAURIN WEISSINGER: Please speak up.

KERRY-ANN BARRETT: Is the audio any better?

LAURIN WEISSINGER: Very quiet.

KERRY-ANN BARRETT: I'll probably ask Brenda to call out again.

BRENDA BREWER: I will call you, Kerry Ann. Private message your phone number, please.

RUSS HOUSLEY: Actually, I've just read back to back that whole group, the two, eight, 11, 27 and 40, and there's significant overlap, and I think we can turn – I don't have a problem with any of the things we're asking for in any of them, I just think we can present it more clearly, and remove that overlap, but what I'm trying to understand from the team – and I'm now confused about Kerry Ann – is whether anyone has concerns with the ideas or the direction that these are going, or have we gotten to consensus? And since our problem was with 10, not 11, I'm not sure.

LAURIN WEISSINGER: Just to note, I'm happy that I appear to not be crazy.

KERRY-ANN BARRETT: Hi. [It's not in my interest] to make anyone feel crazy. The concern was 10, just before you try to move on to 11, I was trying to say that, and apparently that didn't come across. I think Naveed's comment as well was related to 10, not 11, and Naveed [inaudible] because he did mention the CSO and the two roles that [inaudible] the CSO undertaking a risk management, [both] pretty much implementing risk management, and the second part of that recommendation spoke to security staff taking part in negotiations for [contractor] risk management, so ICANN contracts.

So the concern I had before we had moved on to the actual risk management was the fact that we had the term "pertinent," which is why I was using it so frequently so you guys [inaudible] that was the section I was concerned with. Pertinent wasn't very specific for what the Compliance team needed. So the suggested language was [to fix ten as we go] into the actual risk management portion, because recommendation ten spoke about those risk management components being part of the ICANN contracts across the board, not just the SLAs. So that was the concern I had as we left that one, since we're going to sign off on it and going to all the others. So I hope that clears up the ambiguity. I hope the language that I suggested as well clears up what I was trying to achieve with that recommendation.

LAURIN WEISSINGER: Kerry Ann, thanks a lot. Just as a note, the aspect of security and compliance, etc., being part of contract negotiations, that is another one that is repeated, I believe, in recommendation 38, so just for your information that this pops up again. Yes, it is recommendation 38.

KERRY-ANN BARRETT: Noted, Laurin. As I said, because it is distinct to the CSO office [that we're] recommending and being part of the negotiation team for ICANN's [suites] of contract, [it just says] ICANN contract generally, so this could be upstream or downstream suppliers, etc., which his the concern I had just to make sure that we're very clear on what we're asking the CSO to do on the security team in helping to negotiate contract terms.

LAURIN WEISSINGER: Kerry Ann, yeah, makes sense. I just want to let you know that this is another one where we have to probably look at.

RUSS HOUSLEY: Thank you, Kerry Ann. I now understand why I couldn't understand what you were trying to make the point when I'm looking at [Laurin's] text. So anyway, thank you for being persistent and getting your point through. We hear you much better now, by the way.

So I think we have achieved consensus on this topic, that is topic three within the ICANN SSR Work Stream, and if that's not correct, please speak now.

LAURIN WEISSINGER: Just to check, we had something under draft recommendation 11, a comment by someone that it is not measurable and/or specific enough. This comment has now been removed.

RUSS HOUSLEY: Because I wrote that trying to capture what –

LAURIN WEISSINGER: Okay.

RUSS HOUSLEY: Okay, so moving to four.

NAVEED BIN RAIS: Russ?

RUSS HOUSLEY: Go ahead.

NAVEED BIN RAIS: In continuation, I was looking at 12, and I also think that it's like revolving around the same risk management, but there are some confusion in that. So I was just asking if we can discuss it now, or at a later stage, because I see that it is written under topic of DNS SSR, but its still dealing with risk management. So just asking at this point.

RUSS HOUSLEY: Why don't you go ahead and make your point since we're here?

NAVEED BIN RAIS: Yeah, actually, my point is it's also asking about this framework in terms of risk management, and what I could not understand is the last line, which is this analysis should be updated twice a year. So, is it related to what should be in the contract? Because it talks about updating the contracts with the registries and registrars and make it obligation to include those risk management-related stuffs. So I could not understand the last line that is making a point of updating this published and communicated to the stakeholders, because stakeholders also involve those registries and registrars.

So once the contract is done, we should be clear on what [is need of] keep that updating, or can we do it once the contract is already done with that specific registry or registrar?

LAURIN WEISSINGER: Naveed, I think this is just kind of a bit unclear, so I've just put a suggestion in there which would be kind of saying ICANN would issue these reports on threats twice per year and communicate them to the stakeholders so that they can actually react to it. Would that solve the issue?

NAVEED BIN RAIS: Yeah, pretty much. But if we are still asking for the registries' contracts to be updated based on that report, then that would raise a flag maybe that it's something that is not implementable because of the compliance or whatever later. So we should keep that in mind.

LAURIN WEISSINGER: Naveed, maybe this is also not super clear. I think what this wants to say is that the contracts should change so that the contracted parties need to react to these threat reports that ICANN puts out, at least that is what I am reading. So it's like two points, like one is how often ICANN puts it out, and the second one is that they should have to react. Everyone correct me if this is not what you read out of this.

NAVEED BIN RAIS: Like reacting, how measurable that reaction may be, so like they can just say, okay, we listened to you, but they don't do anything. So in that context, I'm just asking, like we can put something in the contract that this is your obligation to react to this, but how much is the extent of that reaction is not clear to me.

LAURIN WEISSINGER: Don't disagree at all. I'm wondering – what would be measurable is if ICANN produces these reports. I'm not sure it would be measurable how contracted parties react. And I'm not sure if it's within our scope to recommend something along those lines.

RUSS HOUSLEY: Perhaps you do this in the opposite order. First say ICANN should issue the report –

LAURIN WEISSINGER: Yeah, [that's what I was doing now.] So I'm just changing the order which is also what Russ is suggesting.

KERRY-ANN BARRETT: [In the middle, while you do that,] I think it would be useful for the rest of the team to – a part of the whole contract thing that Compliance team explained to us is the period of review in terms of it being automatically renewable, and pretty much unless there's something that they defined as [inaudible] if that was not fixable, like there was no remedy on the part of the contracted parties, they pretty much roll the contracts back in unless we publicly recommend more specifically that ICANN introduce terms in the contract that – [I know Laurin was saying] [inaudible] but it has to be that there's a term that says that the contracted parties, whenever they do renegotiate, should at least – if ICANN [issues a report, is it just a report for them to just have] knowledge of, or is it a report with specific risk factors identified that need to have been measured to fix it?

So even if it's in the report, is it just the knowledge of the community? Because unless it's very specific in the output in the report that they can't go into the contract terms as something actionable for the contracted parties to act on, if I'm clear.

So if the report is for public at large, it may not affect every single domain, may not affect everyone the same way based on what security measures you have in place. So it would have to be two distinct things, and maybe we could grab the contract, as Laurin pointed out, later on when we go to recommendation 38. I hope I'm clear. It's really early so I'm really trying.

RUSS HOUSLEY: You're doing really well.

NORM RITCHIE: I'm going to try this again. [inaudible] stay away from the microphone.

NAVEED BIN RAIS: [inaudible].

NORM RITCHIE: It's me. It's totally me. I'm struggling with this a little bit trying to understand the intent, and that is because if there is a risk that warrants change by the registries and registrars, why would you wait for half a year? Wouldn't it be implemented immediately?

I just don't follow this.

KERRY-ANN BARRETT: Hi. One of the things I was suggesting that if it is that they issue the report, for example in our organization, whenever we do the threat analysis, we pick up something that needs to be actioned, we usually send a script out with it. So let's say [inaudible] develops a script that addresses the issue that's out there. We would usually issue that whether it be [amber,] whatever level it is that's actually allowed to be shared, we would then share it accordingly. So if ICANN for example comes up with a specific threat that's going to affect all registries and they don't have a fix, it doesn't really help except to say, okay, hi, yes, noted. Because based on how they run their own house, we have to be

specific. So, are we saying to ICANN that they need to then develop a security team that's able to see this risk, analyze it and make recommendations or make suggestions, or make a high-level directive – [inaudible] they always say that they can't direct the registries, I would just say to them that, find the threat, give suggested fixes, issue that, and then ask everyone to comply with that issue. But it can't just be in the contract terms, because every single registration would have a different way how they're actually managing their own show. And that's why you have strong ones and weak ones and ones that are just the usual [to just create all kinds of] malicious acts, so it's kind of – so I agree with you, it shouldn't wait half a year, but what Compliance has said to us is that right now, how their contract is worded, there's not much more they can do than just that to ask them to remedy, however long that takes them to remedy. And if they finally remedy, there's not much action [that they take] after that. So we just have to distinguish the two actions, developing the report and issuing it. But what else is to be done with the knowledge that's coming out?

LAURIN WEISSINGER: So not to have another addition or something that is related, but when you were talking about kind of stuff happening immediately, this sounds pretty much like the vulnerability disclosure stuff we have, where it's kind of like, oh, ICANN should report vulnerabilities they're made aware of down the chain and there should also be a requirement that if you are a contracted parties, you report it up to ICANN and they react.

So I'm just again wondering, because I read this more as like a kind of risk and threat kind of report that's more on the general end of things

and not this type of specific vulnerability or something like that. But that might be my reading only, and if it is, then the question becomes, how would vulnerability reporting slot into this?

NAVEED BIN RAIS: I just have an additional thing. Just to be clarified, do we mean these reports to be public, or just between ICANN and the contracted parties? Or do we need to specify that here?

LAURIN WEISSINGER: So this might be a key difference. Right now, the recommendation reads registries, registrars and also the community. So if the community is involved, this would be a higher level, more general report whilst vulnerability disclosure would be very specific because you might not want to tell the whole world.

KERRY-ANN BARRETT: Laurin, vulnerabilities [inaudible] specific domain in terms of however they're structured and wherever lies is one thing, but I agree if it is that it affects a specific registrar, they should report that to them and have them fix that or remedy it. But when you speak to the threat report, the threat report could be something that could affect all domains, all registries. That could be something that is for example there's a group that wrote to us, [Cisco,] and they're actually tracking a threat that has been persistent for the past six months and they're now trying to see if anyone else has noticed it. And something like those kinds of threats that ICANN may detect and then be able to communicate is something

that may not be for the community as well. It could just be for the registrar [inaudible] and it is a persistent threat and not necessarily a vulnerability.

So we have to kind of distinguish if we're talking about security and stability, why would we send this to the community? Unless to keep the registrars accountable. But we can definitely have a more high-level report for that, but I think if we're talking about a kind of threat analysis that we know that would be useful to them, it should probably really just go to the registrar, the registry, and then figure out how to let them actually – we should distinguish this information, for example the DAAR report is to the community at large, whatever information they're allowed or whatever they've been permitted to release, but [inaudible] trying to get the registrars and registries into a shape that you're actually integrating threat analysis, threat results into their risk management framework and let it be iterative and improve and improve. What is the end goal of this recommendation if not that part? So just wondering [inaudible] we just have to figure out what exactly is the level that we want to issue for this part.

LAURIN WEISSINGER: Kerry Ann, this is exactly what I'm referring to. I didn't write this one, so I don't know what the initial idea was, but –

KERRY-ANN BARRETT: [inaudible] It's now our language, Laurin. You don't have to defend that you didn't write it. It's all our language.

LAURIN WEISSINGER: No, because I feel you're criticizing me for what I'm saying, but all I'm trying to say is we should think about what we want to get out of this. And I highlighted the vulnerability disclosure because that is somehow going in the same direction.

KERRY-ANN BARRETT: And just for the record, I'm not criticizing. The discussion is for everyone at large. You're the one speaking right now. So just everyone, there's no critique of the language. I think we're all going through it and understanding it, whoever the author was and whoever has a better understanding, explain it. I think that's how I'm approaching it. There is no critique of any specific language. What I usually try to do when I read [inaudible] team is that usually I have [inaudible] see it in black and white and then to say, okay, what is the purpose, what is it achieving? How will I be able to implement it if I have to implement it?

So just for the record, it's not critique of the language, it's just kind of having explained it, it's just to kind of continue with the chain of thought that you had to just fully clarify what you're thinking, and if anyone else has any other thoughts. So just for the record.

LAURIN WEISSINGER: If I was to look at this, I would say something along the lines that ICANN should kind of – so we should probably look at vulnerabilities and like these threat reports, put it in one recommendation, say ICANN should

somehow have a place where this comes in and is then shared out to relevant parties. So that's one aspect.

And [that] should probably be done and this would be more what this recommendation is talking about, kind of some form of reporting or measurement of that happening. Is that a direction everyone would be happy to go into?

SCOTT MCCORMICK: So a comment on this. Currently, ICANN has a private program [where hackers want to disclose on their vulnerability website.] However, they also have an e-mail version of it to send vulnerabilities in. Instead of having two separate programs, it would be good to have one common program as well as those metrics. We send them – obviously those are confidential and have vulnerability data in them, so we have very detailed statistics, the [hacker one sends,] the security team – specifically, it goes to Brian, but I know it touches the entire [inaudible].

DENISE MICHEL: That sounds good. Is this also an appropriate place to make some suggestions about action on systemic problems that we talked about yesterday in addition to the individual entries?

SCOTT MCCORMICK: One of the issues right now – and this is again – are we recording right now?

RUSS HOUSLEY: Yeah.

SCOTT MCCORMICK: Can we stop the recording?

So we're going to expand – what is this, recommendation three? We're going to add on to this, and obviously, include SSR1 recommendations, but also, we're going to add ICANN Org and DNS SSR vulnerability language in here.

LAURIN WEISSINGER: So I merge recommendation three and recommendation 12.

SCOTT MCCORMICK: That works. And break time?

RUSS HOUSLEY: Okay. let's take a break. Please be back in 15 minutes. Thank you.

Okay, we're back from the break, and Alain has joined us. Welcome. So let's see if we can turn to ICANN SSR topic four, which is perform an assessment of how effectively ICANN has implemented a security incident management and response process, and Scott, this is the one that was marked. It seems to be too sensitive to share. So, how are we handling this?

SCOTT MCCORMICK. Yeah, so basically, they said they wouldn't even show this information NDA, which I call bullshit flag on. So, any business shares this type of information with vendors on a regular basis. It's an industry standard. So I'm not sure how we want to put this, but definitely call the bullshit flag on it somehow in that report.

RUSS HOUSLEY: I thought the way forward was to write a recommendation that said something to the effect of we can't tell if you've done this because aren't willing to share information, but this is the kind of system that needs to be in place. And we can't tell how far or how close you are to that system because no information was shared. Do I have that right?

SCOTT MCCORMICK: Yeah. Which recommendation is in the –

RUSS HOUSLEY: I think you were tasked to write one.

SCOTT MCCORMICK: Darn. Got you. I thought I added this to recommendation 10 under – so the last sentence on page eight of draft recommendation 10, it's pretty blatant, but I think that was trying to wrap this into – not create a separate recommendation – that position there. I can add some more specific language about IR into the response as well.

RUSS HOUSLEY: Yeah, I was about to say something needs to be said about how incident response is handled or tie it to vulnerability disclosure or one of those two, but something in that – lack of transparency about how incidents are handled raises concerns. Something like that.

SCOTT MCCORMICK: I feel like I might actually better go with the one Laurin and I were just working on with vulnerability disclosure, because obviously, incident response vulnerability disclosure is –

RUSS HOUSLEY: Which is which number?

SCOTT MCCORMICK: [Closer tied –] that was recommendation three above.

LAURIN WEISSINGER: Yeah, [inaudible].

RUSS HOUSLEY: Okay.

SCOTT MCCORMICK: I'll move this from ICANN SSR up to –

RUSS HOUSLEY: That's fine.

SCOTT MCCORMICK: The SSR1 recommendations.

RUSS HOUSLEY: That's fine.

LAURIN WEISSINGER: Just again [inaudible] we have some other stuff that's also kind of going in this direction, so we would have to again monitor this after [inaudible] to make sure we're not repeating.

NORM RITCHIE: [inaudible].

RUSS HOUSLEY: That was the intent.

NORM RITCHIE: Yes, I know, but – yes.

SCOTT MCCORMICK: The problem is that OCTO is not running a security program. They suck at it and it needs to be called out. I'm trying to put it nicely by saying that, but ...

RUSS HOUSLEY: [inaudible].

SCOTT MCCORMICK: Yeah, the sentence is on page eight under recommendation 10, it's the last sentence there. The lack of transparency disclosure has raised concerns about the lack of resources, competence and oversight of ICANN's security program.

LAURIN WEISSINGER: [inaudible].

SCOTT MCCORMICK: Denise made the comment yesterday, the lack of security professionals around ICANN – not ICANN Org but ICANN the community – obviously has been transparent over time that obviously as more of us get involved from the security industry, like these are issues that are going to blatantly pop up.

NAVEED BIN RAIS: I just have one remark. In recommendation ten, we're proposing a position like CSO or what we call a CISO. That's kind of a very high-level position. The scope that we are giving here maybe is only related to that, but a position like that may involve a lot of other responsibilities as well. So maybe at the end of when we have all the recommendations, maybe we would like to review it and see what are the responsibilities

related to the overall SSR activities that are related to this position, and then put this together back in.

Because just for one thing, like risk management, creating a whole position, because it requires a whole hierarchy after that in the organization. So that might be asking for too much. Just my –

LAURIN WEISSINGER: Yes. I think a lot will kind of fall under that position, like kind of organization [below] and this is exactly the point, at least from how I see it, that you have one person that oversees relevant aspects and makes sure something's happening. So that's totally fine, and as you say, in the end we have to make sure we point correctly.

SCOTT MCCORMICK: Yeah. I think the issue is that OCTO is a CTO, and we had the discussion yesterday, chief technology officer is very different from a chief security officer or a CSO.

LAURIN WEISSINGER: [OCTO but move] under security?

SCOTT MCCORMICK: Not necessarily.

LAURIN WEISSINGER: [inaudible].

SCOTT MCCORMICK: They're separate functions, yeah, and then also, when you think about risk management, there's risk management as a global enterprise and then there's also security risk management which is specific to security. Which I believe is something that is not really looked at that way right now.

It's kind of the old way of thinking versus the new way of how security is evolving.

NAVEED BIN RAIS: Can I follow up? Sorry. Just my point is when we say CTO or CSO or anything, like chief X O, it requires a whole hierarchy and set of dos that are required for the job. If we are going for that term, I'm just proposing that – do we need to have complete model of what are the responsibilities of that position along with this risk management, or we change the name to an advisor on security or something like that? Because when we say chief security officer, that requires a whole bunch of hierarchy and [stream] in the organization itself.

SCOTT MCCORMICK: Correct. It also shows having a C-level is also showing that ICANN takes it seriously as an advisor [is] not acceptable in today's enterprises.

NORM RITCHIE: Yeah, I agree with you on that. Just looking at this recommendation, and it's a powerful last sentence. Very powerful. I'm thinking it should be the first sentence, not the trailer, because [inaudible].

SCOTT MCCORMICK: Yeah. I'm fine with moving that up.

NORM RITCHIE: [inaudible].

RUSS HOUSLEY: Okay. Is there anyone who has concerns with three or ten and the concepts we're asking for? I understand we need some more details to address what Naveed just said, but is the direction here one that has consensus?

SCOTT MCCORMICK: Yeah. I'll add a little bit more verbiage on the incident response side underneath vulnerability disclosure, which is recommendation three so we can come back to it. I think Laurin and I are working on it right now.

RUSS HOUSLEY: Okay. Cool.

NORM RITCHIE: Yeah, I don't necessarily agree that if you have a C-level, it requires a whole organization underneath it. You see many places that –

RUSS HOUSLEY: I do think that we need a little more clarity on what the responsibilities of the c-level person are.

LAURIN WEISSINGER: I was just writing the comment.

SCOTT MCCORMICK: Oh, wait, that's what an ISMS is.

NAVEED BIN RAIS: Yeah. So I will say this because more we put or stronger the responsibilities that we put in the document, less would be the chances of getting that away from the ICANN perspective. Like if we put it too lightly, they might say that, no, this can be done by someone like this. So it has to be specific set of responsibilities that should convince the ICANN responsible personalities that this has to be implemented this way.

RUSS HOUSLEY: Okay. Not hearing any disagreement, but just things that need to be added to for clarity. And Brenda, did you see Kerry wants to be dialed back in? Alright. She said she was going to stay until 6:00.

BRENDA BREWER: [inaudible] private message. That's her time.

RUSS HOUSLEY: Right, which is another hour.

LAURIN WEISSINGER: [inaudible].

BRENDA BREWER: [inaudible].

RUSS HOUSLEY: Right, which means that –

BRENDA BREWER: [inaudible].

RUSS HOUSLEY: Okay. I see. Thank you. Alright, so turning to ICANN SSR – wait a minute. Danko's – so if you could capture what Danko's just put into the chat as a comment in the document.

Let's turn to topic five, which is perform an assessment of internal SSR of ICANN's operation processes. We have a bunch of stuff already related to DAAR and Compliance. Yesterday, we said there are other things, but all of the questions that we asked under this topic were either DAAR or Compliance. So we don't have any other aspects of the system captured in any recommendations.

Okay. Anyone want to put forward a recommendation that goes beyond [our compliance?] If not, we'll just move on from this one, topic five.

No, ICANN SSR 5, which is about ICANN's operation processes and services.

LAURIN WEISSINGER: What about stuff like internal procedures, internal security, which we identified as issues in the past?

RUSS HOUSLEY: And have recommendations from those others not here.

LAURIN WEISSINGER: I'm just wondering, and I'm just trying to think about Thursday when I read through all of them if there's anything in there that really goes to the internal operation of [IT.] I don't think we really have something.

RUSS HOUSLEY: And do we need something?

LAURIN WEISSINGER: That would be up to the team. I'm just saying I don't think for internal IT operations there is anything. Just so everyone's aware.

RUSS HOUSLEY: Well, I think that the vulnerability and incident response stuff as expanded by Scott goes beyond the new gTLDs and ccTLD IDN stuff to the internal systems, and I think that's –

LAURIN WEISSINGER: Okay, so Scott, should we just put like a bullet under recommendation three to kind of say when something is detected there is also an internal process to react? And then that would be covered.

SCOTT MCCORMICK: Well, this is a performance assessment of internal SSR.

LAURIN WEISSINGER: Yes. The question is just how do we cover this. Do we want to slot it in like as I understood Russ' comment, or is it too different?

SCOTT MCCORMICK: I guess I realize we're talking about resiliency of ICANN's operational process and services, but when we talk about performing an assessment of internal SSR process and services, that's a [sock two] or [inaudible].

RUSS HOUSLEY: Yeah, [no, it was] the team doing the assessment and the aspects we focused on were DAAR and Compliance, which we have recommendations for. The question is, is there anything else we want to cover?

SCOTT MCCORMICK: Not that we haven't covered already.

RUSS HOUSLEY: Okay. So other topics –

SCOTT MCCORMICK: Again, the internal security though is already covered under – where is that at?

LAURIN WEISSINGER: So that’s what I'm not sure where we cover, like the internal issues.

RUSS HOUSLEY: I thought ten was expanded to do that.

SCOTT MCCORMICK: Recommendation two under SSR1 covers that.

RUSS HOUSLEY: Yes, [that’s true as well.]

SCOTT MCCORMICK: Because it talks about [inaudible]

LAURIN WEISSINGER: Yeah, okay. That's fine.

SCOTT MCCORMICK: Which is all internal. Internal and external, but mostly internal.

RUSS HOUSLEY: So DAAR part falls under nine, but we're going to get to that when we talk about some other things, and we did a big thing on Compliance at the end of the day, which Laurin reported out as this morning, which had to do with recommendation 38 I think he said. Yes. So two, nine, and 38 will be related to this topic then.

LAURIN WEISSINGER: I'd note there's some more stuff relating to compliance that just came out of – I think that is [17] in the document you sent.

DENISE MICHEL: Yeah, that we've been assessing. Norm, Naveed –

LAURIN WEISSINGER: Yeah. So just to say there are more things regarding compliance, contracts and stuff like that.

DENISE MICHEL: DAAR.

LAURIN WEISSINGER: DAAR.

DENISE MICHEL: [inaudible].

LAURIN WEISSINGER: So this is at the bottom of the document, but these have not been edited yet. So I'm not sure how we should approach this if it makes sense to discuss them now, because it's still in the rough.

DENISE MICHEL: So if we have time to discuss the ideas of each of the recommendations, I think that would be helpful, but just noting that this captures ideas from sort of a running discussion and that the subgroup has had – and so there is some repetition, there's certainly some synthesis that needs to occur, but if we have time to just go through the ideas, make sure that we get people's input, and then we can, I think, work with a technical writer to put them in a more streamlined format.

RUSS HOUSLEY: So those new recommendations are related to which topic?

LAURIN WEISSINGER: 1-7.

RUSS HOUSLEY: Okay. Thank you. We'll get to it then.

LAURIN WEISSINGER: [We were just talking about it,] that's why we brought it up.

NORM RITCHIE: [inaudible].

RUSS HOUSLEY: Sure. Yeah. Okay, so let's move to ICANN SSR topic six. Norm. ICANN SSR six, you're the lead on that topic. So the topic is perform an assessment of how effectively ICANN has implemented its processes around vetting, registry operators and services concerning the new gTLD delegation and transition process.

NORM RITCHIE: Yes. So we talked about this yesterday. There was one recommendation that came out of that. I'm trying to find it. [inaudible] here somewhere.

RUSS HOUSLEY: [inaudible].

DENISE MICHEL: And while you're looking for that, there was another issue that was raised a while ago, and that was that the community doesn't necessarily have the ability to react to and provide input on the commitments in the applications during the application period and delegation period.

The commitments made by gTLD applicants. This includes the SSR-related commitments of the gTLD applicants.

So I think we may want to discuss a recommendation around more transparency on the commitments made during the application process and more transparency around how those commitments are codified in the contract, and then enforced in the contract. Specifically relating to SSR.

NAVEED BIN RAIS: Like when we say something like more commitments, what kind of – how much more or something like that? Do we relate it to something previous in terms of how quantifiable that is? I'm just wondering, like if you use something like this. I'm not saying that we are putting it as it is, but I'm just saying, going forward, whenever we say something more has to be done, how much quantifiable that is to be measured later? Like whether it is done or not.

DENISE MICHEL: Right. Well, I think that's a really good point, and I think relating to the idea that I just addressed the measurement of the recommendation would be the follow-through on posting SSR-related commitments in new gTLD applications, posting related language in the contract that carries those commitments from the application into the contract, and then publicly posting, say, an annual audit or review of compliance with those SSR-related contractual obligations. So I think that would be a fairly straight-forward metric.

NORM RITCHIE: It's recommendation 39. Just bouncing around a lot. Okay, so as we discussed yesterday, the assessment of the SSR within the new gTLD process actually was admirable, the requirements [inaudible] for the application process, the amount of testing they did. Basically, I believe they did a fairly good job.

It actually goes to speak to the requirements for the new gTLD applicant. That's what we're asking of ICANN, actually, as far as the security fostering goes. The only thing was to make sure what was specified within the applications regarding SSR is actually being carried out. So there needs to be some way of ensuring that there's an audit to make sure that post-delegation there's audits to make sure that the SSR activities are actually being [carried out] as stated, and also, within the transfer of a TLD, that a new operator fulfills those obligations.

DENISE MICHEL: Do you want me to add some language to that effect for you to look at?

NORM RITCHIE: Sure.

DENISE MICHEL: Okay. Yeah, I was just suggesting a little more specificity that talks about transparency and carrying through the commitments such as the SSR-related commitments from the approved application to the contract

and from the contract to the auditing results. But I agree with this recommendation.

RUSS HOUSLEY: Okay. So when Denise adds that, since there didn't seem to be any disagreement with what she was proposing, she can type that in there. And let's turn to topic seven. This is the recommendation 38. I think we went over it already this morning.

If anybody has any new thoughts, now is the time. Okay. Sorry.

DENISE MICHEL: What number?

RUSS HOUSLEY: 38.

LAURIN WEISSINGER: Just again as a note there are additional draft recommendations regarding compliance at the bottom which have not been worked into this yet because they kind of came out this morning. [It's on the rough,] so if we can get rough consensus, it's good, but we have to revisit.

NORM RITCHIE: I think [we're going to cycle on this] quite a bit more.

RUSS HOUSLEY: Sure. But I think we have from yesterday set out the basic direction.

DENISE MICHEL: Yeah. I think we're on the right track, but yeah, we have a lot more ideas and a lot more material to synthesize and work through.

RUSS HOUSLEY: Okay. We're waiting for text from KC on DNS SSR 1-1. So we'll come back to that one when we edit. She said she'll get it to us this weekend. So next one is business continuity and disaster recovery. Boban? And by the way, the answers came. [You saw that?]

BOBAN KRSIC: Yeah. I saw them. Thank you, Jennifer. I've added this recommendation yesterday, recommendation 40 regarding the disaster recovery plan. So the idea was to address strategic objective one and associated goals, ICANN should continue the development because they said, "Okay, we are in the development process of a new disaster recovery plan and we will finish it 2019." So that was the idea, we should continue it, we should [inaudible] process to have actual [continuity plans,] and this plan should also include all relevant systems, and that was a yes from this morning and the message. So that's the idea. If you have any ideas how to maybe specify it better, then feel free.

LAURIN WEISSINGER: Suggestion to consider merge with recommendation 27, which starts with ICANN [inaudible] to address community [inaudible] disaster

recovery plan for the global DNS root. So question is, do we want one on disaster recovery?

BOBAN KRSIC: Just [inaudible] 27.

LAURIN WEISSINGER: Say again?

BOBAN KRSIC: Just merge it with 27.

LAURIN WEISSINGER: Okay.

BOBAN KRSIC: Sounds good. Yeah.

LAURIN WEISSINGER: So I'm pulling up 42, 27 so we can see them next to each other.

NAVEED BIN RAIS: I [inaudible] SSR1 we had this problem of assessing those recommendations which talk about “continue to do this.” I'm just wondering if we should maybe better rephrase this, because when we say “ICANN should continue to do this,” there is no way to [trend] this

back whether it was continued or not. So something better that precisely says, “Okay, you have been doing this. Now it’s time to do this. In the next five years, you have got to do this,” so that we can see whether it was done or not. Something like this.

LAURIN WEISSINGER: Just as a note, in recommendation 27, we do have something like that, so that there is regular public comments, stuff like that. So you would actually see that this thing is in development and you would see if they stopped doing it.

BOBAN KRSIC: Laurin, maybe we can add something like actuality. That’s quite [inaudible] measure [inaudible] actual. So we have a continuous process.

NORM RITCHIE: So, is there – reading this, I get the sense that there's an overall disaster recovery plan, but then you're asking for one that specifically addresses the [root.]

LAURIN WEISSINGER: Yes, that was part of the root zone management, and we talk about disaster recovery plans. And there is a general one, and the question was – and we got an answer this morning – does this plan also include root zone management, and the answer was yes.

NORM RITCHIE: Okay.

LAURIN WEISSINGER: So I would say let's merge it to one recommendation.

NORM RITCHIE: Okay, so that's not so much a recommendation, it's basically just carry on.

LAURIN WEISSINGER: Yeah.

NORM RITCHIE: Is recommendation the right word?

RUSS HOUSLEY: Okay, we've been watching Laurin type the merging of 40 and 27, so 40 will be empty, 27 will have all the meat. Anyone have concerns about the – from a consensus perspective on 27?

NAVEED BIN RAIS: I'm just wondering, are we talking about only a plan, DR plan, or we are talking about DRMS for example, disaster recovery management systems? Do we require something like that? It might include –

LAURIN WEISSINGER: Okay, here we are talking only about disaster recovery plans as an outcome, and the process of disaster recovery, it's part of the business continuity management that we referenced in the beginning of the security part.

NORM RITCHIE: [inaudible].

LAURIN WEISSINGER: Yeah, I would say [let's reference it] because there is business continuity in general, and here we are only reference to disaster recovery plans.

NORM RITCHIE: Yeah, you were talking about the same document [inaudible].

LAURIN WEISSINGER: Yeah.

NORM RITCHIE: [inaudible].

LAURIN WEISSINGER: [inaudible] Yes.

NORM RITCHIE: [inaudible].

RUSS HOUSLEY: Okay. Are we ready to move on to the next one? Okay. So the next one is 1.3, and this is name collision, and this is Denise. Can you tell us where this ended up?

I don't think this is recommendation 28. Recommendation – oh, I see. Wrong –

So Lauren, the suggestion is we expand 28 to cover both abuse and what we called systemic abuse yesterday.

LAURIN WEISSINGER: That sounds good, but someone else would have to edit it because I'm still editing 27. Okay, Denise.

DENISE MICHEL: We identified a lot of confusion and concern about the bigger and more systemic name collision problems like auto discover, and we don't know who's responsible for addressing them, how to report them, who to report them to, who's responsible for addressing them, what the state of SSAC's work on this is and how we can contribute to improving the space. So, is it asking the board to direct SSAC or staff to create a plan? Or I'm not clear what the step would be here.

SCOTT MCCORMICK: One of the things that we as well as a lot of startups have been pushing is a single point for input to an organization for security-related matters, and so we started [security@] as kind of that focal point, and that's something that right now if you go onto the ICANN website, there's really no single point to report things like that, whether it's vulnerabilities, incidents, systemic issues that affect security.

It really boils down to, I think, pushing a single point like that, and I'm not sure – I don't know if ICANN has as security@ address, but that's something that I think we need to probably push through this, is something like that so we can kind of bring this all together under one roof, or at least have one point where the community can send information. Because like you said, [inaudible] this point.

DENISE MICHEL: Yeah.

RUSS HOUSLEY: So just a thought, as you were speaking, maybe the CSO-CISO description should say it should be expanded to include the management of a single reporting place for security-related things, and then be responsible for the follow-through after the report.

SCOTT MCCORMICK: Absolutely.

RUSS HOUSLEY: You want to put some text there?

NAVEED BIN RAIS: Are we advising ICANN of producing it, or producing and publishing it? Like it might be two different things, and just to be more specific, do we require them to publish it somewhere, or just produce it and use it? I'm supposing everything has to be published.

RUSS HOUSLEY: The result from the published plan is what it says. So, ICANN should publish the plan, milestones for the studies and then link the results from the published plan.

NORM RITCHIE: There is a page that says how to report security [inaudible].

SCOTT MCCORMICK: Yeah, but that's vulnerabilities, right? By the way, there's two separate ways to report it.

NORM RITCHIE: Yeah, [there's four.]

SCOTT MCCORMICK: Is there four? Even better.

DENISE MICHEL: Is that just ICANN systems?

NORM RITCHIE: It's everything.

SCOTT MCCORMICK: It's everything. But my point being that it's not – when you're talking about collision, it's not necessarily – it's a vulnerability on a global scale, but if somebody has another security issue, issues are different than vulnerabilities, right?

RUSS HOUSLEY: [inaudible].

SCOTT MCCORMICK: I will say that if you typed in ICANN.org/security, which I would expect to be a reference, it does take you directly to how to report a security issue to the ICANN Organization, or how to report security issues.

RUSS HOUSLEY: Yeah, that's the link that Norm just posted in the chat.

NORM RITCHIE: On this recommendation, do you think that the board understands what NCAP research report would be? Is this too technical for them, board and community?

DENISE MICHEL: I don't know. Maybe Scott knows. But I would hope that if they don't understand, they would ask.

SCOTT MCCORMICK: What's that?

RUSS HOUSLEY: There would also be discussion for each [of these, right?]

SCOTT MCCORMICK: Well, we need to define these [inaudible] definition to.

RUSS HOUSLEY: Exactly.

SCOTT MCCORMICK: I would definitely – if it was the first time it's being used in here, I would definitely spell it out and put it in parentheses.

LAURIN WEISSINGER: Just a note, Danko just posted in chat, "my understanding is NCAP was mostly discussed in relation for the new gTLD subsequent procedures. Certainly, there – I assume – is also an SSR security aspect."

DENISE MICHEL: Part of my concern is I did –

DANKO JEVTOVIC: [inaudible].

LAURIN WEISSINGER: Speak up, please.

DANKO JEVTOVIC: Sorry that I'm interrupting with the voice. I thought it is easier to type it just in chat, but I did send a link about this decision by the board for the name collisions study, but my comment was this is mainly for the SubPro and you are mostly discussing the security aspects. So it's a bit related, but it's not replacing your discussion, of course. Sorry to interrupt.

DENISE MICHEL: Thank you. So I think a part of my issue as well is that I did report a sort of systemwide name collision issue to OCTO staff and it's been a year now, I haven't heard anything back, and the vulnerability is still live. So there's a policy component to this as well.

SCOTT MCCORMICK: Yeah. I think this goes back to policies and procedures within ICANN, right? So what's the [SLAs,] what's your classification, what's your matrix on that?

RUSS HOUSLEY: I think that c-level thing where we said single place to report and establish the SLAs and measure them.

SCOTT MCCORMICK: Yeah. And I'm thinking from a final reporting – I know we talked about a mind map before and not really wanting to do that, but I feel like there's a lot of dependencies between these. So linking those somehow in showing the dependencies would be good.

RUSS HOUSLEY: We have to figure that out, because it would be bad for the board to say we're going to implement one and not another, and then find out they have a huge dependency between them. So that's why we have to do that.

Okay, are we done with this one from a consensus perspective? Any concerns? Okay. Laurin, the next one's yours, and that is –

LAURIN WEISSINGER: Just reading. 28 again. [inaudible].

RUSS HOUSLEY: It's 28 again?

LAURIN WEISSINGER: I just want to read it before I –

RUSS HOUSLEY: Well you should have been doing that.

LAURIN WEISSINGER: Okay, looks good. Which one is the next?

RUSS HOUSLEY: Then next one is 1.4, and it is root zone change management and verification.

LAURIN WEISSINGER: Yes. There are multiple recommendations attached. Boban helped me with this [and we found] all of them. So there is one on the IANA portal draft recommendation 14. This is essentially about the portal, website, that is used by TLD managers to ask for changes. We saw that it's essentially a username, password, nothing else. So we're recommending that to change.

Furthermore, right now, essentially their response to this is via an encrypted e-mail, and we're kind of saying, well, either don't use e-mail or use something like S/MIME to ensure that this cannot be read or otherwise abused.

RUSS HOUSLEY: So, is there a confidentiality concern or just an authentication and integrity concern? In other words, are you asking for signature, or are you asking for signature and encryption?

LAURIN WEISSINGER: It should probably be also encryption, because otherwise, you would be able to access the confirmation link, and then ... well, yeah. We shall add.

Boban, whichever one's – I think 15. Right?

BOBAN KRSIC: Yes.

LAURIN WEISSINGER: Okay, so the other one is 15, which is essentially develop baseline security requirements for root server operator and operations, and report on those. This should again be in close cooperation with RSSAC and the operators.

Further note, because the operators are independent to quite an extent, the idea is essentially that ICANN will kind of report on what are the current best practices or baseline security requirements and then kind of say that has been done to promote those, because that's as far as we can go.

RUSS HOUSLEY: [inaudible] this is the two recommendations we should make here?

NAVEED BIN RAIS: So as part of RSSAC 37 that was published recently, they talked about this [an infrastructure comment to all] root server operators. And there is definitely a recommendation coming from there, and KC is working on that. Maybe [inaudible] today. So I would think that this should have been merged with that one, because that infrastructure lacks security, so they don't have any function related to security of the root servers as such.

So even there, we are proposing to include security as a function there, so I think this can be merged with that later. It's not there yet in the recommendation because I'm hoping KC would add and would share it today, I would think.

RUSS HOUSLEY: I guess we'll have to see what we get. Yeah. Okay. So let's move on to 1.5, which is TLD label management. Boban.

LAURIN WEISSINGER: I think some of it was the same and some we integrated, so essentially, what came out of this, I think there's some of that is in 16 as Boban said. Wait, wherever else? And then there's some stuff in 20, which is the provisions against abusive naming. So this is essentially distributed along other recommendations. And yes, [inaudible] also is – oh, this is also 15 and 14. Which you're currently changing.

Okay, there's also recommendation 29 which isn't hardening root, which also relates to recommendation 15. That refers to essentially the

three groups that Boban, Zarko and I looked at, which is root zone management, TLD labels and names – 1.6 as well and [inaudible].

Furthermore, there's also a link to stuff like IANA measures, root SSR metrics, root zone measures, root zone delays. So this is essentially the whole group of data stuff that is 30 to 35, but we really have to kind of look at those and merge them because they're essentially the same recommendation multiple times.

DENISE MICHEL: No, not even close.

RUSS HOUSLEY: No.

LAURIN WEISSINGER: That's why it says please develop this in close cooperation with RSSAC [and the] root server operators.

DENISE MICHEL: Norm, are you suggesting [inaudible]?

ALAIN AINA: Russ, can I?

RUSS HOUSLEY: Sure.

ALAIN AINA: Probably go back to recommendation 14 on the IANA [portal.] So I don't know if we will discuss this with the IANA stuff, but IANA has started to implement a new root zone management portal which includes [certification] etc. So I don't know if – because this recommendation didn't say anything about these kind of existing services, but I remember that they were doing these kinds of things, and even we as RIR, we roll in such system with IANA so that then [every change, we use certificate,] so we no longer use the e-mail. And we are supposed to extend this to the TLDs. So maybe – I don't know if we have to confirm it, that this system is in place, and they're supposed to migrate from the e-mail to that system or they've abandoned the system. So we need to get an update of this one.

DENISE MICHEL: Do you have the ability to ask them?

LAURIN WEISSINGER: So when we looked at it in Japan, it wasn't available. It might be the case now, who knows.

NORM RITCHIE: Another question in this regard: can L-root handle the entire load of the root? Like should someone walk up with a bag of money to all the root operators and say, "Here, do this," all you have left is L-root, can that handle the entire load?

LAURIN WEISSINGER: Are you saying L-root should have the ability to handle the entire load?

DENISE MICHEL: Logically. If L-root's the only one that they have control over that has SLAs and best practices and you can actually harden it, the only one you can certify, then logic takes you to that should be able to handle the full load. If you can't –

RUSS HOUSLEY: If who is contracted?

NORM RITCHIE: Verisign.

RUSS HOUSLEY: No. They're contracted to do what they called the publisher.

NORM RITCHIE: Right.

RUSS HOUSLEY: Right. But the A-root part of Verisign is not contracted.

LAURIN WEISSINGER: So [they're following only principles, and they reference those] principles on the website. [All roots have principles, it's RSSAC 37 document. How [inaudible] root server is another one.] So there are different principles and they follow them, and that's it. They're not contractual obligations.

NORM RITCHIE: Yeah, so I don't know if this falls under disaster recovery or whatnot, but it may be that the L-root should have the capacity to assume the entire load of root traffic.

LAURIN WEISSINGER: So recommendation 29 is essentially on hardening strategies on the root, and kind of making L-root kind of best practice. So we could rewrite that into and make sure that if everything else blows up, this thing holds.

RUSS HOUSLEY: [Why is it not just a bullet?] Ensure the capacity is bla bla.

DENISE MICHEL: Yeah, that's what I'm thinking.

LAURIN WEISSINGER: Because the whole thing right now is like to write a document about hardening strategies and how this is best practice. There is nothing on kind of ensuring availability.

RUSS HOUSLEY: So don't you say writing the best practices for disaster recovery – I'm sorry, I'm reading the wrong one.

LAURIN WEISSINGER: 29.

RUSS HOUSLEY: 29 is where you talk about SSR risks, [just say] availability and SSR risks. Or, well, maximize availability and minimize SSR risks. Alright, so but now the concept is there. So I could ask the question about whether we have anybody who has concerns with this direction.

NORM RITCHIE: [inaudible].

RUSS HOUSLEY: It is a nonstarter.

NORM RITCHIE: [inaudible].

RUSS HOUSLEY: I could tell you that one.

DENISE MICHEL: Next.

RUSS HOUSLEY: Yeah, exactly. NS DS record management. Boban, that is topic 1.6. Okay, so in doing that, they were merged, so it's the same list of recommendations, so we're done with that one. So moving to section two, best practices and system hardening of L-root. Is that –

LAURIN WEISSINGER: 29.

RUSS HOUSLEY: 29, or is it anywhere else as well? This is DNS SSR section two, item one.

ALAIN AINA: On the 29 and [inaudible] regarding root, I think there is one thing I want us to keep in mind and be careful [inaudible]. ICANN manage L-root, but ICANN also has some responsibility in coordinating the [RSSAC.] But if you look at most of the time, there are always conflicts between ICANN and RSSAC. [inaudible] if we want to talk about L-root, we directly mention ICANN and what ICANN should do relating to L-root, but when we are talking about the root server system, so if we're trying to give responsibility to ICANN Org, the RSSAC people would object to it.

DENISE MICHEL: [inaudible].

ALAIN AINA: Yeah, the RSSAC people, so we just need to be careful. If we are talking about L-root, the thing there is, are we talking about hardening L-root or the root in general? So if the root in general, then [it goes beyond] ICANN Org. So maybe we have to be [inaudible] knowing who has responsibility. Okay, so [inaudible]. Are we talking about the L-root? I saw someone change it to L-root. Okay.

DENISE MICHEL: And did you have any other recommendations, Alain, about hardening the root system overall that you wanted to consider here?

ALAIN AINA: Okay, current situation is the RSSAC [27] document is on the table, and ICANN, the board issue a resolution – I don't know if you saw the resolution, there is a resolution from ICANN board on the root server strategy. Then if you look at the resolution [about the] root server strategy, the content is to add ICANN Org to develop a strategy for L-root itself. And maybe [inaudible] resolution 2018-091510, ICANN board resolution 2018.09.15.10. I think it's good that we look at it.

So just to say that something is going on, and then ICANN board ask ICANN staff to work on how to harden to protect the L-root to be more resilient, etc., and then this attached to the recommendation and implementation of the L-root people.

So the RSSAC people are saying that instead of ICANN doing this standalone, it should be done as something global for the root server

system itself, not only for the L-root. So there are some [animosities] going on there. So just to see how we [inaudible]. But if we go back and as it is now that we are now addressing only the L-root, I think maybe make our life easier if we focused on L-root alone and make our life easier.

LAURIN WEISSINGER: Alain, just to note, this is kind of in recommendation 29, because the last sentence essentially says at the moment no such documents exist, and clear summary of best practices [would support a more secure root zone.] So if they did it and they said what they're doing, then other people could pick it up. So it's like an indirect effect.

NAVEED BIN RAIS: We also need to understand the relation between ICANN Org and the L-root itself. Is it like a subsidiary of ICANN, is it an independent body, is it governed by independent board, or it's the ICANN board who oversees that? And there's all these functions if it has full power on it, right? Okay.

ALAIN AINA: You saw the resolution. So my question is, do we refer to that resolution? Because it is already given [instruction] to ICANN to work on hardening the L-root. So you saw the resolution?

DENISE MICHEL: So I'm reading the resolution. It's 2019.9.16.10, the board instructs the ICANN Org as the operator of the ICANN managed root server-L-root to work with the community to finalize a strategy to reduce effects of attacks on the IMRS and once finalized, directs the CEO to begin implementation of that strategy by developing a project plan with associated timelines and potential expenditures for subsequent board review and approval.

So it's been about a year. Do you know where they are with that plan? [inaudible]? Yeah, that's a good point. Maybe we should ask what the status of that is.

LAURIN WEISSINGER: Are people now happy with recommendation 29?

DENISE MICHEL: Yes. I think for now, we would note for staff that – I just dropped a link to the board resolution into the comments of the document on 29, if staff could please ask the appropriate staff what the status of the implementation of that – and if – yeah, we would like to –

RUSS HOUSLEY: Yeah, so you're going to take that one. Thank you. [Sure, that goes to Terri.] Okay, for 2.2, we're waiting on KC, I believe. Alain and Naveed, you're both working on that one as well. Is that correct?

NAVEED BIN RAIS: Yeah. Just a few comments on that. The bottom line that we found is that this RSSAC 27 talks about the governance model of the RSS, but apparently there's no implementation plan about when this is going to happen and then what [inaudible] this is going to happen. So the need would be to come up with a specific timeline about implementation of this, even in 2018 study, the office of CTO, they said that they're planning to implement this, but after that, there's no implementation status on that. So that's the main thing.

The second is that there's no direct security framework in that document as such. It has five different functions as a model, but it seems that the security of the RSS is not priority or it is implicitly understood as a sub-function of any of that. So there is no – it's kind of similar to what we discussed before as I think recommendation 15 somewhere, we're asking for a security framework about this root server system. So that would kind of overlap with recommendation 15.

DENISE MICHEL: That's a great point.

DANKO JEVTOVIC: If I may chip in –

RUSS HOUSLEY: So can you put some text in there to cover that?

NAVEED BIN RAIS: Yeah, I sent my text to KC, and I'm waiting for her to integrate all that.

RUSS HOUSLEY: Thank you.

NAVEED BIN RAIS: I think Danko –

BRENDA BREWER: Danko, go ahead.

DANKO JEVTOVIC: Okay. Thank you. I was just trying to follow discussions, so I might repeat some things that are obvious, but due to the root server operators' independence, this is very important point for both technical stuff and the other, and I've dropped the link to the new statement on the [root server operator independence that is like five there is all,] so that might be of interest.

Speaking of the L-root system, this is ICANN function, it is done by the Org. Of course, the board does the oversight, but this is something that we can directly influence. But the operation of other root servers cannot. And as I said, there is recommendation number 37 for the SSAC, and this is a voluntary process. And also, there is evaluation parallel to that which is happening due to the review of the RSSAC that is happening.

So regarding the current updates, I can paste into the Zoom chat some information about the current status of the process leading to the implementation of the RSSAC 37, but this is not something that should be pasted back into the document, it's just for your information if that is okay. Thanks.

DENISE MICHEL: Great. Thank you.

RUSS HOUSLEY: Okay, so we're going to move to 3.1, which was Eric and Naveed working on accountability and transparency. Yesterday, we said we cannot find text on this topic, and it seems to be addressed by the recommendation regarding outreach to the research community with the yearly report. Remember which recommendation that was so I can look – here it is, it's 19. So it's pretty short. Take a look at that.

LAURIN WEISSINGER: So on that note, we agreed to kind of look at the list of topics that we want to mention so that it's not complete. So we definitely have to look at the specific topics we're recommending.

RUSS HOUSLEY: Okay. Why don't we take a break here, grab some lunch and then do a working lunch? Because we're going pretty slow here. Alright, so take five or ten minutes to gather your food, and then we'll reconvene. Probably want to stop the recording.

Okay, welcome back. Hope we can be productive while we eat. The next section that we're working on is section four. Section four, item one is SLA compliance. Kerry Ann says she's shared draft text. I don't remember – whatever recommendations her text had are not in the – can you tell us where to find that? I think it starts on page seven. It says KB:SA compliance.

Oh, I see. Okay. So Laurin, there are three recommendations here that need to be pulled over. So the recommendations are on page 11.

LAURIN WEISSINGER: [inaudible]. Sorry, I don't want to touch my keyboard right now. At the bottom, there is a section [inaudible].

RUSS HOUSLEY: So basically, these three recommendations have to do with – the first one is having a specific team within Compliance for dealing with SLA metrics. Second one has to do with having a team within Compliance that focuses on the requirements for privacy and how to facilitate the needs of law enforcement related to WHOIS. And the third one has to do with SLA renewal clause, but not automated, but reviewed in year four with the intent to measure compliance by the registrar and inclusion of requirements to strengthen security and resilience. So basically that automatic renewal part gets put into section three, into the third of these recommendations. So that's the recommendation she's put forward here. Any people have concerns with any of those?

LAURIN WEISSINGER: The measures we have here are at least partly in a different recommendation. I'm not sure which one. I'm trying to figure it out. It might be 16, SSR concerns and contracts. That looks about right.

RUSS HOUSLEY: It will have to be reintegrated in there. But it's a slightly different direction.

LAURIN WEISSINGER: Yeah, so action item would be integrate Kerry Ann's SLA text into recommendation –

NORM RITCHIE: I'm just looking at financial incentives, and it's unclear, at least to me, what the consensus – how do you achieve one, how do you get that.

LAURIN WEISSINGER: So I think if you fulfill all the conditions below, you get 5% off.

NORM RITCHIE: Okay.

LAURIN WEISSINGER: At least that's my reading.

NORM RITCHIE: The financial [inaudible] is totally wrong. Well, registries, registrars and ICANN make money on domain name registrations. If we ask them to curtail abuse, they actually have less registrations, and therefore, the amount of money goes down [inaudible].

LAURIN WEISSINGER: That's why [inaudible].

NORM RITCHIE: [inaudible] financial impact on – no, but the money in the entire pool. [inaudible] And furthermore, the impact of abuse is not borne by the registries, registrars or ICANN, it's borne by somebody else. It's just a wonky financial model. So we're actually then asking that we're going to take more money out of it.

RUSS HOUSLEY: I wasn't sure where you were going.

NORM RITCHIE: No, I don't know if – I have my doubts that they will agree to financial incentives given that they're apparently tight on money now, is my concern. And if you assume – let's say there's 10% abuse of domain registrations out there, then you take 20% [off the revenue] for each one, that's a sizeable chunk of money.

So I'm doubtful that this will get through. However, I would support it.

DENISE MICHEL: Which one [inaudible]?

NORM RITCHIE: Oh, give them 5 cents off per domain, basically. It's page 26 of the recommendation. Although I support that model, I'm doubtful that it's going to get approved. What I'm saying is I don't want to tie other recommendations to here.

RUSS HOUSLEY: Now we're getting to something I understand. So Laurin, we don't want to merge it completely. You can keep the financials [on its own.]

DENISE MICHEL: I think this is a great –

LAURIN WEISSINGER: No, it –

DENISE MICHEL: Yeah, I think these should be separable. I'm a little more optimistic, I think, than you. A majority of the registrars and registries spend a lot of time and money and resources on doing the right thing and mitigating abuse. And this is an opportunity for them to recoup some costs, and I would expect them to be supportive, which is an important part of the community when it comes to –

NORM RITCHIE: Yeah, I get the registries and registrars being supportive, but this is also the money that's going towards ICANN that – it reduces the ICANN funding.

DENISE MICHEL: The board has already once taken a chunk of auction proceeds that are at around $250 million sitting there gaining interest. So it's all relative.

RUSS HOUSLEY: Okay, the next one, we're waiting on KC's text on the propagation delay. The one after that, number three, we deleted yesterday. The one after that is KPI for SSR measurements, and that is Laurin.

LAURIN WEISSINGER: Okay. This is one of the difficult ones. Essentially, what's happening is we have multiple recommendations that speak to measurement and data. Multiple related ones. So on data, we have something on root SSR metrics, SSR measurement, IANA measures, summary root zone measures, root zone delays, which are recommendations 30 to 34.

They're essentially the same in text, and I would propose let's do one and just do a list of the things that are under this. So number one, and then there is number three, so recommendation three, which is on metrics as well. So that's related.

Number three is slated for being rewritten, but it hasn't been rewritten yet, which means it's still in there.

DENISE MICHEL: I think these are good and useful. I have a question on whether you think it's feasible to have a meta recommendation on metrics and measurements and have these as sub-recommendations under that. Would that – do you think that's useful?

LAURIN WEISSINGER: That's my idea. Yes.

DENISE MICHEL: Oh, yes. Great. Good. Brilliant minds.

RUSS HOUSLEY: Okay. Given that all of those, we have talked about before, except for three –

LAURIN WEISSINGER: No, three also.

RUSS HOUSLEY: Oh, yes, three is back in. So we've talked about all of them before. So I'm assuming none of that has changed.

LAURIN WEISSINGER: My apologies, I forgot to – there's also two on measurement which are 24 and 25. So measurement and data is 24, 25, 30, 31, 32, 33, 34. It is also in the table, I just didn't [say] it.

RUSS HOUSLEY: Okay, so we have not talked about 24 and 25 yet, so let's take a look at them.

LAURIN WEISSINGER: Okay, and I would say that essentially, the data team should go ahead and try to reduce the number of recommendations.

NAVEED BIN RAIS: Laurin, I was just wondering, when we say that we should publish about the health of these metrics, do we need to provide a frequency of the update, like is it an online portal, or it is getting updated like quarterly or annually or monthly? Because I don't find that information in this text. So are we just saying that we need to come up with metrics and sort of publish them into a directory? But do we need to specify that frequency?

LAURIN WEISSINGER: In the global SSR measurement – that's the one you mean, 25, or 24?

NAVEED BIN RAIS: I mean 24.

LAURIN WEISSINGER: Oh. So you would want to have like a kind of this is the minimum frequency at which data has to be released?

RUSS HOUSLEY: Well, or since the call's for community discussion, we can say that we want the community to decide what frequency is adequate.

NAVEED BIN RAIS: That's more political. Yeah. Because when we say health, it can vary every minute, every hour, every week. So when we are maintaining an online portal, it should be online and reflect about the current situation.

NORM RITCHIE: Isn't there a health indicator initiative that's already going on? [inaudible] or something? [What? it's always] broken? [inaudible].

LAURIN WEISSINGER: I think the key here is to kind of have something on the more technical side as well, to kind of see what is available at what times. So if you go down to the more detailed ones, as in 30 to 34, you can see the type of stuff that this kind of cluster is interested in. So stuff like availability for IANA-related stuff, some remeasures of what's going on the root zone, this type of usually more technical information. Essentially, multiple things. So this would help with like monitoring security, this would help with PDP processes, because it would allow review teams, etc. to

essentially look at availability over time. It would allow for researchers, academic or otherwise, to look at the data, study what's going on, etc.

RUSS HOUSLEY: Are you satisfied, Norm? I can't tell.

NORM RITCHIE: I'm trying to think of what objections are going to come for any of these [inaudible] or not, and in this case, it'll be, “Are we measuring things for the sake of measuring, or is there a purpose for this?”

RUSS HOUSLEY: I thought we had that discussion in LA, and I remember Eric pushing back pretty hard on that.

LAURIN WEISSINGER: Yeah, I just want to say from the academic side of things, there is definitely a lot of stuff you could do if you had access to data. And for matters of transparency, accountability, all that kind of stuff, it is also helpful to have at least something, because right now, this would be very little on certain aspects of this stuff.

RUSS HOUSLEY: [No twos.] Okay. I'm sensing that we’re okay on this one. Okay, so next one then is 5.1. Norm, this one’s yours. Transparency, respect to abuse. This is DAAR?

DENISE MICHEL: There is a number of elements that fall under transparency with respect to abuse. A number of initial draft recommendations were added at the end of the Google doc for further discussion, but this covers not only more transparency and more aggregated data from DAAR being published on a regular basis, but also covers better transparency with respect to compliance action, audits and so forth. It also includes transparency with respect to abuse-related actions and operations with contracted parties, so [inaudible] a number of things.

RUSS HOUSLEY: So looking at this recommendation 20 has to do with provisions against abusive naming and the first bullet has to do with the DAAR reporting, which it notes is not a perfect process. So clearly, 20 is part of this. I'm not sure what else to put here.

DENISE MICHEL: So when we have time, we need to integrate some of the recommendations that are tacked on at the bottom and integrate those in.

RUSS HOUSLEY: Is there any at the bottom that are related to the transparency parts that you want to highlight now?

LAURIN WEISSINGER: I think this one would also kind of deal with some of the general compliance stuff where we also have this transparency regarding enforcement action, etc., which will be difficult to integrate now because of the next two. We're still waiting on answers, but we only have draft recommendations right now that kind of came in this morning.

NORM RITCHIE: It's kind of twofold. There's two parts to this. One is that DAAR is a tool. What we're really talking about here is compliance and abuse. So that's why it's a bit muddled on how we present these issues about being proactive on abuse and compliance measures, and DAAR is below that as a tool to inform those. So that's why I'm a bit – I don't think it's the right way to approach it, just saying, "Make these changes to DAAR" because that's not what we're really talking about.

RUSS HOUSLEY: Right. I see.

NORM RITCHIE: Yeah, so it's really –

LAURIN WEISSINGER: [inaudible].

NORM RITCHIE: Yes. And DAAR is the tool to help you with it.

DENISE MICHEL: So I don't disagree, but there are other reasons to improve the DAAR publications. It absolutely can be used by Compliance, but it also importantly can be used by the community. Community's better informed when they make policy, or even businesses and entities on the Internet that want more visibility into high abuse levels in registrars and registries so they can factor that into any security measures that they want to implement.

So I think it has a range of uses. So I was thinking of combining abuse data related – data and transparency related to abuse as one bucket, and then compliance as another bucket. But I wasn't thinking of combining DAAR and compliance activities.

NORM RITCHIE: What I'm trying to do is avoid trying to build a tool for them. [I could do that, say you need] more sources of data in there, you need to make that data public. But that's to get an outcome. So that's what I'm trying to focus us on, what are those outcomes we're after, then say these changes need to happen to DAAR rather than say these changes have to happen to DAAR separately.

LAURIN WEISSINGER: So why don't we include it in the data and measurement bucket? Because that would be on publishing the things in DAAR and then we do a second one on compliance, and there might be additional

requirements on DAAR from there that are independent of the kind of sharing and measurement for [DAAR in] general.

DENISE MICHEL: And so if we start the data and measurement bucket with a broad description of here is the reason why we're recommending this, here's the impact we're aiming for, and to achieve this impact, actionable data – here are the following changes we'd recommend. Is that what you're thinking of?

LAURIN WEISSINGER: Something along those lines. We would have to see how it works out in practice.

DENISE MICHEL: Norm, were you thinking about something else?

NORM RITCHIE: DAAR is specifically geared towards abusive registrations. So just to lump it with the other measurements which are more about stability and resiliency, I don't feel is the right [clumping.] It definitely falls under compliance. It definitely falls under informing policies. I don't know if that's an SSR issue or not, but it definitely informs policy.

And I'm wholeheartedly supportive of enhancing DAAR, but I'm just trying to figure the right way of presenting that and selling it.

DENISE MICHEL: I wouldn't object to putting it under compliance. A number of our compliance-related recommendations go towards more transparency and certainly more proactive and systemic action. So I certainly see a nice pairing there, and we can also note the additional uses of DAAR, but still group it with compliance. It's going to be a big section. Well, I can work with Laurin and Norm to synthesize, reorder and edit this group of recommendations.

NORM RITCHIE: Yeah, I think I'd like to add one more recommendation, and it's to look at the follow-up report. So if at one point in time you have abuse, then those are actioned, that's when you get to the point where they're actionable and they're actioned and there actually is a follow-up on those to see that those domains have been actioned.

DENISE MICHEL: Yes.

LAURIN WEISSINGER: Norm, recommendation 38, I believe, has that. This approach to include follow-ups and compliance action from the previous quarter. That's what we have right now.

RUSS HOUSLEY: Okay. Have we come to consensus here? Clearly, there's work to be done, but have all the topics been gathered?

DENISE MICHEL: Yes.

RUSS HOUSLEY: Great. I can't see them.

NORM RITCHIE: [inaudible] more visibility.

RUSS HOUSLEY: Alright. [I'm outrunning my sniffer.] 5.2, reactive versus proactive. Laurin says this part needs to be integrated with the DAAR section. Denis, you have the lead on this one. Can you point us to the recommendations where they all go into the bottom we just talked about? 5.2.

DENISE MICHEL: Yeah, several of the recommendations at the bottom address this point. It's covered, but it needs to be, again, synthesized and edited down. So I'll be doing that.

RUSS HOUSLEY: Thank you. Okay, 5.3, it's Denise again, leadership. Give ICANN Compliance a big stick. This also seems to overlap with the SLA ones from Kerry Ann.

NORM RITCHIE: [inaudible] compliance bucket.

DENISE MICHEL: Yeah, it's a big compliance bucket, but we've got lots of text we need to synthesize and edit.

RUSS HOUSLEY: Okay.

LAURIN WEISSINGER: [inaudible] and we have follow-up questions on – yeah, sorry about that. We have to somehow magic [inaudible].

RUSS HOUSLEY: Okay. So the next one –

DENISE MICHEL: I sent you an e-mail on that, Norm.

NORM RITCHIE: [inaudible].

RUSS HOUSLEY: 5.4, which has to do with IDN, and that would be recommendation 20.

LAURIN WEISSINGER: Yeah, merged.

RUSS HOUSLEY: Yeah, that's fine. I was like, wait, this isn't [inaudible]. There it is. The IDN part is the second bullet. Any concerns?

DENISE MICHEL: On which one?

RUSS HOUSLEY: 20.

NAVEED BIN RAIS: I just have – I see ICANN should continue investigating – again, something I remarked earlier – should avoid using word "continue to do something." We should rather specify, "Okay, this is what you have been doing," and that would come in the pretext of the recommendation, and then we say, okay, let's do this now, kind of be more specific [inaudible] the first paragraph of this.

RUSS HOUSLEY: I think the first bullet is keep doing what you've been doing, and then the next –

NAVEED BIN RAIS: Keep doing might not be a recommendation. I don't see it as a recommendation that if it's something that they're doing, it can come in

the pretext. [inaudible] recommendation, what is the background? And then we can say, okay, because I see something new here as well include this type of abuse in the DAAR reporting and develop policies. This I think – as I understand is not something that they're doing. So it's kind of mixing both.

RUSS HOUSLEY: But I think it builds on the "continue doing", so if they were to stop doing, I don't think – right? I think that's why it's written this way. That's how I read it. If that's not the intent –

NAVEED BIN RAIS: My –

RUSS HOUSLEY: [inaudible]?

LAURIN WEISSINGER: Yeah, I think so.

NAVEED BIN RAIS: My point is we can say that extend to this or something like that rather than just continue doing.

LAURIN WEISSINGER: [inaudible].

RUSS HOUSLEY: So I think it's "continue investigating," and it's asking for development and mitigation of best practices.

NAVEED BIN RAIS: I would rather say, should investigate more or something like this rather than continue investigating, or enhance the investigation, kind of that, because the second half of this paragraph is asking ICANN to do more, actually, in a way.

RUSS HOUSLEY: How about build upon the current activities?

NAVEED BIN RAIS: Yeah, [inaudible].

RUSS HOUSLEY: Keep calm and carry on.

LAURIN WEISSINGER: [inaudible] I put in there yesterday.

RUSS HOUSLEY: Yesterday [inaudible].

LAURIN WEISSINGER: Yeah, I thought we'll have it for coffee, and then didn't happen.

NORM RITCHIE: [inaudible].

RUSS HOUSLEY: Alright, Boban, [inaudible]. Okay, is there any other concerns here? Okay.

NAVEED BIN RAIS: [inaudible].

RUSS HOUSLEY: Laurin's back, so we can move to section 6.1, which is about testbed of software variance. You're reporting on this one.

LAURIN WEISSINGER: So that's recommendation 13. Just for context, ICANN is developing something along those lines, so we're just kind of saying, "Well, they should continue development of [tools for] DNS regression testing, kind of underlining the importance of being able to test different configurations of software versions. Platform is in development but isn't complete. So we're kind of saying, well, get it done. Recommendation 13.

RUSS HOUSLEY: Are you reading your e-mail or are you reading recommendation 13? I can't tell, [inaudible] bunch of people staring at screens. Maybe you're reading the most recent [inaudible].

NAVEED BIN RAIS: And this is kind of not clear, because we need to have boundaries between what is being done and what should be done, like continue to do something, again, does not really reflect on what is – like what is actually happening and what we should extend that into or build that upon.

ANGIE GRAVES: I have a question. And my lack of familiarity with the document at the moment may be the reason for this question, but wouldn't the first part of what you're saying be in the findings? And then the recommendation would be reflection of the finding, plus – okay. Thank you.

LAURIN WEISSINGER: So just to answer this, what's happening – and this is why we use the "should continue" – is that we know something is being developed right now. We had a chat with the person who is doing it, but it's not complete. And when we talked to them, it was kind of like, "Oh, yeah, this and this I've done, and these things, I will be doing," etc. That's what why we're saying "continue." And we can't really say this is what has happened right now, because it's like a process. We're building it right now.

NAVEED BIN RAIS: I don't disagree with that, I'm just saying that we should keep in mind while we put that into the recommendation that in the pretext that precedes this recommendation, we should exactly specify that the efforts are ongoing regarding that things and with all the references that we have. And then we say that, okay, we should continue doing this, or a better way might be to ask ICANN to make sure that this is done, which is kind of implicitly saying that, okay, let's continue doing this and make sure that this is done. So it is an ongoing thing.

Like if it supports by some [inaudible] which actually reflects that this is ongoing, then it's fine. But I just would like to see the justification against that, like we have proof or references that it's an ongoing activity, and we just want it to continue.

LAURIN WEISSINGER: So I'm essentially just looking at Paul Hoffman's Git and trying to see if there's anything we can kind of link.

RUSS HOUSLEY: I think what we're really saying is get her done.

LAURIN WEISSINGER: Yeah. Right. Although there is one important issue, which is when we talked to Paul, not everything Eric and I kind of talked about and thought was particularly important was that – that's why we're like specifically saying allowing the testing of different configurations and software versions. [So this is why.] We don't really know how that works. We know that Paul is the one who is the kind of main coder,

designer behind it. Not sure how this was informed prior to this project starting.

RUSS HOUSLEY: Must be real, it's in GitHub. Okay.

LAURIN WEISSINGER: [inaudible].

NAVEED BIN RAIS: So when we say that – and focus on allowing the testing and whatever follows that, are we saying that this is something that is in addition to what they have been doing? [Like just] need a line to draw between what is happening and what additional we are recommending. So, is it not that they're doing, or is it just repetition of [that] and we are emphasizing that it must be done?

LAURIN WEISSINGER: It's like a beta version right now, so it's not complete. So right now –

RUSS HOUSLEY: [inaudible].

LAURIN WEISSINGER: Yeah, well, maybe it's also alpha. So this is the thing, that's why we're just saying make sure that these things are in there. And make sure it's getting done, because it's clear they're doing it, you can go to the

GitHub. But we are saying, “Well, get it done and make sure these two things are –“

NAVEED BIN RAIS: I'm not saying about the completion of something. I'm just saying from the perspective of what they plan to do. Like if they plan to do this or not, we don’t know, right?

LAURIN WEISSINGER: We don’t know their plan.

NAVEED BIN RAIS: Okay. So this is kind of our input to that, right? So that’s [inaudible].

LAURIN WEISSINGER: [inaudible] make sure these things are possible.

NAVEED BIN RAIS: Then this is what I'm saying, so continue to do this, and focus on this, these are – I see them as two different things, right? One is, “Okay, let’s continue developing this, but make sure that you also include this.” Like you might focus on testing and all that. Am I understanding it correctly?

LAURIN WEISSINGER: Yeah. So I'm looking at text and recommendations, so I'm unclear what you would like to change. Because they're saying, “Should continue development of this thing,” we link the GitHub in the footnote, and then

we say, “And focus on [allowing the] testing of different configurations and software versions.”

NAVEED BIN RAIS: This text is confusing in a way that I can read it as ICANN should continue the development, that is one part, and ICANN should continue to focus on ... So that can be read like this. Or it can be read like completely two different things, like focus is not part of the continuation, it’s like our own input to that. So this is not distinguishable.

LAURIN WEISSINGER: Okay. That makes sense. So ICANN should ensure that testing of different configurations and software versions is implemented.

RUSS HOUSLEY: Okay. Any further concerns? Your mic’s still on, that’s why I'm not sure. Okay. Alright. We’re now moving to domain name hijacking protection. Zarko had the lead here. He's not here, so can either Denise, Norm or Boban – I don't know.

LAURIN WEISSINGER: Registry, registrar lock, stuff like that? because that’s in some recommendation.

NORM RITCHIE: Yeah. Multi-factor.

LAURIN WEISSINGER: It should be early. 16. SSR concerns and contracts, I think this is ... yeah, it's there.

RUSS HOUSLEY: In 16?

LAURIN WEISSINGER: Yeah.

DENISE MICHEL: We may not use the titles in the table to organize, right?

RUSS HOUSLEY: No, that was how we organized the work, not how we're organizing the [report.]

DENISE MICHEL: I just want to validate that. We have recommendations related to hijacking in a few different areas in the recommendation document, and I'll work with Zarko to pull those [inaudible].

RUSS HOUSLEY: Okay. Is there anything we need to revisit on the DNS SSR? I know we've got several that need work, and we've got a couple where we're still

waiting for KC, but the other ones, I think we're ready to move to future challenge. Okay.

Future challenges, one, Denise, Norm and Boban. This is the coalescence. Yesterday, we observed that we can't find any text. This is kind of at the edge of our remit. But maybe we can add to the study of the SSR – can add the study of SSR consequences of the coalescence to one of the other recs.

DENISE MICHEL: I think that's a good idea.

RUSS HOUSLEY: Okay. I'm going to turn to Laurin. Which rec is that best added to? You've cached them all in your head.

LAURIN WEISSINGER: Cache is not really useful right now.

RUSS HOUSLEY: Your cache is not useful?

LAURIN WEISSINGER: I could see it actually in recommendation 16, which is the SSR concerns and contracts. So we can kind of say, "Well, look at how big you are, what your risk profile is. As far as I can see, that's probably the best so far that I've looked at.

UNIDENTIFIED MALE: [inaudible].

LAURIN WEISSINGER: I don’t think there's anything better, but I'm scrolling through. Cache not that good.

DENISE MICHEL: [inaudible] not working.

LAURIN WEISSINGER: Yeah. I'm sticking to 16.

RUSS HOUSLEY: Okay. Moving on to topic two. Yesterday, we observed we can't find text but there's still several places where recommendations are made about information sharing, and then –

LAURIN WEISSINGER: [inaudible].

RUSS HOUSLEY: So three, nine and 12 have some of that.

LAURIN WEISSINGER: 12 is the one that will be merged into number three, that's why it's in brackets. Recommendation nine is on threat intelligence. ICANN needs to be more transparent about [inaudible] threat intelligence. And then essentially, as you can see, we have kind of made a note in the recommendations to make sure this is integrated into the data recommendations when these are reworked, and then second point will probably go into recommendation three. And third point should also go into recommendation three, which is the one Scott and I have to rewrite.

RUSS HOUSLEY: Right, we talked about that one earlier. So given the overlap here, I'm thinking that there aren't any concerns. Is that correct? Alright. So the crypto systems one, let me find it.

ALAIN AINA: I also have something to say on the cryptographic [inaudible].

RUSS HOUSLEY: So what we have is the recommendation – I just can't find it right this second.

ALAIN AINA: Recommendation 35?

RUSS HOUSLEY: 25.

ALAIN AINA: 25.

LAURIN WEISSINGER: [inaudible].

RUSS HOUSLEY: That's right. That's it.

ALAIN AINA: Yes, I think we should – PTI is the root KSK manager, not ICANN per se. PTI is what you call a [subsidiary] organization of ICANN, but if you look at the [DPS,] the owner of the DPS is PTI, not ICANN, so we may be more specific in saying PTI should instead of ICANN.

Then second thing I want to suggest is that – and Russ, I think we had this discussion – the DPS should be changed to accept transition to any algorithm, [not ECC right now] because we are also talking about [inaudible] So maybe we should make it [inaudible] instead of focusing on changing it [inaudible] we have provision to facilitate the migration to any [inaudible].

RUSS HOUSLEY: Yes, it is. It is not. So I tried to accommodate that. And anything else? In the findings part of the write-up, we talk about what's going on and that it's going to be five years until there's a standard in that space, so let's focus on the near term, but keep your eye on that ball. And we don't yet

know the consequences on the DNS, because we don't know the signature size yet. Some of them are humongous. As in kilobytes.

DENISE MICHEL: Is there a range?

RUSS HOUSLEY: No. We don't know the winner of the competition yet. Okay. Laurin, and Naveed. Can you talk about the new uses for DNS part, recommendation 19?

LAURIN WEISSINGER: Yes, just to kind of reach out to research community, reporting recommendation, IoT, and should be focusing on. And that's essentially it. I believe we talked about that in general.

RUSS HOUSLEY: That's a different issue.

LAURIN WEISSINGER: No, I just want to say [inaudible] in here.

RUSS HOUSLEY: That's talking about the privacy protection of encrypting the queries and responses. Right? On 19?

UNIDENTIFIED MALE: [inaudible].

RUSS HOUSLEY: Okay. [inaudible] you're not going to change algorithms all over the tree. [Or not effective.] Any concerns about recommendation 19? Okay. Moving on to the next one, it's recommendation 30, it talks about this, I think, but Norm or Laurin, you guys are the ones who worked –

LAURIN WEISSINGER: Yes, [essentially,] this is in recommendation 30, [which is one of those] we'll probably have to kind of reduce [into fewer,] but essentially, it says produce metrics of ICANN's root zone, plus a list of alternate DNS root zones that ICANN [inaudible] protection and kind of offering global resolution.

So it's essentially part of the root zone SSR metrics.

RUSS HOUSLEY: Any concerns here?

NORM RITCHIE: If we're asking for metrics, should we be specific on at least some of them, saying these are the metrics that we look for rather than saying broadly to be determined?

LAURIN WEISSINGER: So there is actually stuff in there [inaudible] snapshot management, [longitudinal] analysis of [measurement] deltas, any observed [qualitative analysis,] such as the impact of alternate root zone traffic [structure,] protocol evolution, any observation of issues related to coexistence of alternate roots with the official ICANN [global] – so we do have something. Maybe not exactly what you want, Norm.

NORM RITCHIE: Yeah, I'm just thinking if I was handed this, if I was tasked with this, I'd kind of go –

LAURIN WEISSINGER: "What do I measure?"

NORM RITCHIE: Yeah, what do you want?

LAURIN WEISSINGER: Should we just make a comment in 30, kind of say that we need to define these measurements, give examples and then think about it at a later date, or do we want to do this now?

NORM RITCHIE: We could either do it [inaudible] later date, I think, and add them in, or suggest that the community be – ask the community what they want. Metrics. That's what I mean, any type of metrics, [we just kind of say,]

"Do metrics. Measure things." But we're not being very specific about anything.

LAURIN WEISSINGER: Considering that we are likely to make one recommendation out of this 34, 33, 32, 31, 30, maybe even 25 and 24, probably asking the community to define this for this group of stuff would be the best way to do it.

RUSS HOUSLEY: Put a comment in the document somewhere so that [on that pass,] we do it. Are you happy with that, Norm? Good. Okay. Moving to future six, this is recommendation five. Norm and Laurin are in the room on this one. Well, yesterday, I believe, we said let's add something to this, and I thought it happened.

NORM RITCHIE: [inaudible].

LAURIN WEISSINGER: Isn't this like number three again?

RUSS HOUSLEY: What it said a minute ago was expand the response to SSR1 recommendation six, which our recommendation five is, to cover this.

LAURIN WEISSINGER: So I'm more thinking, wouldn't kind of threatscape assessment not fall under the kind of recommendation three stuff which is vulnerabilities, threat assessment, sharing of relevant parties, that type of stuff? So should we just turn this into recommendation three? And I'll make a note we're considering that.

RUSS HOUSLEY: Okay. Well, we've already talked about recommendation three, so that should be okay. And privacy protections is next, future seven, which I think is recommendation 36. That would be Norm and Laurin.

LAURIN WEISSINGER: Yeah. This breaks up into two elements. One is privacy as an issue per se, and then privacy legislation, which obviously has an effect on ICANN. So this is like security, this is about what people want for DNS, and obviously also financial if it comes to legislation. And it's essentially about looking at privacy technologies, monitor what's going on with legislation, have a policy regarding PII and that there should be a responsible party.

RUSS HOUSLEY: When you say responsible party, we're not talking about a c-level –

LAURIN WEISSINGER: No, ICANN CTO.

RUSS HOUSLEY: Okay. I thought it was you. So I'm not hearing any concerns on this one. So I think the next thing to talk about is how we get all of the changes that we've discussed, the things that got thrown on the bottom, how we're going to go about dividing the work to get that integrated.

So I think what I'd like to do is take a five- or ten-minute break and maybe people can have some side discussions, basically some brainstorming, come back from the break, and we'll talk about how we're going to get the findings text put together and get the recommendations correlated, racked, stacked, merged and so on. Alright, ten minutes.

Okay, we have 27 pages of recommendations. And KC still owes us a couple.

LAURIN WEISSINGER: And then there are additional ones at the bottom.

RUSS HOUSLEY: No, I'm counting that.

LAURIN WEISSINGER: Oh, yeah.

RUSS HOUSLEY: So we clearly have some work to do to organize, merge, figure this out. I'm struggling with how we can do it in parallel, given the number of overlaps. So at some point, we need to turn it over to Angie and say,

"Make it read coherent." But I think we have not put in an adequate – I don't think we're at the point where we can do that to Angie yet, is I guess what I'm trying to say.

I think we need to make one more pass here, and the question is, how do we organize it so that more than one of us is involved? I'm struggling with – do we just go make a pass now and say which ones are related using maybe Laurin's table as the start and then assign rows on Laurin's table to individuals? That's the closest I've come to a plan. I'm struggling for a better one or an improvement upon that one.

I think it's going to be hard to do that if multiple people are working on the same recommendations. I think it will be possible for example in the security risk management, business continuity part, we identified two, eight, 11, 27 and 40. So if we said those are yours and you can do whatever in the text of that, you're not going to stomp on somebody who's doing the handling of 30, 31, 32, 33, 34. That's why I'm thinking it can be a doc still and get that done. But I'm open to suggestions. We're doing something here I've never done before.

DENISE MICHEL: I guess I would recommend that we use the assignment table to indicate who holds the pen on broad topics with an eye towards those people synthesizing and combining and deleting repetition and streamlining things in particular buckets, and then use a separate, new Google doc to start putting – I know – to put that synthesized text – because here's the thing, like if you disagree with how someone has synthesized five recommendations down to one and you want to refer back, I mean, is

everyone comfortable using the history mechanism in Google docs to do that? It just may get a little messy if people are cutting and pasting and – yeah, so that's why I'm thinking of starting a new draft, and that's where people will park the updated new text.

ANGIE GRAVES: [inaudible].

DENISE MICHEL: I'm open to any ideas that people have.

NAVEED BIN RAIS: My suggestion is we put someone in the lead in each of the main topics, like in terms of for future challenges, somebody would hold the pen as a whole, not topic by topic. And then we can have like in this manner we can have teams with one penholder from each team, and between those penholders, if there's any overlap, they only coordinate between them to see whether there's something that needs to be moved to one stream or another.

LAURIN WEISSINGER: So we merged a lot of stuff though. So a lot of the initial – like the Work Streams, they refer to different recommendations because we already started folding this in. so I'm not sure if we can go down that route or if we indeed have to go by recommendation number in the document and say this is X and Y is the next one.

NAVEED BIN RAIS: There's no harm if two teams are working on the same, because I'm just saying that if two teams rather than two individuals are working on the same, it will be better to coordinate [even later.] So there's no harm of a set of people working on the same thing in parallel rather than individuals working on things in parallel, because that [inaudible].

And I don't think we can remove a lot of overlap. There would be some common areas, even despite the substreams that we created. Only in the final document we will know, okay, where to place that and where not to place that. That's what I'm trying to say.

ANGIE GRAVES: I just want to give a little bit of my feedback. I like Denise's idea of a new document. I know we're adding significantly to the count of documents, however, for just the reasons that you said, history, having a new document that is the one that Angie's fiddling with I think is a nice line, distinction, and recognition that we'll be working toward a final – or at least a draft.

Secondly, I like the subdivision and the penholder, but not distinct to a topic or a group of topics. If I have questions, I can put some comments in the text of the document. However, if I need to reach out to somebody, it really would be helpful to have the name of a penholder. I'm happy to write to the whole list, but just for efficiency's sake.

So that's my only feedback. And I'm very flexible with how we go with this. Thanks.

JENNIFER BRYCE: So just on what Angie was saying, however you all want to communicate, whether it's on list or individually, but – and by the way, Angie, you're added to the SSR2 list, so you can contribute and receive the e-mails. If you are reaching out to the review team members individually at any point, please copy staff so that we can keep track of – you don't have to copy the whole list, but keep staff copied if you could. Thanks.

NAVEED BIN RAIS: And also, it's better to have for example even if we create new document, I don't mind creating at all, but it should have a pointer to the old document. So the start of the each document should say, okay, these are the older versions of the same, for example the questions and answers, we keep tracking them, searching for them, so in the start of each document, we can place a table, "Okay, these can be found" or relevant documents or this, this, this. And once you open one, you can actually trace back all of them, like kind of an idea for [inaudible].

DENISE MICHEL: That would be so helpful. That's a great suggestion. Also, just as an aside, I wanted to note that there are several points in this draft document that track either whole or in part to recommendations that are contained in the CCT review relevant to those, and some that will be relevant to the RDS WHOIS II review.

So we'll want to make sure we call those out in addition to the connections to the proposed strategic plan and other things. So I'm just telling you that as a placeholder, and when schedule permits, I'll go back and highlight those items, and I may add a few more notes into this document.

NORM RITCHIE: I think it's a good idea. Just further on that, I wonder if we should sit down and talk with the CCT team or ex-team and just let them know what our recommendations are. And they could tell us, they could give us pointers, right? I think they probably have a lot of the discussions that we had. I don't know who's going to be there from that team. I know Drew was not there.

DENISE MICHEL: [inaudible].

NORM RITCHIE: Yeah, [it's true.]

ANGIE GRAVES: Norm, at what point do you think is appropriate to do that?

NORM RITCHIE: Next iteration.

ANGIE GRAVES: Okay. Yeah.

NORM RITCHIE: Just a crazy thought, do we have to submit this as a paper doc, like as a document, or could we actually use a Wiki hyperlink type thing? The final report when it's done, is it supposed to be a document?

DENISE MICHEL: Yeah.

NORM RITCHIE: Okay.

DENISE MICHEL: I think if you want to put it on a Wiki, we could do that too as a Wiki doc.

NORM RITCHIE: [inaudible].

DENISE MICHEL: Sure.

NORM RITCHIE: [inaudible].

DENISE MICHEL: Sure. I think it's a good idea.

RUSS HOUSLEY: So would it be a good use of the time to spend this afternoon dividing this and working now so that tomorrow, we have that document? Maybe we can even get KC's inputs overnight. I know she said this weekend. I don't know what that means.

If that makes sense, I think we have three – you're leaving in an hour, is that right?

DENISE MICHEL: No, like half an hour, 20 minutes.

LAURIN WEISSINGER: And I'm leaving this evening.

RUSS HOUSLEY: This evening means after 5:00?

LAURIN WEISSINGER: Yeah.

RUSS HOUSLEY: Okay. So if we divided this up into like six chunks, we could each take one and maybe get somewhere. What do people think about that?

DENISE MICHEL: I think that's fine, but also just because I'm physically not here doesn't mean I can't work. I'll be flying, so I can [inaudible].

RUSS HOUSLEY: I assumed you were going to be somewhere not connected. Is that not right?

DENISE MICHEL: Yeah. That's true. Google doc might be hard depending on the airplane. Also, of course we need to put pen to paper to add findings to all these recommendations.

RUSS HOUSLEY: We do.

DENISE MICHEL: [We may] want to have people go back and do findings now and then –

RUSS HOUSLEY: What we promised was to report out into Marrakech what the recommendations are. The findings, of course, has to be done for the whole thing to make sense.

DENISE MICHEL: [inaudible]?

RUSS HOUSLEY: Yeah, that's what I have in my head. I just verbalized.

ANGIE GRAVES: With respect to the organization of the document, the reports can be – I would like to just have a general understanding of groupings. I understand the dependencies and interconnectedness. Those can definitely be represented a number of different ways. Not only via organization and the document. If that's something that can be considered today, that would be great. And with respect to findings, I have seen reports written for MSSI ICANN that were all the findings, and then all the recommendations. I have also seen finding one, recommendation one, two and three, finding two, recommendation four, bla bla.

So if you could consider just those two points for organization, I think that would be helpful in me thinking about the outline. Thank you.

DENISE MICHEL: Yeah. And personally, I'd like to be driven by brevity, trying to keep it as succinct as possible, put as much in an annex as possible. People don't tend to read long reports, so we'd want to put our recommendations in buckets at the very front, and if we can do findings, one finding that supports four or five recommendations would be great, I think.

ANGIE GRAVES: Do consider that there won't be an introduction and/or executive summary that will be very brief. And then I like what you said, Denise, about putting as much in annexes as possible.

NAVEED BIN RAIS: Yeah, we have a lot of sample recommendations available for ICANN for example CCT RT recently. There has to be an introduction and executive summary, and topic by topic, what I generally found is you have a set of – not in terms of with the heading Finding One or something, but you cover a topic, based on that, you present your recommendations in those paragraphs, like four, five paragraphs that precedes each recommendation or a set of recommendations, for example if we have group of recommendations with respect to DNS SSR, for example abuse or something, it can precede by two, three paragraphs explaining things like how we come to those findings, because that always helps us understand why the recommendation is being done rather than – because recommendation itself is going to be one sentence, two sentence itself. So it has to be preceded by an explanation of why that recommendation was actually made.

ANGIE GRAVES: So in my experience, the finding is the context. The finding is what you're talking about which precedes the recommendation. If we add another section prior to finding, that might not allow us to be as succinct as we want.

And then with respect to the recommendation being a sentence or two, one of the ways I've seen it done is a short one line, maybe two

recommendation, but then an explanation of that that's a couple or a few paragraphs.

And same with the finding. The finding could also be summarized in a line or two, literally a line on a page, and then with additional explanation, which may end up partly or wholly going into the appendix, but finding and recommendation is what I'm accustomed to seeing.

And Jennifer's done a lot of these, so she might have input that [inaudible].

NAVEED BIN RAIS: Generally, a recommendation is the last thing of a segment or a finding, as you're putting it. So there should be no explanation after we present the recommendation in a section. Like all the explanation related to that recommendation should come first like that helps the user knowing and understanding why that recommendation is made. Once the recommendation is presented in that paragraph, then there is full stop, then we move to the next paragraph and next section. So this is how I see it being put.

And Russ, I was just thinking, I'm not sure how many of us will be there tomorrow, so why don't we discuss things that are relevant to more people this afternoon? And then we can use tomorrow's time to divide the work further. Like how do we see ourselves in Marrakech and post-Marrakech, and what are the things to do? Maybe with more people here, we can take [inaudible].

LAURIN WEISSINGER: Or until Marrakech.

NAVEED BIN RAIS: Yeah, until Marrakech and beyond is what I said.

RUSS HOUSLEY: Okay. What I have learned is we have something significant to discuss in trying to divide this up. I realize our pass through the topics and calling out recommendations, we called out 27 of the 40. So maybe there's some that need to be trimmed, or we need to explain why we're keeping them. So that, I think, falls in your category.

DENISE MICHEL: I would suggest that the penholders edit and synthesize down, and create buckets or combinations of recommendation, and then after we do that, we go through and have a discussion about prioritization and whether a majority of the review team feels that it's an important enough recommendation to meet our thresholds or make those types of choices. But I think it's a little – especially in the abuse and compliance area, it's still a little bit too messy to make those choices.

RUSS HOUSLEY: Okay, so I think we have to figure out why the ones that we have recommendation text for but we didn't call out and therefore we don't know if we even have consensus for is part of that, because I don't know how to assign them to topic teams if we don't know which topic team the recommendation fits with.

So interestingly, the first recommendation that we don't know where it belongs is recommendation one.

NORM RITCHIE: So I have [inaudible].

RUSS HOUSLEY: That'd be interesting to see if your approach matches my approach. Okay. So one –

NORM RITCHIE: [inaudible].

RUSS HOUSLEY: We'll find out. So we both agree we don't know about one, so that has to do with public comment and transparency. What topic group does that belong to? Is it still relevant? And do we have consensus? Those are my three questions.

NORM RITCHIE: It's kind of a category that is lessons learned.

RUSS HOUSLEY: Right. This particular one, actually, I wrote. [Now I want to] read it. And what it really has to do with is how do we – we're making a suggestion to make things easier on SSR3 and every other review team that comes after in order to find – to do the step [where, "Were the

recommendations of the previous guy done?" And they can do their asses part.]

So I'm thinking this should become a suggestion. It is a recommendation, but at the same time, it's not in SSR.

DENISE MICHEL: I think we should have a small section about how this review was conducted. The things we found that worked well, the things that we would suggest be changed. I think I would suggest that we delete recommendation one from the recommendations and we incorporate that as an operational, administrative item in our suggestions of how to improve doing this review.

RUSS HOUSLEY: I agree.

DENISE MICHEL: We should have a discussion about doing this review better before we –

NORM RITCHIE: [inaudible].

RUSS HOUSLEY: Yes. Start with that. Okay, the next one we need to look at is four. This one is flat out just SSR1 follow-up.

DENISE MICHEL: Yeah, but I think it's a really important one.

RUSS HOUSLEY: I agree.

DENISE MICHEL: Because, yeah, I think it kind of goes to the heart of tracking and accountability and decision making and transparency in the SSR space. Not having an SSR budget with line items that are aggregated at least to the point that you can understand broadly how the budget and staffing is evolving is really doing a disservice to this space.

I think we'll find other things that we could put in a bucket of SSR operations and something like that.

RUSS HOUSLEY: So I think we all agree that this is an important one to say something about, given it was an SSR1 recommendation that was not fully implemented. The question is, do we have consensus on what's here?

NORM RITCHIE: I agree that it should be highlighted in the budget. [If we're going to] elevate the posture of SSR and security, then it needs to be reflected in the budget.

RUSS HOUSLEY: Okay, so I'm hearing consensus to keep this. Good.

DENISE MICHEL: But on recommendation five, I guess I would like to understand – so we have an into to SSR1 assessment, and that would broadly note what was implemented and what was not, and impacts that we found.

And I think an SSR1 recommendation has to rise to a fairly high level, like we need SSR budget line items to be included as a separate recommendation. And if people feel that clarifying the roles of SSAC and RSSAC rise to that level of importance, I'd like to hear a little bit more about that and understand what they envision success to be.

RUSS HOUSLEY: What I think success would be in this space would be a consensus document that explains the roles of the two organizations, which is what is in the document that they created, but they never went to public comment with it.

DENISE MICHEL: And so if you find that broadly so be an acceptable document, it seems to me that this is more of an administrative action where you could in a summary of SSR1 implementation note the following number of recommendations were not fully implemented and we recommend the board direct staff to bring those to closure. It could be as simple as that. This one for me doesn't seem to rise to the level of – unless you think something is fundamentally wrong or missing with the draft, articulation of the roles of SSAC and RSSAC.

RUSS HOUSLEY: Actually, that isn't the issue that I have with it. It's that they say it was fully implemented and it clearly wasn't.

DENISE MICHEL: Yeah. We have several of those.

RUSS HOUSLEY: So what I would like to do is clump those together and say we were told these were fully implemented, we found otherwise. We just want you to finish the job, A, B, C, D, E.

DENISE MICHEL: I completely agree with that. So I would take recommendation five off our recommendation list, and note that we're going to park that with our summary findings of SSR1.

NAVEED BIN RAIS: So actually, it depends on how do we see, because this is SSR2, and we are in a specific scenario, because the first is done and we don't have an SSR0 before that to see how SSR1 recommendation actually were made based on those.

So we are the ones who are setting up this, like how a follow-up review was made, actually. So here, we need to make a decision of how do we see if some recommendation from SSR1 was not implemented, then we'll have to make a decision whether it signifies something or not.

If it is not implemented, it has to be a recommendation, or not. So from a personal perspective, I think if there was a recommendation in SSR1 and it was not implemented, we have to put it under the category of SSR1 assessment and recommend it as it is under the recommendation.

So the section SSR1 assessment should contain a couple of recommendations that are based on what we think whether the assessments were implemented or not. So this is what we as a team need to make a decision, and then we can –

RUSS HOUSLEY: I disagree with you. I think that we can state all of our findings, but that the recommendation at the bottom can be just finish what you set out to do, and it includes bla bla. [inaudible] be lots of finding, and lots of, "Yes, we determined this is still relevant and that's why we're asking you to finish it," but I don't think we need to have a recommendation per place we found that they felt short.

NAVEED BIN RAIS: It also depends on if it is still relevant and significant, for example if it is still relevant and significant and it was made as a recommendation and was not implemented as such, in my opinion, it has to be a recommendation again.

We can place it under another category.

RUSS HOUSLEY: No, I disagree. I think there's a judgment call to be made, like the budgetary transparency is a big deal, we want to make it a recommendation all of its own again, and this one for example – which I did the investigation of – is, "Okay, they didn't do it, but let's just clump that with the other things they didn't finish." Even though the findings will have all of the information about what was done and what wasn't done, it doesn't have to be – and therefore repeat the recommendation.

DENISE MICHEL: In my mind, I go back to the board unanimously accepted all of the SSR1 recommendations, they directed staff to implement every one of them, and then the implementation report indicates that all of them were implemented when team members found that several of them were not fully implemented.

So I think I agree with Russ that in a summary way, we can take care of the ones that we've pointed out and have not been fully implemented and recommend that they come to closure on those. But I also think that for those that we think are highly relevant and a high priority, we draw those out into a recommendation and note that this is really important and a priority for us, like the SSR budget.

NAVEED BIN RAIS: So, is it like just our understanding on different – that can vary from person to person? Is it something like – as I'm saying, this is the second only, so we are setting the tone and the convention that is to be followed. So for example the first of the objectives – and one of the

major objectives – of SSR is to conduct an assessment of the previous SSR.

So that can always follow with a couple of recommendations, like why can't we have recommendations based on SSR1, which is one third of what we have to do. This is one of the three streams we're targeting. So, are we just eliminating that possibility that based on the assessment of the SSR1, we cannot or we will not recommend anything, or are we just saying that we can recommend if it is too relevant even today and so on and so forth?

So what I'm getting the feeling is that we are saying, no, we will do the assessment, but we are not going to put any recommendation under the category of SSR1 assessment, which is one third of the –

RUSS HOUSLEY: No, no one said that.

NAVEED BIN RAIS: Okay.

RUSS HOUSLEY: What we said is clump the ones where a good plan was started but not finished together and say finish it, which includes, A, this – go to public comment on this report, B, whatever other ones we find. But the budgetary transparency one is a big enough deal we want it to stand alone to highlight, because we think it was a big thing that wasn't done.

So that's the judgment. Is it just in the list, or is it a big thing we want to highlight?

DENISE MICHEL: I have to run to the airport. Thank you, everyone. Feel free to volunteer me for things.

LAURIN WEISSINGER: [inaudible].

DENISE MICHEL: Use some restraint though.

ALAIN AINA: So Russ, on the topics on SSR1 and not complete that –

DENISE MICHEL: [inaudible].

ALAIN AINA: So Russ, I was saying that [inaudible] discuss on the SSR1 recommendation which we found were not fully implemented, okay, I think we should do something, as you said, about it. But I also was thinking that, [we check with staff and then we've got staff feedback on a judgment on them?]

RUSS HOUSLEY: I don't think we should do that. It says we are to do an assessment of whether the implementation achieved the objective, not ask staff if the implementation achieved the objective.

ALAIN AINA: Yeah, I'm not saying that we should ask them. We are the ones making additions, but just to make sure that this is what we are using as information or data to back our decision and make sure that we are in agreement with staff, because staff said this is fully implemented, and then give us something [– we are] based on some analysis saying that [we are not,] so we look like we have one, staff saying something, and we're saying something else, maybe looking at the data or information we have. Are we using the same metrics, or we have different metrics compared to staff?

RUSS HOUSLEY: I don't think that that can possibly apply to this recommendation, because the report says fully implemented, here's the URL to the document, you go to the document, it says top and bottom of every page – or the title page, I don't remember – that says, not yet reviewed or something, and you go to the history of all the public comments, it's not in there.

So I don't think there's any wiggle room to talk about.

LAURIN WEISSINGER: Danko has his hand up.

RUSS HOUSLEY: Oh. Sorry. Go ahead.

DANKO JEVTOVIC: Yes. So I am, as you know, new to this process, so maybe my comment will be just a bit off the course in a personal, but my view is that Russ is absolutely correct, it is the role of the team to assess about the implementation of the SSR1 recommendations, and I would like to comment on a few small topics I overheard during the conversation.

So for example, if there is something really important, like your point about budget, I would expect that to be specifically laid out, a specific number of recommendations from your team, because that way, it will be like itemized differently and with full amount of attention from your team.

Then as I read through your draft of the SSR1 evaluation of the implementation, a lot of stuff hasn't been fully completed, but maybe it will be challenging if you just write, "Okay, just finish the stuff you were doing." It will be maybe easier if this is also itemized in a way we recommended it should be completed in this and this way.

So I'm saying that because I've noted [while] discussion a few smaller [inaudible] like for example there was a recommendation regarding the role of the RSSAC and SSAC, and basically, it's formally defined in the bylaws which have been amended for the IANA and everything process, and also, there is – what was the name of the document? Charters for the RSSAC and SSAC where it's defined.

So of course, there was some document that you mentioned that is not fully defined and published, but it seems like a rather small item, and it's basically back to the advisory committees, and the role of the committees in formal sense is fully defined in the bylaws.

Also, on the budget, if you want connected things, the budget, I would agree from the security point of view that it's very important that financial aspect of the SSR is shown clearly, and from my personal point of view while sitting on the Finance Committee, this is one of the points [inaudible] very much like to see the budget, because I believe that we are not seeing that figure clearly. The importance of this topic is not fully presented in the way how the money is distributed, but basically, the budget currently is billed from the bottom up by the projects.

So that would be required either to fully change the way how the budget is prepared, or maybe just the recommendation could be more general. I think it would be maybe more realistic to be implemented in the budget. There is a special section that will somehow bring up the financial stuff that is going into SSR so it is visible.

So the point is, from my understanding, about visibility of the finance, not about recommendation how the budget should be built up. But basically, I've just chipped in to support Russ' point of the need of your team to [relate what has been] done, and that's a good way to go. Thanks.

ALAIN AINA: I think Danko just said differently what I was trying to say, that if we are going to say "Go finish this, we have to look at exactly," because for

example we noticed that some of these things started, as he said, started, but were not completed, but were achieved differently, etc. through something else.

Okay, so that's why I'm saying that we have to find out exactly what really happened and how that should be completed. Yeah. Because for example for the budget, we were told that they no longer produce the budget for SSR directly but now SSR budget is included in the general budgeting following the strategic objective, etc.

So if we're going to say "You didn't complete this," we have to be specific, because they said, "No, we said we no longer run a budget for SSR specific, but you'll find SSR in the general [inaudible] objective. So that's why I'm saying we really need to know what we want them to complete or finish and how.

DANKO JEVTOVIC: One more small additional point. Sorry to drop in again. So first, yes, exactly, it has to be in a way actionable. But another thing I learned during the CCT review is that actually, some – [while] recommendations from the specific review teams are going to the Organizational Effectiveness Committee of the board, but then it goes to the full board, as some of the recommendations are actually for board not possible to do anything about it [indirectly,] because the board can direct [order] to do something, or board can initiate some policy development or something. But for the CCT, some of the recommendations were actually directed to the SOs or ACs, for example to GNSO, and the only thing that board could do with them was actually to direct them to GNSO and bring them to GNSO attention without saying to GNSO what

has to be done, because we have this bottom-up process and the board is not making policies.

So of course, you know about the process, and you've been briefed about all that, but for me, it was a big takeaway. So it's not coming back to any of your discussion directly. I didn't observe anything that could be impacted directly by this observation. But I think it is good to have it in the back of your mind when you write stuff down. Thanks.

RUSS HOUSLEY: Danko, we've been paying a lot of attention to that, and I don't think anyone was surprised by the recommendations that were not actually implementable by the board being forwarded to the appropriate part of the community. That wasn't the part of the response to the CCT team that upset the other review teams.

DANKO JEVTOVIC: Okay. Yes. Sorry that I'm repeating that again, because I'm sure you do, and of course, we spoke also in Kobe about the other part and trying to avoid any challenging [words] to describe this situation that we created, but anyway, things are getting better now, at least I hope. Thanks.

NAVEED BIN RAIS: Why don't we use another category, which is called observation number one, observation number two, observation number three along with this recommendation one, two, three? So that way, we can put what we found as an assessment. Just to put that, and to highlight, because otherwise, the assessment can be hidden in the text otherwise.

RUSS HOUSLEY: I think what we're seeing is we're going to make a recommendation, if it's not like the budget one that it needs a spotlight, that there will be subpoints, but it'd still be a recommendation. I think that is where we ended up.

LAURIN WEISSINGER: One recommendation –

RUSS HOUSLEY: One recommendation says finish the following things that you've already started. Because the observation is you didn't finish. The recommendation is "Finish please." Unless we found that it wasn't still relevant five years hence.

Okay, the next one we need to talk about is six. So my feeling is this, like five, becomes a bullet in "finish what you started." Do others feel that this needs a spotlight or that it should be merged in with the big section we have regarding compliance?

LAURIN WEISSINGER: In addition to that option, we could also integrate this into the ISMS, because this is essentially – it would work with that, and we would just note, oh, by the way, this was also SSR1 recommendation to kind of avoid duplication. Because this kind of stuff is necessary for doing the things we request in that – I'll just call it a topic area.

So two could become like a big one. It's on certification, ISMS, mentioning kind of the relevant things that need to happen for that to work, and so we could essentially say, have this strategy and framework, and one of them would be implementing that. And I'm not sure if we want to do that. Scott, I can see your head is kind of – you're unsure. I'm just saying it might be a possibility we would want to agree what to do. Scott is stretching, for the record.

NORM RITCHIE: Do you know off hand what recommendations 12 through –

LAURIN WEISSINGER: So to answer your question, recommendation 12 –

RUSS HOUSLEY: 12 is best practices.

LAURIN WEISSINGER: Should work with the community to identify SSR-related best practices, support implementation of such practice for contract agreement and MOUs and other mechanisms. So I definitely want to address, and then 16, still scrolling. 16 was ICANN should continue its outreach efforts and fund community participation, and input into the SSR framework development process should also establish process for obtaining more systemic input from other [ecosystem participants.]

RUSS HOUSLEY: Okay, so anyone have a problem with merging that with two?

LAURIN WEISSINGER: This is all related.

RUSS HOUSLEY: I understand.

LAURIN WEISSINGER: So I'm not sure if it'll be two. So we might want to say –

RUSS HOUSLEY: No, into what is now [recommendation two.]

LAURIN WEISSINGER: Yeah, include –

RUSS HOUSLEY: However that gets structured to make sense.

LAURIN WEISSINGER: [inaudible] it referred to what was then next round, but the next next round is coming.

RUSS HOUSLEY: So the question is, does this one need a spotlight, or should it be merged with someone else? Or should it be a bullet in the "just finish it" list?

NORM RITCHIE: This is an odd one because it's conditional on whether they adopt the other recommendations that we're talking about as far as setting up [like an anti-abuse center of excellence,] etc.

UNIDENTIFIED MALE: [inaudible].

NORM RITCHIE: No, but you're saying it now applies to the next round of new gTLDs.

LAURIN WEISSINGER: So the SSR1 thing was recommendation 22. Give me a second.

RUSS HOUSLEY: It's right there, "Plan a properly funded –"

LAURIN WEISSINGER: No, this is the strategic plan. Recommendation 22 SSR1 is ICANN should publish [inaudible] documentation on the organization and budget resources needed to manage SSR issues in conjunction with the introduction of new gTLDs. So this was the old one, and then in the

recommendation, I quoted strategic goal 3.4, which is to plan a properly funded management risk evaluated new round of gTLDs.

NORM RITCHIE: [inaudible] SSR around the new gTLD program, so what's the additional budgetary hit for? My point is though is that we're –

RUSS HOUSLEY: I think it goes with five. It's a list of stuff you didn't –

LAURIN WEISSINGER: So the question would be, would we want to highlight this considering the next line of gTLD coming –

RUSS HOUSLEY: But we have so much other stuff. That was my –

LAURIN WEISSINGER: I was raising that possibility.

RUSS HOUSLEY: I'm just [inaudible] spotlight you want to put on it.

NAVEED BIN RAIS: When we say that this is not fully implemented and we had discussion on many of these earlier, did that mean that it was started but not

finished, or some of them were not even started? So I'm just making sure that we are not using the same word “not fully implemented” for all of them regardless of whether and how much they were started or partially implemented. Just don’t want to mix all of these, because when I see in the SSR1 recommendation document that we made, I see that this one was not even started properly. So saying that it was not fully implemented means that it was partially done, but I don’t see an evidence regarding that. So in that case, we cannot even say that it was not fully implemented.

RUSS HOUSLEY: So you're recommending that this one stand on its own?

NAVEED BIN RAIS: Yeah.

RUSS HOUSLEY: Okay. Anyone have a problem with that?

NAVEED BIN RAIS: And I'm also proposing to remove the “fully implemented.” That creates confusion.

RUSS HOUSLEY: So just –

LAURIN WEISSINGER: Implemented.

RUSS HOUSLEY: Delete the word “fully?” The next one is 12.

LAURIN WEISSINGER: The next one would be enforcement against abuse [harboring] parties. We did touch on it. We did not discuss the specific recommendation. We are talking recommendation 17.

RUSS HOUSLEY: So this is part of the CENTR thing?

NORM RITCHIE: No. [inaudible].

LAURIN WEISSINGER: My first question is, are we happy at least roughly with the text?

NORM RITCHIE: Yes, but given our bigger discussions now regarding compliance and the abuse, this has gone deeper. We have much more detail.

LAURIN WEISSINGER: Okay.

RUSS HOUSLEY: [Where's that?]

LAURIN WEISSINGER: There's just a section we call compliance because it doesn't have numbers yet, Russ.

NAVEED BIN RAIS: I'm not comfortable with using the word "no sufficiently functional process exists," because it's like a kind of mix, because we're not sure how much sufficient it will be. Like we can just say no functional process exists, because it is kind of a black and white – when we say sufficient, not sufficient, everybody would interpret it in a different way.

RUSS HOUSLEY: No, we discussed this yesterday.

NORM RITCHIE: [inaudible].

NAVEED BIN RAIS: So we just say no process?

LAURIN WEISSINGER: No process exist. Okay. Changed.

RUSS HOUSLEY: Anything else for 17? Okay, we'll look at 18.

LAURIN WEISSINGER: I'm not sure where this one came from. It's essentially financial accountability, and changing the structure. So I've remembered the context of this, even though it's not coming from me, so the discussion was essentially on making ICANN financially, fiscally responsible towards registrants.

NORM RITCHIE: [To the people.]

LAURIN WEISSINGER: Yes, the people. And that would require changing the way ICANN is paid.

NAVEED BIN RAIS: I'm just trying to make a connection of this with SSR in that perspective, like how is it related to security, stability or resilience, this financial structure towards registrants? Is it a direct relationship between the two? If not, then it can't be a recommendation in itself. [inaudible].

LAURIN WEISSINGER: Yeah. I think the argument would be that it has to do with things like accountability and with strategy setting. So it depends whom you're responsible for and who's paying your bills. These are the kind of

principles you work for. If you change who your principles are, you change strategy and kind of also financial – like financial responsibilities.

NAVEED BIN RAIS: Yeah, that's okay, but accountability is not under SSR, as I see. Like it can be a separate thing. I'm just saying if it is not directly relevant, it should not be a recommendation. It can be part of some other stream or in the findings or whatever, but putting it as an observation can be directly neglected or rejected by ICANN later saying that you don't have mandate to comment on this because it's not related to SSR.

So I don't know what others think about that.

LAURIN WEISSINGER: So I think this is one where we might want to figure out where this came from and what the context was. When I edited the document on Thursday, I also thought, okay, I might see where this is coming from, but we need to make sure we discuss it with the persons that wrote it.

ANGIE GRAVES: You're using the word "observation" quite a bit, and your definition of observation earlier, I just want to note, was about what was found, which made it sound a little bit like findings. So if there's any vagary there between findings and observations –

LAURIN WEISSINGER: [inaudible].

ANGIE GRAVES: Okay. Thank you.

LAURIN WEISSINGER: Yes, this is exactly what I'm kind of writing as well in the to-do list, so we have to make sure we understand this before we actually discuss it.

NAVEED BIN RAIS: And especially when you're asking too much, like changing the financial structure is not a one-day task. It can't be done like that, so you're asking too much with that one sentence. It should not be there like that.

LAURIN WEISSINGER: Yeah, so essentially, as I've mentioned before, when I did kind of adjustments at first, I made sure I didn't delete anything. That is why a lot of stuff is still in there so that we can make a decision as a team.

UNIDENTIFIED MALE: [inaudible].

LAURIN WEISSINGER: We can. It’s already in the to-do list of the table. But I will.

RUSS HOUSLEY: Okay, so 21, 22, 23 were all merged into 20 already, so those are not ones we need to talk about.

LAURIN WEISSINGER: [They're not even on the list.]

RUSS HOUSLEY: No. But there are numbers that have disappeared. So 26 is the next one we need to talk about. This is an Eric around the tabletop. I remember this from L.A.

NORM RITCHIE: I don't know if you followed the IETF discussions on this, Russ.

RUSS HOUSLEY: Oh, yes.

NORM RITCHIE: Okay. I just saw parts of it, and I understand [they might have actually just changed] the entire process. So, is this still applicable?

RUSS HOUSLEY: It is still applicable because the IETF is certainly not going to change it quickly. And you know there was a [inaudible] at the last meeting that was actually run by ICANN's folks to – Paul Hoffman to talk about what are the lessons learned from the last rollover.

So I think this should have been tagged against one of the DNS SSR topics, and we missed it.

NAVEED BIN RAIS: I'm just wondering, asking for it to create a separate stakeholder group might be advisable for this kind of activity, what this recommendation says in the second last sentence? It's like ICANN must create a stakeholder group of relevant personnel. So maybe stakeholder group, this is not what stakeholder group at ICANN community that we understand. In that case, we should use some other word, because stakeholder group comes from the community itself. So how can we create it based on some relevant personnel? It should not be called a stakeholder group in that case, because SGs have a specific meaning under ICANN.

RUSS HOUSLEY: So I've added six as part of the root zone change management topic, because the key that we're talking about losing the root zone, now we have to find out whether we have consensus on what's here, [inaudible] people stop changing it, I can ask that question.

Okay, is everyone happy with it? You're happy enough with the topics [inaudible]? Okay, I'm not hearing any objections. Next one's 37.

LAURIN WEISSINGER: Russ, this is struck because this is vulnerability disclosure. This will go into three.

NORM RITCHIE: [inaudible].

LAURIN WEISSINGER: [inaudible] will go in there.

RUSS HOUSLEY: That's it. We've completed that exercise.

LAURIN WEISSINGER: No, 39.

RUSS HOUSLEY: 29 we did.

LAURIN WEISSINGER: 39.

RUSS HOUSLEY: Somebody [inaudible] was talked about at some point.

LAURIN WEISSINGER: No, this is something else. New gTLD application procedures should include safeguards to ensure that [technical and security] aspects of the – what are we doing with this?

NORM RITCHIE: [inaudible]

RUSS HOUSLEY: If you look at ICANN SSR six, we talked about recommendation 39.

LAURIN WEISSINGER: Do we keep it as one recommendation now?

RUSS HOUSLEY: Yes.

LAURIN WEISSINGER: On its own?

RUSS HOUSLEY: Yes.

LAURIN WEISSINGER: Okay.

RUSS HOUSLEY: This was the last one. Easy.

LAURIN WEISSINGER: Perfect.

RUSS HOUSLEY: Okay. Any concerns? We talked about this one already. So somehow, [I'd just want to put it into the spreadsheet, right?] Alright, so let's take a 15-minute break, snacks are available. Reconvene.

NORM RITCHIE: For people who didn't participate yesterday or weren't here yesterday, you might want to read the other recommendations.

RUSS HOUSLEY: [inaudible] a significant change in direction from yesterday, so yes. Alright, let's take the break, we'll be back in.

Okay, so it was observed during the break that after all that discussion about things that were started but not completed, that we only had one in that category, so it's going to end up as a standalone recommendation anyway. Thought that should be included in the recording somehow.

Anyway, and KC has just joined us. So she has just confirmed that ones where we are waiting on text, we will have that text from here in the morning. She'll finish it today so that we can determine whether we have consensus on those as well, and we'll have a way forward by the time we head home. Awesome.

KC CLAFFY: [inaudible]? Put it in the chat room.

RUSS HOUSLEY: It depends whether you're writing finding text or recommendation text. There's two different places.

KC CLAFFY: Finding.

RUSS HOUSLEY: Okay. So finding, we are hoping to have the recommendations that go with those findings, and I realize the thought processes, you need to do the findings first, but we're doing the recommendations in terms of consensus first.

So there's a Google doc per Work Stream, so Jennifer, if you would just send KC an e-mail with those Google docs, one for the recommendations and then for the findings, one per Work Stream. So you'll get that in a minute.

KC CLAFFY: Can I make a comment?

RUSS HOUSLEY: Please go ahead.

KC CLAFFY: Just a couple of days ago, the SSAC published its – I don't know if this is already talked about, let me know. I don't want to waste time – what they're calling a feasibility assessment and implementation plan for the

SSAC review. So that happened over the course of last year, and then SSAC had a whole working group trying to process the recommendations and figure out what could be done, what couldn't be done, what do they agree with. So that report just came out a couple days ago. [inaudible] myself.

And I was part of the work party, so I stand behind everything in the report, in that feasibility assessment. But I think it behooves somebody on this team to read it. And I can send my markup of it to see a lot of these things, a lot of these recommendations and SSAC's decision on how to deal with them have SSR implications, obviously.

And my reaction reading it without my SSAC hat on or trying to put myself in an SSR2 frame of mind was, jeez, a lot of these things that the review team wanted from SSAC, SSAC can't do because it's just not feasible with the current structure of SSAC, volunteer and everything else.

And I'm wondering if it's something that SSR2 wants to comment on. I've got my thoughts, but I don't consider myself objective so I'd like someone else to volunteer to look at it with fresh eyes. And then I can talk to them about it and answer any questions.

RUSS HOUSLEY: Sure. So you're going to send that to the list, or where?

KC CLAFFY: Yeah. [I'll send it to the] Zoom room, and then I can go to the list.

RUSS HOUSLEY: Okay.

NAVEED BIN RAIS: My question is, do we need to consider whether a constituency, SO/AC is in a position to implement that or not while making the recommendation? Or we just need to recommend what is necessary to do, notwithstanding whether ICANN has resources or structure to do that?

And I see a lot of the recommendations that we're making where we are asking for having new structure, having new position, so that's also not there, but we are recommending that.

So, should we keep that in mind while making a recommendation? That's the question to the team.

RUSS HOUSLEY: I think that we considered a bunch of things, and the ones that filtered to the top are the ones we want to – but I do think we need to, as we'd go through the drafting process, if we find we've overstepped, we can pull back a little. But there's certainly – some of these recommendations are certainly going to cost money. There's no doubt about that.

Okay, so what we said we were going to do next was look at that block of recommendations that emerged yesterday that were quite the anti-

abuse center, and Norm, you want to lead us through that? Thank you. I think that's 38, right? Yeah.

NORM RITCHIE: Okay. For the people that weren't able to make it yesterday, a synopsis of our call with Compliance and where we've gone since then, the conversation with the Compliance team, a number of things came out that were kind of clear.

One is that they really don't have any way of dealing with systemic abuse by the registrar or registry, because they work on a case-by-case basis, so complaint by complaint, and they have to follow exactly what's in the contracts. So the contracts don't allow that to be addressed currently. So that's one issue.

Another issue was they don't really have the data they need.

RUSS HOUSLEY: Kerry Ann can't hear you.

NORM RITCHIE: Sorry. Okay. So that was point one, is that they have to deal on a complaint by complaint basis, and even if they know that there is systemic abuse, they have no way of really addressing that or taking any action.

The other thing is that they also don't really have a good source of abuse data. They have DAAR right now, and they do look at that, and

that informs them as far as doing an audit, but other than doing an audit, they couldn't actually take action any other way.

So that's not a good situation, because you basically have no one that's really looking after abuse, and couple that with the changes to WHOIS, which has curtailed a lot of the research and analysis that's done by parties outside of ICANN.

So I came up with this idea that we form a – for lack of a better word – center of excellence within ICANN that is staffed with technical experts in the analysis of domain name abuse. They could also have access to the WHOIS data, so that would be part of it, the full set, which then allows them to determine who [else may be the] gateway. And we'd have to change the contracts as well to allow action to be taken against abusive players.

So [this would basically make the] center of excellence for domain abuse mitigation very proactive within ICANN itself. I really like this idea a lot. And it comes out with a whole big set of recommendations on how it could be structures. Those recommendations are in the document, but I left my laptop over there.

See if I can remember them. In no particular order, the recommendations are to do the – okay, thank you. Yeah, so [inaudible] modify the contracts and give Compliance the ability to analyze systemic abuse and address it .

That would also require the tools to do that, as we talked about. The DAAR product could be enhanced as well to basically be that tool to do the analysis. So it's a good start. However, it needs some more work, it

needs some more data. It needs data that could be shared, so the data that's supplied needs to be actionable, not kept private.

The other thing is the staffing of that group would be staffed with subject matter experts. The people that do domain name abuse are few and far between in the world, and right now, they are scattered throughout everywhere, but this would make a center of excellent, so you'd actually have a core group that would be able to tackle the abuse.

And along with that, you'd obviously have reports that [it would be putting out.] Those reports would be made public on what's being done. The systemic abuse cases would be – they typically would fall on a few parties. There's actually not that many typically, and it's not the ones that show up in the ICANN meetings. That's not typically where the problem is.

So they really [need a] way of dealing with that, because that really drags down the entire industry. And that problem has been around for a long time.

As far as funding of this, there is a great deal of money right now sitting in not the reserve fund but in the auction fund, and given that the new gTLDs have added to the abuse problem substantially –

UNIDENTIFIED MALE: [inaudible].

NORM RITCHIE: We think it's totally logical to take some money from that fund to fund this group to fix the problem. So looking at making that part of the recommendation as well, or at least something to consider. Obviously, that's up to the board.

There's more questions still that we have for the Compliance group, just so we get everything straight. One of the questions that came up is if you currently are not able to do anything outside of what it says in the contracts, have you done the gap analysis of what it would take to actually go after systemic abuse and deal with it, and what would be required to change? I'm assuming that's been done at some point. Maybe it has and I don't know. We'll find out.

And I think that kind of covers the gist of it, but there's a bunch of recommendations and more to come, probably, on this as well as a fairly large writeup on it.

ALAIN AINA: [inaudible] question. I think at the beginning of this review, we had a briefing from [an ICANN staff called Dave] who was working actively on abuse. So what happened to that project? Now [we're hearing that] we don't have data on the abuse, etc.

NORM RITCHIE: Dave left ICANN. I don't think he's been replaced. He's a tough person to replace, actually. And he was in the SSR team, but that doesn't mean that he actually deals with the abuse. He could identify it, but it's compliance that would deal with –

ALAIN AINA: I mean, [I think there is one point that] we don't have any data, but he was working on data, was designing how to collect data. He was working on data. I thought ICANN was building a set of data on –

NORM RITCHIE: [That's DAAR.]

ALAIN AINA: [inaudible]. Okay. Then the second thing I want to add is when I hear what you just described, we don't have this to deal with, so it reminds me that ICANN has tried something some years ago about building a [cert, DNS cert][inaudible]. So it looks like now we're trying to maybe call it a center of excellence, trying to do it. So, have we learned anything from this [cert] project which was cancelled at some point before we started looking at this? Because I remember that the [DNS cert] project was to deal with kind of – have an entity inside ICANN to coordinate the response, including this abuse, because like you said, there are parties outside, inside, etc. [inaudible].

But [that has failed] at some point, because people said, "We don't want ICANN to do that, etc., spend ICANN money on that," but now I'm hearing that, okay, they want to try something else. [inaudible] during the discussion they mentioned what has been tried before. I don't think this should be seen as some new or something coming from nowhere or something. It must be based on existing attempt to address the problem. And I don't know if there is [inaudible].

NORM RITCHIE: I'm not aware of any past attempts to do this within ICANN. They typically have not really tackled abuse. So the SSR team obviously deals with it, but then they deal with groups outside of Compliance area. And they get dragged into a [reactive] point of view or law enforcement contacts them or whatever. But to my knowledge, I don't think this has been tackled before.

I think it'd be awesome, actually. I think it'd be huge for ICANN. Big win. So any thoughts or anything? Everyone kind of just like "whatever?"

One of the things that we're discussing is whether it should be part of ICANN or an arm's length organization, a new organization but arm's length from ICANN. I don't know.

RUSS HOUSLEY: My concern about it being too far a distance would be then you would have to use a huge amount of that money to make an endowment to keep it continually funded. So I think closer gives the board more options.

The original plan for tomorrow was to spend the time getting the recommendation writing done. I think we have an opportunity to start that now and finish it tomorrow. We have about an hour left today. I knew that we were going to end up in a place where we had some editing, merging, combining to do.

There's a couple clusters here that seem to make sense, for example the 30, 31, 32, 33, 34 all need to be smushed together. That's probably

going to take the whole time left for somebody to do. Somebody want to do that?

LAURIN WEISSINGER: So the issue with those is that a lot of them come from Eric, and Eric is, I believe, not on the call.

RUSS HOUSLEY: That's correct.

LAURIN WEISSINGER: So that might be – I'm not sure if it makes sense to do this without having [inaudible] because they're literally all his.

RUSS HOUSLEY: Yeah, but I think we came to an agreement that they are highly redundant and repetitive, so let's take the parts that are the same and then make the rest bullets about the things – right? Was that not what we said yesterday?

UNIDENTIFIED MALE: Ish.

RUSS HOUSLEY: Ish? Oh, KC, Laurin and Eric should do these.

NAVEED BIN RAIS: Before we move on, I just would like to ask, there are a bunch of like draft recommendations at the end of this document, which are stated as in progress. So should we discuss this now since we have time, or are we waiting for somebody to propose something better than that one before we can discuss it?

RUSS HOUSLEY: So Denise said she would take that action, so I thought we'd let her. Does that make sense? We did briefly, very quickly, look at hem when she pasted them in there. But it's certainly reasonable use of our time to read through them and highlight anything where there's a concern.

NAVEED BIN RAIS: But what is my first concern is that there are 21 of them.

RUSS HOUSLEY: Yes.

NAVEED BIN RAIS: 21 along with these 40-odd would be too much.

RUSS HOUSLEY: But she admitted there's overlap. So we're not adding another 20. She knew she had worked separately and therefore there was no merging beforehand.

Alright, well, they're lettered now. I don't know who did that.

LAURIN WEISSINGER: That is as it was. I copied it in.

RUSS HOUSLEY: Okay. Like A absolutely overlaps with a recommendation we already made about doing audit. There's some point here that aren't there, and that's the kind of merging that needs to be done. The next one's very DAAR-oriented, but it talks about pulling some things from the CCT recommendation and the WHOIS RDS review.

NORM RITCHIE: You mean B?

RUSS HOUSLEY: I'm sorry, B.

NORM RITCHIE: Yeah, so B is I believe right now with the DAAR data, they get data on TLDs, but not on a registrar basis, so they can do that easily, of course, so they should get it on a registrar basis.

RUSS HOUSLEY: C is already covered in part in the one from Kerry Ann where it says don't just make automatic renewals but make sure there's a review process. [And like I said, in part.] [I don't know if] the first part of D is anywhere else, but then the DAAR parts are I think elsewhere.

LAURIN WEISSINGER: The first part should also be somewhere, because it's the proactive anti-abuse, which is covered somewhere.

RUSS HOUSLEY: It's also covered in the CENTR recommendation.

LAURIN WEISSINGER: Yes.

NORM RITCHIE: Right now, Compliance is very reactive.

RUSS HOUSLEY: Right. Okay. I think that list that appears in the third paragraph – so this one may end up standing [alone.] F is DAAR. I think these are things that she would like to see improved about DAAR, right? So it should be merged with the other DAAR discussion.

LAURIN WEISSINGER: It's more about like this specific text and this being broken up into specific points is something we talked about but didn't have written down.

NORM RITCHIE: Yeah, so DAAR currently serves two main purposes. One is for presentation of aggregate data, so what's the health of the industry, what's going on, and the other one is actually a tool to do analysis of registries, registrars and abuse trends.

So one is public, one tends to be more sensitive and internal. So G is talking about WHOIS rate limiting. Even ICANN can't query the WHOIS servers in the volume that they require. It's very weird, but true.

RUSS HOUSLEY: But true.

KC CLAFFY: I should note that SSAC –

LAURIN WEISSINGER: KC, we got as far as "I have to note that SSAC," then nothing.

KC CLAFFY: [inaudible] advisory on this last year. It actually got some serious pushback, but there was a second version released. I won't go into details, but it's not just ICANN that has difficulty reaching the WHOIS servers, rate limiting, there are issues. It's everybody.

LAURIN WEISSINGER: KC, is this SAC 101 that is mentioned? Do you happen to know?

KC CLAFFY: Yes. I think so. And then there's like a V2 of 101 [inaudible].

RUSS HOUSLEY: So H overlaps with other transparency reporting that we're calling for, although I'm not sure the CCT review part, the interplay with that is called out there.

NORM RITCHIE: Yeah, the [inaudible] report was specifically targeted towards new gTLDs though because that's what the CCT was tasked with. So that should actually be expanded to cover all TLDs.

KC CLAFFY: You mean 101 was only [inaudible]?

NORM RITCHIE: No, the [inaudible] report. So that was the abuse analysis was in new gTLDs.

KC CLAFFY: Oh, got it. Yes.

RUSS HOUSLEY: Put that in a comment in the Google doc.

KC CLAFFY: One of the things that report did was comparing the new gTLDs to the older ones, legacy ones, but I don't remember if they did [inaudible].

RUSS HOUSLEY: So recommendation I is part of the systemic part that will be addressed by the proposed center, and so is J, right?

KC CLAFFY: [inaudible] I have some qualms about the center of excellence [inaudible] that I shared [inaudible]. I'm worried it's a [inaudible] declared checked off, and SSR3 won't have [inaudible] whether it's achieved its objectives. So I'm wondering if we can [inaudible] some measurable metrics [inaudible] what we wanted it to do.

RUSS HOUSLEY: Yes. We know that it needs to be measurable and so on as opposed to just establishing the center, "We're done." But that work, basically since the idea came up based on last Tuesday's call, it hasn't gotten attention enough to be fleshed out a bit more and made crisp and measurable.

KC CLAFFY: Okay. I'm happy to help with that.

RUSS HOUSLEY: Awesome.

NORM RITCHIE: I think the key measurement there should be the decline in abusive registrations.

RUSS HOUSLEY: Well, that would be how SSR3 should measure whether it had the intended effect. And maybe we should just flat out say that.

KC CLAFFY: We could, except I'm worried we'd get mired in "What's the definition of [inaudible]? Which categories of abuse [inaudible]?"

RUSS HOUSLEY: That's why part of that recommendation says, "Get consensus on what systemic abuse and the various other kinds of DNS abuse are," because you're right, you could spend forever arguing that.

NORM RITCHIE: Yeah. I agree. So the precondition on all of this is that we're all speaking the same language. So that requires defining abuse and the different types of abuse, and also putting some narrative around them about common words on what this means, what it looks like, so everybody understands it, but also have legal definitions that then can actually go into agreements [inaudible].

KC CLAFFY: I mean, again, this conversation has been going on for over a decade and it's going on right now in the EPDP [inaudible] kind of potential

abuse should justify access [to redacted WHOIS data.] So I don't think we get to say. We need legal definitions, because the pushback is going to be, "Which country's legal definitions?"

NORM RITCHIE: Yeah, but I think there's some that we can agree on. I know there are some gray areas, but I think there are some that everybody can agree on, like everyone could agree on what is Phishing.

KC CLAFFY: I think we should not necessarily leave this to the community but say this is our understanding of the best available definition right now based on what [inaudible], based on something. But again, I [inaudible] all get pushed forward or we kick the can down the road for ten years. So if we just say, "Go make consensus on the definition of abuse," we're doing it again.

NORM RITCHIE: Oh, yeah. Okay. Got you. Totally agree, and I believe the recommendation actually says consult cybersecurity experts to start with the definition.

RUSS HOUSLEY: But I think that she's proposing that we say, "And use these definitions until you get a better one from the community."

KC CLAFFY: And we can cite – we can go – it doesn't take that long, I'm sure M3AAWG will tell us in an hour what they think the definition should be. But we should go say, "According to this, CCT used this, we think it's reasonable unless somebody has a peer reviewed reason it's not, and M3AAWG says this and it agrees with CCT's definition except for this."

And again, I'm willing to do that work or help do that work. But it means we as SSR2 team should get consensus. And if we can't get consensus on what the definition in the review says, all bets are off for the rest of the community getting consensus.

NORM RITCHIE: Yeah. That's a great idea, and we can go to like APWG and ask them what's the definition of phishing. That's what they do.

RUSS HOUSLEY: Or M3AAWG.

NORM RITCHIE: Well, M3AAWG does it as well, but APWG as well.

RUSS HOUSLEY: That's a great idea. Please, but do your other writing first.

KC CLAFFY: [inaudible].

RUSS HOUSLEY: Okay. I think we're up to K. This one is different than the others. Basically, this is one that CCT pointed at us. This is Denise picking up the reference from them, suggesting a way forward. But some of this is related with the CENTR as well. It's probably the place we would –

LAURIN WEISSINGER: Just as a note for the remaining recommendations, I have put a suggestion where we could move them off into [– so Russ, nothing?] [inaudible]. So this could also go into compliance, because it's kind of talking about compliance, so we could just fold that into a compliance recommendation.

RUSS HOUSLEY: [He had] nothing on this one.

LAURIN WEISSINGER: No, there, move into compliance recommendation.

RUSS HOUSLEY: Where?

LAURIN WEISSINGER: There, in the title.

RUSS HOUSLEY: Oh, there. Okay, so moving to L, Laurin's recommending that this goes to the research part of 19. [inaudible] what 19 is?

LAURIN WEISSINGER: 19 is recommendation on research and briefings. So this could go in there that we say “Get external insight into the following topics and do some of your own stuff.” We have two or three more that we could move into that, and that’s like one set.

RUSS HOUSLEY: Okay, and then this one you're saying 39?

LAURIN WEISSINGER: Yes. So this would be 38. I'm sorry, that’s a typo. This is 38, which is the compliance and excellence center. No, sorry, 38 is just compliance.

RUSS HOUSLEY: Actually, I don't know if that GAC advice has a definition of abuse in it. It’d be interesting if we steal it.

NORM RITCHIE: [They] recognize those ones I picked. I think actually in the registry agreements, there's five areas covered. Not spam, oddly, but it’s farming, phishing, malware, botnets and child endangerment. And child endangerment is the only globally agreed to abuse. There's no debate. But all the other ones are debatable, of course.

RUSS HOUSLEY: Okay. N is another DAAR-related one, so –

LAURIN WEISSINGER: No, this is not actually DAAR-related. This is literally on rate limiting registrations by registrars based on abuse. And the only one I could see is number 16 where we're talking about our concerns and what kind of measures should be added to the contracts. And I think this is the only place where this would go, because this would essentially be a contract change.

RUSS HOUSLEY: I see. And it's about measurements as well.

NORM RITCHIE: [inaudible].

LAURIN WEISSINGER: [inaudible].

RUSS HOUSLEY: As is O. Laurin's.

LAURIN WEISSINGER: Yes. The reason for that is that that also includes a variety of other measures and not just validation but also technical and nontechnical measures of reducing domain abuse. So this is probably something that could go into that list of issues.

RUSS HOUSLEY: K and P clearly goes in the compliance section. Yeah, it's an extra point I think we want the center to pay attention to.

NORM RITCHIE: Yeah, I didn't get a chance to talk to Denise on this one, so I'm reading this as assuming to say that ICANN should be allowed to purge out the abusive registrations before the others are transferred over.

RUSS HOUSLEY: Yeah.

NORM RITCHIE: So they basically have their own – the registrar of last resort exists and is operated by Shadowserver, but this seems to be implying another holding tank.

LAURIN WEISSINGER: I think this belongs together with item – oh, it doesn't have anything. It's third paragraph page 25, and it's recommendation and then revision of procedures to ensure safety, and then my note is "Move together with item P" because this is also like a [inaudible] takeaway.

NORM RITCHIE: Yeah, so ideally if you have abusive registrations [inaudible] abusive, you don't want to turn them off, you actually want to analyze them to see what traffic's coming in. So I'd fall back into that abuse center of excellence that we need a better name for.

RUSS HOUSLEY: Okay, so statement about Q or R?

LAURIN WEISSINGER: No, this was about P.

NORM RITCHIE: [inaudible].

LAURIN WEISSINGER: So there is P, which refers to this issue, and then the third paragraph on page 25, which does not have a letter anymore.

RUSS HOUSLEY: Which is down in R.

LAURIN WEISSINGER: No, it's already past R.

RUSS HOUSLEY: I see.

LAURIN WEISSINGER: This would be probably S.

RUSS HOUSLEY: No, S is below. I see. It's P prime.

LAURIN WEISSINGER: It is R2 then. I don't know. So essentially then we move item P and what is now R2 into the anti-abuse center.

RUSS HOUSLEY: Yeah.

LAURIN WEISSINGER: Okay.

RUSS HOUSLEY: Okay, so what are we doing with R? It's also going there. R1.

LAURIN WEISSINGER: R1 is compliance, although probably, again as a note, there will be a lot of stuff that refers to compliance and that anti-abuse center, because they obviously are highly related.

RUSS HOUSLEY: [inaudible]. Okay, S. Move to contract [centered rec.] Which one is that?

LAURIN WEISSINGER: Give me a second.

RUSS HOUSLEY: Oh, I see. Okay. That wasn't a whole thought before.

LAURIN WEISSINGER: No, it was not.

RUSS HOUSLEY: Okay. T, fold into rec 16.

LAURIN WEISSINGER: Yes. So a lot of this stuff is already in recommendation 16, for example the multi-factor authentication or two-factor authentication's in there, registry lock is in there, DNSSEC is in there. So most of this is already there, we just have to make sure we're not losing anything.

NAVEED BIN RAIS: One quick remark, actually, a recommendation when we see like a sample recommendation, we talked about this earlier as well, might be like one, two sentences as a whole in the end. And I see that we are moving too much towards the same recommendation.

We can say [it's a] recommendation set, but I think it would eventually be resulting in more than one, and those will have to be split, under one section of course, like compliance will have a section, but compliance will result eventually into, as I see, four to five different recommendations that may be related to each other, but a recommendation can't be like really long one including subpoints and all that. If we have subpoints, we have to put it as a separate

recommendation. And there's a lot of stuff I see that we're pushing towards the same.

RUSS HOUSLEY: I'm not sure – I think we need to look at each one and figure out what the dependencies are and write it in such a way that it's easy for the reader to see the dependencies. And maybe that's subpoints, or maybe that's text in them, "Don't do this without doing that." But that's part of the next pass. We're going to have to figure that out.

LAURIN WEISSINGER: The other thing is that if we look for example at how ICANN does the strategic plan, that is actually an approach that works, where there is kind of like a key objective, if you want, that is, "Do X," and then there are defined goals below that, but you'll essentially say, "To get to this point, these are the things you have to do." Which is another option how we could approach it.

So for example in this case, essentially, the same points are there, we just want to make sure that we're not losing anything in the process. But most of it is just out there.

RUSS HOUSLEY: Okay, that's it, and then we went through the three that Kerry Ann offered that we then pasted at the bottom. So we have now –

LAURIN WEISSINGER: [Can we put those just all SLA?]

RUSS HOUSLEY: Yes, it's all SLA. I think it's more like make an SLA recommendation out of those.

LAURIN WEISSINGER: Yeah.

RUSS HOUSLEY: Okay.

LAURIN WEISSINGER: We have an SLA [cluster, I think, that exists as such.]

RUSS HOUSLEY: I don't think so. Right. Okay, I know I'm fading quickly. Are others?

LAURIN WEISSINGER: That's when they usually call for everyone to get up, walk around the table twice, that kind of stuff.

RUSS HOUSLEY: I'm observing we have about a half hour left.

LAURIN WEISSINGER: [We can take like five minutes.]

NAVEED BIN RAIS: It's because you took our lunch time.

RUSS HOUSLEY: Okay. Fair enough. I did. So we're breaking even, that's what you're saying. Okay, I think tomorrow, we will make a writing pass, divide that work up, start a new Google doc so that Angie doesn't get mad. That's the goal for tomorrow. I think we'll wrap here.

UNIDENTIFIED MALE: [inaudible].

RUSS HOUSLEY: Yes, we will be doing that, I hope, before we wrap up tomorrow. We're also going to do the agenda for the call next Thursday, because –

KERRY-ANN BARRETT: Russ, can I [inaudible]?

RUSS HOUSLEY: –there'll be a leader call in-between. Go ahead, Kerry Ann.

KERRY-ANN BARRETT: I'm so sorry, I've been trying to talk for the past two hours and for some reason my audio has just not been working, and then you guys would move on, so I just decided not to hold you guys back. So I'm so sorry that I haven't been inputting. I find it hard to go on the computer to unmute myself to be able to unmute myself on the phone. So I'm registry sorry, guys.

I had just one suggestion before you guys end. At some point, other persons are going to be reading the Google docs, and agreed text, I don't know how much you guys would want persons – after we've had the agreement throughout these two days – to be changing the text dramatically. Is there any way to just put probably a key that says either agreed, like something besides the ones we don't want altered too much at this stage, and more the text hat needs to be drafted for persons who come in afterwards, no? Or you think it should be safe until you guys start back tomorrow?

RUSS HOUSLEY: So I think it's safe, because the issue would be if someone wanted to make a major change, whereas I think we've agreed to a basic direction as opposed to agreed to this particular text.

KERRY-ANN BARRETT: Okay. [inaudible].

LAURIN WEISSINGER: In that table, you will see the following things: consensus, which is there is either a "yes" if there is really everyone was like "Uh-huh," then

there's like a “rough” when we said “okay, we’re happy with the direction,” and then there's some where it’s like either “clarification needed” or “edit outstanding” where we essentially haven't discussed it properly because it’s not at a point yet where we can make that determination. So that might be a helpful resource for that.

KERRY-ANN BARRETT: It is. Apologies for the compliance text. I pasted over and saved all the [privacy] stuff I was working on in the document I had, that’s why I wasn’t able to add it. But I know what I had said, so I'll redraft this and I'll include it so at least you guys will have the text again.

RUSS HOUSLEY: Okay. I think if that’s where we are, that’s where we are. So you'll see we pasted your three recommendations to the bottom of the recommendations doc.

KERRY-ANN BARRETT: Yes.

[END OF TRANSCRIPTION]