MONTREAL – SSR2 Review Team (Day 1) [C]
Friday, November 1, 2019 – 09:00 to 17:00 EDT
ICANN66 | Montréal, Canada

NEGAR FARZINNIA: Good morning, everyone. Welcome to the day one of your face-to-face meeting in Montréal at ICANN 66. Today is Friday, November 1st, SSR2 meeting, and I'm going to start going around the table introducing ourselves. Negar Farzinnia, ICANN Org.

CHARLA SHAMBLEY: Charla Shambley, ICANN Org.

KERRY ANN BARRETT: Kerry Ann Barrett, review member.

LAURIN WEISSINGER: Laurin Weissinger, also a review team member.

ALAIN AINA: Alain Aina, SSR2 review team member.

HEATHER FLANAGAN: Heather Flanagan, technical writer.

RUSS HOUSLEY: Russ Housley, review team.

DANKO JEVTOVIC: Danko Jevtovic, board member and liaison to the team.

NORM RITCHIE: Norm Ritchie, review team member.

STEVE CONTE: Steve Conte, ICANN.

NEGAR FARZINNIA: Thank you, everyone. I have the agenda up. First item on the agenda as we've gone through the roll call and the welcomes is going over any SOI updates. I'll turn that over to Russ.

RUSS HOUSLEY: I'm not aware of any SOI updates, but we can move into the next thing. We have had this document which I call the red-letter document, because you can't remember the URLs for Google docs.

[This week, we] kind of wrapped up that document on the call on Wednesday, and then Heather went through and made a cleaned up version that has no numbers in it to totally confuse us, I guess, so we can rearrange things, and then number. So I'd like to work from the other document, Heather's cleaned up one.

HEATHER FLANAGAN: While she pulls it up, can I say a few things about it?

RUSS HOUSLEY: Yes.

HEATHER FLANAGAN: Okay. Within this document, you're going to see a couple of artifacts from how it was created, some extraneous spaces, colons that don't make sense quite where they are. That's because I have another copy, not too dissimilar from the red-letter document in terms of just how marked up it is. I haven't shared that because I don't think it's legible, but to create this copy, it was an accept all changes to that, so you're going to see some weird artifacts from that.

as I mentioned on the mailing list, I don't consider this edited at all, so it still needs work in terms of fixing the references, finding the right citations, even some spellchecking could help in places. I was really just pulling it together so that we could read it successfully, which I think was something that needed to happen, because otherwise we were never going to finish the recommendations.

RUSS HOUSLEY: Yes, I actually really appreciate that because I found it far easier to go through, which I spent a couple hours yesterday doing, just to understand where we are, the organization of it. I put a bunch of comments in. I don't know if those are visible or not.

Anyway, the idea is to go through this and make sure that we have addressed each of the recommendations. We'll look at each one of them and make sure that now that you can see the flow of the document and those other things that were all lost in the red-letter document, how we want to deal with each one of these.

So I think we can skip all the front matter dealing with background and why the SSR2 exists and the pointer to the bylaws and all of that stuff. I think that's just factual context. What?

NEGAR FARZINNIA: [inaudible]

RUSS HOUSLEY: To the section right after this horribly colored table. Okay, so right now, each of the sections has a discussion of what the Work Stream is about, what methodology was used, and then some recommendations. So I think we, in the case of the SSR1, have gone through this front matter several times so I don't think there's any open issues. If there are, please raise them now.

HEATHER FLANAGAN: This isn't an open issue but an observation, Negar, I'm not seeing any of the comments. There should be like a comment based on methodology from me.

NEGAR FARZINNIA: Thank you. Give me one minute to see if I can change the settings.

HEATHER FLANAGAN: And for everyone who has it open in front of them, remember that suggestion mode will make our lives a lot easier later, or at least my life a lot easier later. I mean I can figure out what you did from the change log, but it becomes much more complicated.

NEGAR FARZINNIA: There you go, it should be all good now. It only takes like four people.

RUSS HOUSLEY: Norm, go ahead.

NORM RITCHIE: Could you just reiterate where we want to be at the end of Saturday or Sunday morning?

RUSS HOUSLEY: On Sunday, we are briefing the community on our recommendations. So where I want to be by the end of our time between the two days is totally fine with all the recommendations in this document, all the review team members, and have a slide deck that talks to them for use on Sunday.

NORM RITCHIE: How big is the time slot? There's a lot of recommendations, so you're obviously not going to present them all.

RUSS HOUSLEY:	Yes, we are.
NORM RITCHIE:	Oh, really?
RUSS HOUSLEY:	Because how else do we share with the community what we want to talk about in the halls this week? What the draft slide deck looks like is bullets about each of the recommendations followed by a slide with the full text of the recommendation. So we can talk to the bullets, but anybody who downloads the deck will have the full text. So we need to synchronize that. I know Heather will have a long day on Monday morning synchronizing those slides to what we come up with during the two days. Make sense?
NORM RITCHIE:	I just don't know how we're going to present all of them in a session.
RUSS HOUSLEY:	I totally get that, but how else do we show to the community where we are?
NORM RITCHIE:	Maybe we should show the high priorities?
RUSS HOUSLEY:	Right now, we have only one priority level.

NORM RITCHIE: Yeah, so that's something we'd have to rectify.

RUSS HOUSLEY: Indeed. Let's see how far we get. Yes, Laurin.

LAURIN WEISSINGER: Hi. Just as a note as well, I'm not sure if everyone has seen it, there is quite a lot of discussion coming from the board regarding prioritization, all that kind of stuff. So most likely, after session I believe on Monday when this is supposed to be discussed, then we can look at stuff like that again based on what they actually want.

RUSS HOUSLEY: Well, they had the call on Wednesday.

LAURIN WEISSINGER: Yes. But it wasn't all clear from that call.

RUSS HOUSLEY: No, it wasn't. So on Wednesday, there was a call between the board caucus and all of the review team leaderships or all of the review teams. They shared what their vision was, basically asked for some feedback, and then while we were flying, they sent an invite to participate in a panel session on Monday regarding that. Sure would have been very helpful to know there was such a panel session coming before that phone call, but that isn't what happened.

Anyway, so the team leadership needs to figure out how we're going to handle that. I'd like to focus on the recommendations now as opposed to that. So let's see how many of these we can consolidate, how many of them we can – we've often asked ourselves the question, what if we can only make ten, where would we draw the line? And it's clear we're not going to get to ten, but let's make sure everything that we are recommending is important and has consensus. Yes, Kerry Ann.

KERRY-ANN BARRETT: So Russ, given what Norm's mentioned and the fact that we do want to focus on the recommendations for presentation, maybe we could skip over this text now, because I think the preamble and interaction –

RUSS HOUSLEY: I think that's what I was suggesting.

KERRY-ANN BARRETT: It wasn't clear, I wanted to make sure. So let's skip all this now and let's just jump in.

RUSS HOUSLEY: Yes, that's what I was suggesting when Heather said, "Wait, where's the comments?" Go ahead.

LAURIN WEISSINGER: Just a small point, regarding the slides, because in my mind, it's a little bit fresh this document that heather prepared. So while reading through the recommendations, I noticed that some of them are of course clear but have a number of more than one action item below that. So if you're presenting them in a slide, it will be nice to point them out, like what ... Thanks.

RUSS HOUSLEY: Okay, let's scroll down to the first recommendation. Yeah, this one, which is one that I did, by the way, way back in ... I don't even remember when, when we divided up the SSR1s and did the work.

As I read it again yesterday, it read a lot like "Just do what you said you were going to do." So I suggest we just delete this recommendation but move that stuff that's there into the findings to the recommendation that says finish the implementation of SSR1. Make it so. That's what I think.

HEATHER FLANAGAN: I'm going to make notes to myself rather than try to change it on the fly.

RUSS HOUSLEY: It's up to you. Sure.

LAURIN WEISSINGER: I have a question regarding the finishing of the SSR1 implementations, because I understand, while I was not on the team from the beginning, but when I joined, there was some discussion also about [inaudible] standard, like the report from the Org was done. And of course, the team analyzed, made a clear framework and do its work and found it’s lacking and some stuff needs to be done. But maybe it’s not – somewhere in the document, it has to be clear what is the gap, because otherwise, if you just tell them to finish it, it’s not actionable.

RUSS HOUSLEY: I understand that, but I think that in this particular case, there's a heck of a lot of this is what we found when we looked as opposed to this is what needs to be done, which is really just one sentence and I think those one sentences can be summarized in bullets at the end of that one. Okay, next one.

That top comment is to the previous, I believe.

HEATHER FLANAGAN: [Are you happy with just accepting that change?]

RUSS HOUSLEY: So now you're French? That’s funny, now it’s coming up in French.

HEATHER FLANAGAN: It’s just you. I'm fine.

NEGAR FARZINNIA: Yeah, it’s the presentation laptop, so if everyone’s logged into the Google doc directly, you'll see everything in English. I'll work on getting the language changed for you guys on the presentation laptop.

RUSS HOUSLEY: Is that Negar’s tend, or Steven’s tent? Go ahead, Steve.

STEVE CONTE: I think this is going to be kind of a theme for the SSR1 recommendations, so I'll make a blanket statement. This one, I think, fits well. There's a bunch of shoulds in here, and I'm not sure exactly where the recommendation starts, but like in the beginning it says ICANN should follow security management system as defined by ISO 27001. And I know at least a number of years ago, we had a conversation face-to-face in Los Angeles with the IT team, and my memory – which arguably is faulty – was that they embraced various certifications and pieces of various security management teams.

So if the review team is looking at implementing ISO 27001, I just want to caution the review team on creating either unimplementable, or if as we look at the other SSR1 recommendations and it says you should go implement this, and as you noted before, ICANN thought that it did, so it’s a perception of completion. Please try to remove all ambiguity from what you're saying what we should be implementing for SSR1. Thank you.

RUSS HOUSLEY: So I actually vividly remember that conversation, because the question that remained was, hey, okay, if you believe you have aligned yourself with that document in principle, where's the certification? So the question is to go all the way through certification. And I very much remember a whole bunch of discussion about whether this was the right document or if we should use this cybersecurity framework, and on and on, and the subteam that did this said, "No, we want 27001 and we want it done fully certified, audited, the whole bit."

So I think that's what it says in the last sentence, complete certification. And that's really the point of this. The rest of it is, how did we get here? Yes.

LAURIN WEISSINGER: A few notes on this. Number one, I think the text is far too long right now, so it's unclear. We have to significantly shorten this recommendation.

RUSS HOUSLEY: It's a Google doc.

LAURIN WEISSINGER: In the Google doc.

RUSS HOUSLEY: No, it is a Google doc. You can help.

LAURIN WEISSINGER: Yeah, I already did, actually. And I think the key stuff has to come out. And in terms of what Steve said, as I was part of these discussions, it's mainly this kind of choose something but have a third party audit this. It's not so much about okay, it has to be specifically that standard. That's actually the key.

RUSS HOUSLEY: [inaudible].

HEATHER FLANAGAN: And that was actually one of the points where I was confused on this one where it seems to drift from specifically ISO 27001 to accepted international standards, then back to ISO 27001. I couldn't tell what you wanted to do.

STEVE CONTE: And granted, there was a period of time when I was not here for this discussion. So if you had already spoken to – I guess my main point is that engineering and IT should be aware that this recommendation is coming in order to make sure that this recommendation is implementable. So if that happened, then I withdraw my comment on that.

RUSS HOUSLEY: I'm not saying that we're done, I'm saying that we had that discussion. Norm.

NORM RITCHIE: Yeah, let's take it back to the original meeting with ICANN in LA, and this topic came up. Not so much under SSR1 though but it just came up as part of the rest of the review. To Laurin's point, that was actually what the result was, it was kind of like if there was a recognizable certification in place, then we just say, has it been audited? Yes? Check, done. It would be that simple. So we were really favoring towards having that, but not in particular – I don't remember being in particular 27001.

RUSS HOUSLEY: So then we should change the words to say, instead of – I remember Scott McCormick saying, "But 27001 defines the term information security management system, and that's the definition we want them to use."

LAURIN WEISSINGER: Obviously, if we're just going for the definition, probably that's [why] we're saying as defined by. It doesn't mean you [then] have to get audited according to that standard.

NORM RITCHIE: I don't think we should, to that level of specificity, say it has to be that certification. I think that's a bit too much. That's like kind of saying you have to write code this way, use this language.

RUSS HOUSLEY: So Laurin has made a bunch of suggestions, deleting like a third of the text which is a good thing, as long as it didn't create ambiguity. So my thought is that the yellow text probably doesn't belong in the recommendation but belongs in the findings.

Okay, I'm not seeing any tents. Does that mean that people are now happy with the recommendation as Laurin has put suggestions in? Laurin, you want to share?

LAURIN WEISSINGER: This is just editing right now. Kerry Ann found more superfluous language.

HEATHER FLANAGAN: As an observation, when going through this, if I saw the word "should," I assume that turned it into a recommendation, "ICANN should do something." And that's why I pulled this out of the findings text, because you've got a "should" in there. You're telling them to do something.

KERRY-ANN BARRETT: It could still stay in the findings text by just making it a suggested way of implementation, so like in relation to that they could consider, so they could move to a "could consider" doing a roadmap because that would help for the transparency and the openness, bla bla.

HEATHER FLANAGAN: That's pretty much exactly what I was thinking, if we turned it into like "ICANN may find it useful to create ..."

LAURIN WEISSINGER: Go ahead, have a look now if this is fine. There we have all the text that's relevant. Okay, so I essentially went through, deleted everything that was kind of doubled up. Particularly the yellow part was actually reflected apart from one sentence in another paragraph. So now we're at a two-paragraph recommendation which I hope is slightly better.

RUSS HOUSLEY: So in the first word of the second sentence, I think it should be ICANN Org. ICANN, space, capital O. We have like three different ways of doing that in this document. we need to pick one.

ALAIN AINA: By the way, to add while you're writing that, that's one of the things I noted. It's ICANN but sometimes it's clear that ICANN Org is meant, and sometimes you write ICANN but I'm thinking that is actually f or the community because Org cannot implement that. So it needs another run through.

RUSS HOUSLEY: Heather has pointed that out and asked for help identifying where we mean the community and where we mean Org so that – so if we can do that while we're making this pass, let's correct it. Yes, Laurin.

LAURIN WEISSINGER: This is a question to Steve, do you think that the rewrite now up in front works better?

STEVE CONTE: It is much less ambiguous and I appreciate that. So now I'll pick a different nit. Where did that go? So right here, there's an explicit that the team recommends, and all the other ones are should. So now we get back into the weeds of wording.

RUSS HOUSLEY: So we should replace the word “recommends” with “should,”

UNIDENTIFIED FEMALE: No, just [inaudible].

RUSS HOUSLEY: Because all of our recommendations are written with “should.”

STEVE CONTE: And that’s fine, it’s just when you say ICANN recommends, that becomes a much stronger statement than all these “shoulds” that are within that section.

RUSS HOUSLEY: Well, we can't say “must,” we can't say “shall.”

LAURIN WEISSINGER: “Should” is clear.

RUSS HOUSLEY: Right, as long as it’s clear, I think we’re happy. So I wonder if we want to add to that list this cybersecurity framework, just because we talked about it. Kerry Ann, you're shaking your head.

KERRY-ANN BARRETT: I think there's no need to add it. Everyone knows [NIST,] and if they decide to – but I think saying the certification, they can choose, I don’t think we need to put [NIST] necessarily.

RUSS HOUSLEY: Okay. I'm fine, we could just – I remember we’d explicitly discussed that one. That’s the only reason I said that. Alright, anything else on SSR1 9?

ALAIN AINA: Russ, the full text of recommendation 9 is not what we have there, so maybe at some point we made a decision to – because the full text of the recommendation said ICANN shall access certification options with a commonly accepted international standard, bla bla, for its operational responsibility. ICANN should publish a clear roadmap towards certification. That’s the text from SSR1 document.

RUSS HOUSLEY: So you want to repeat the original recommendation? Is that what you're suggesting?

ALAIN AINA: No, just to make sure that we all agree on what we had done, because if you look at this text, for example the full text, it shows more that the Organization is asked to study and show and provide a roadmap [then doing] the certification itself. But the text the way it is here, it just looks like they're supposed to do some kind of certifications which they have not done, but the recommendation was saying that they should look at options and develop a roadmap. So it's just to make sure that we have a common understanding of what we had done here.

RUSS HOUSLEY: Isn't that what the second paragraph says?

ALAIN AINA: Yeah, exactly. The paragraph is there, but my point is that you saw the time it took for us to agree on what, what not, and so that maybe we should refer to the original test of the recommendation. Maybe it can also help us to really understand what – because we are assessing the implementation of a recommendation [inaudible].

RUSS HOUSLEY: Oh, the assessment is elsewhere. This is what we think they should do going forward, because it's more than just finish what was started.

This is where we're adding either clarity or measurability, or even sometimes changing directions slightly.

KERRY-ANN BARRETT: I think just based on what Alain says, just to make sure in terms of uniformity, what Laurin just did is to put the assessment, the creation of the roadmap, [inaudible] further, we think that having done that, execute by getting certified. You've done the scanning, execute after. So I think the reverse, we flipped it, would help here.

RUSS HOUSLEY: Is that what you meant? I'm sorry. I'm glad Laurin understood what you meant, because I obviously missed something.

KERRY-ANN BARRETT: Just to add the element that you said, once Heather gets into it, and then further, having done your environmental scanning, you know which one you're going to get, at least get certified now.

RUSS HOUSLEY: Laurin?

LAURIN WEISSINGER: Quick question. You can see the text marked in red, that is me. Shouldn't that be also ICANN Org?

HEATHER FLANAGAN: Yeah.

LAURIN WEISSINGER: Okay, just wanted to call consensus.

STEVE CONTE: Maybe also the ICANN above it as well, the line above.

NEGAR FARZINNIA: I just wanted to highlight for everyone that we do have a fix of the language issue, but we have to stop sharing, so I asked the support team to wait until the break time to fix this.

RUSS HOUSLEY: When we started, was the Zoom room up? Okay, so we have no remote participants? Okay, it just occurred to me that we didn't ask any of them to –

NEGAR FARZINNIA: Actually, we do, Ramkrishna is.

RUSS HOUSLEY: Ram is remote?

NEGAR FARZINNIA: Yeah.

RUSS HOUSLEY: Ram, welcome. I know it's a bad time zone where you are, so thank you for joining us, and please speak up, don't wait for us to notice a hand, because we're staring at the Google doc, not Zoom. Thank you.

STEVE CONTE: Ram says thank you and acknowledges your comment.

RUSS HOUSLEY: Okay, we're moving now, I think, to SSR1 recommendations 12 and 16, the SSR strategy and framework.

DANKO JEVTOVIC: I have a question that's actually related to what's written here, but more general. By reading through the document, I have noticed that some of the things have not – on the number of places that stated that – like here, ICANN must address security issues clearly, publicly and [inaudible]. So a lot about public information, but for the security issues, my understanding – I'm not very much expert in this particular field as you are, but some of the issues are often not publicly stated because of the security reasons. So, does it have to be clarified, maybe not here but some other places where the public information is mentioned?

So if you just make the old recommendations that everything should be public – and at least it was my brief reading, maybe you know we're getting a bit too far in some directions. Thank you.

RUSS HOUSLEY: So my memory of that discussion was, sure, there might be a moratorium for a certain amount of time to let people do things, but we should all learn the lessons of the past and that was what was discussed. So maybe there's some words we can add here to make it clear that there can be a time frame while the issue is being dealt with before it becomes public.

KERRY-ANN BARRETT: And Russ, one of the things I remembered from our discussions, Danko, was that we had two approaches. Tell me if I'm wrong, it was one kind of – [not forecasting but actually seeing trending,] so the information would be anonymized and then shared with the community so the community would see the trends that are happening, and the other angle, I remember when we discussed it – I don't know, someone on the team who was technical had pointed out that entities that have specific issues – because we do have that data that ICANN Org should contact that them because if it is that it threatens the entire ecosystem, that information would be publicly available to them and then work with them to fix it. But the whole idea was once we saw any future trends coming out of behaviors that we're seeing, that's what should be publicly shared for the community's benefit.

So I think it's to make it more distinguish real-time threats that are more seen trends being developed. I remember that discussion clearly.

DANKO JEVTOVIC: Okay. thank you for the clarification. I don't have issue with the text in this particular recommendation, but [just remind you of my] general ask about keeping confidential some of the security-related information for obvious reasons.

RUSS HOUSLEY: Heather, are you going to stick some words in after “publicly,” or make a new sentence?

HEATHER FLANAGAN: I was thinking of doing something like this. I need to wordsmith it because “appropriate” is too vague.

RUSS HOUSLEY: How about established? Because the whole point later is that we have a consensus document on what the practice is going to be. So they could, as part of that document, establish a maximum for the moratorium. Okay, anything else? Steve, I recognize you.

STEVE CONTE: Can I ask the review team to look at that very next section where it says enforce baseline security across both parties? Could I ask the review team to consider what “All parties” means and what “enforce” means around that?

RUSS HOUSLEY: I think enforce is forecasting – the foreword where it says implement the practices in contracts, agreements and MOUs.

STEVE CONTE: More specifically, all parties, what does –

RUSS HOUSLEY: I don't have an answer for that one.

LAURIN WEISSINGER: I might not remember this correctly, but I guess we were onto like baseline security across probably the contracted parties, and then we could change "enforce" to "promote."

RUSS HOUSLEY: Yeah, I like that, actually.

LAURIN WEISSINGER: Which is less powerful, but something ICANN can actually do.

RUSS HOUSLEY: Yeah, exactly. We'd like it to be broader, but we have a remit issue. Okay, seeing no tents, hearing nothing from – go ahead, Norm.

NORM RITCHIE: That's kind of low threshold to say "baseline security," and it's kind of like saying "This is as much as you need to do." I don't think that's a good thing to be promoting.

RUSS HOUSLEY: So what you're saying is you can establish a bar, but people should be encouraged to exceed it?

NORM RITCHIE: Yes, exactly. that works, whoever just did that.

LAURIN WEISSINGER: Norm, would that work?

NORM RITCHIE: Yeah, works for me.

RUSS HOUSLEY: Go ahead, Kerry Ann.

KERRY-ANN BARRETT: [Sorry, I had to cancel] because I try not to speak out of turn. I was just asking Steve – and I'll put it on the table. It's not a new recommendation, so don't freak out when I speak, but I think there'll be some benefit under here if not under the previous SSR1, but at least as a part of our findings, to suggest some form of a MISP because I think the information sharing platforms among either operators or somewhere along the line where there's a more free space for them to discuss it, and discuss the threats that they're seeing at a more [inaudible] level, and it would address the issue of privacy, security and all that. But I don't know how or where we could stick it, but I think there would be some value.

As I'm reading this and hearing some of the concerns that come, we've never discussed a MISP during the calls, and I think it would be a good way forward for them to consider organizing, whether they come up with what they actually want to share, what levels they would want to share it, and the common person could share at those levels openly without it being just a broad brush publicly with different issues being disclosed at different times. And that would kind of help them to organize the threats that they're seeing, what levels, who it affects, it if goes to the root or the DNS or not, and kind of help to build that public information that we want to be issued out. It could be categorized and shared among the operators that it impacts directly quicker.

So I'm saying I wouldn't want a new recommendation, I'm not proposing that, but at least consider how we could frame that thinking or plant the seed for something like that to be developed as ICANN goes forward. I'm really sorry, just when I'm reading it, the first thing that came to my mind is a MISP.

HEATHER FLANAGAN: You're using, I think, an acronym as a word and I'm not familiar with it.

KERRY-ANN BARRETT: It's an information sharing platform, ISP. The MISP is a technology or kind of methodology that works among a lot of [certs] to share information. We implement it within our organization and our member states, and it's been done in Europe and a couple of other places have these platforms. But it's an open technology platform that allows information sharing without any issues on cybersecurity threats.

RUSS HOUSLEY: I wonder if we shouldn't take that not here but in the abuse reporting section. I realize that you're talking about something more than abuse, but that's where we already have the discussion about public reporting of all complaints and all of that stuff. So what you're really saying is, let's create a forum for these guys to share with each other.

We also have some discussion in the futures privacy section, and maybe that's a place where we could broaden – where we talk about monitoring relevant and evolving privacy legislation. That would be a place where parties could talk amongst each other about those as well.

KERRY-ANN BARRETT: And I think more than anything else, what's resting on me when I see this and the questions that Steve has raised about being specific, if we can say to ICANN not actually [set to do very] specific categories and the players – because I think it's when he said, "Who are the all parties?" And it hit me that, yeah, we need to actually segment the different levels of persons that would need to speak to – operators would be different. So just to kind of see who would need to speak to each other and what are they talking about, what are they sharing publicly? Because unless they have that taxonomy for them to be able to say, okay, this is what I need to share on, they won't identify the stuff and they just won't speak. So I was just thinking out loud as I saw when he said all parties, I just automatically, my brain went to that.

HEATHER FLANAGAN: If this is something that's going to be a suggestion across multiple recommendations – because I've heard I think three different sections where this kind of thing could live – we have the suggestions at the bottom of the document, and sounds like that would be the right place for it.

KERRY-ANN BARRETT: Agreed.

RUSS HOUSLEY: Sure, because it actually covers a lot of these. Yeah.

KERRY-ANN BARRETT: And I can help get the language for it. As I said, we're currently implementing it right now for the Pacific Alliance, and we've done a lot of work on it, so I can help. Probably anyone else who's done it in their region could let me know, and if not, I could ask around and see.

ZARKO KECIC: Can you elaborate what we should or what [we have done envision?]

KERRY-ANN BARRETT: In terms of what I'm proposing as the suggestion for them? Yeah, so pretty much, we've been talking about the different stakeholders that were asking ICANN for the DNS specifically, there are different persons who are participants in the DNS system and we're asking them to share information on threats.

One of the things that just because Steve said who are the all parties, and then he mentioned, okay, what are they sharing? And then Danko raised the whole issue of what should be publicly shared and what should be confidential because of security concerns.

The information sharing platform allows persons to actually – some persons have done the technical thing of putting nodes on their networks and been able to share the information fluidly. Other persons have done –

ZARKO KECIC: I'm familiar with MISP. You mentioned that we're using that as well.

KERRY-ANN BARRETT: Okay. So I think specifically, what I'm suggesting is that in the suggestion section, as Heather pointed out, we could say to ICANN Org to explore how this could be implemented among certain stakeholders to make the information more fluid and quicker for them to be able to disclose. So it's just to see how can we facilitate this information sharing, and that's just one methodology, but I was just thinking out loud, as I said. If it's not something we could concretize ...

NORM RITCHIE: So you're just really saying, a pointer, for instance, you could use this.

KERRY-ANN BARRETT: Yeah.

NORM RITCHIE: Should we do that generally?

KERRY-ANN BARRETT: I think that's why Heather suggested that we'll put it in the bottom.

RUSS HOUSLEY: She suggested we make a fourth suggestion. We have three down there now that are not recommendations but are process things that are not always SSR. But what would have made our job easier is whether we put suggestions.

NORM RITCHIE: But I'm thinking just generally – well, specifically and generally – we actually – when we have a pointer like that, such as, because it adds clarity to the recommendation, I believe, it also I think would help out ICANN or the community understanding what our thoughts were. But the other point, you don't want to say "You have to use this."

RUSS HOUSLEY: We can add the pointer, “See suggestion blah.” Go ahead, Kerry Ann.

ZARKO KECIC: I'm just thinking what kind of sharing will be. How I understand this, that ICANN should disseminate information to other parties, not receive anything. So there's different kind of information sharing systems, and I'm thinking of RDS or some similar system to implement in regard of this.

KERRY-ANN BARRETT: That’s a good point, and you guys are more in the field and [inaudible] what's out there. I was just thinking that as the technology is going and how people are using the DNS, are we confident that ICANN Org will see everything? That’s my concern. There are things that academics, different persons would be seeing that – if it is that we’re sure that ICANN Org where they sit, they really have a bird’s eye view on everything that’s happening, then fine. It could be from ICANN down. But I'm just not convinced right now with how the technology is going. To me, I think there’ll be some benefit, and that’s why the definition of what they're sharing and what could go both ways, and we could actually define what goes bidirectional and what is one directional.

So I think that’s what I'm thinking of.

ZARKO KECIC: I agree, but serious project to do.

KERRY-ANN BARRETT: Suggestion.

HEATHER FLANAGAN: I've added suggestion four and tagged Kerry Ann to help make the language work.

KERRY-ANN BARRETT: I would tag Zarko too.

HEATHER FLANAGAN: Perfect.

KERRY-ANN BARRETT: If you'll be tagged. Do you accept my tag?

RUSS HOUSLEY: Okay, I'm not seeing any more tent cards. Are we ready for the next one? Okay. SSR1 15. Hopefully there never is an SSR1 15.

ZARKO KECIC: Just one question about SSR1 recommendations. Are we going to get rid of them when we finalize this document, or they're going to stay?

RUSS HOUSLEY: The ones that we’re doing now are going to stay. There will be one that says finish the implementation plan that you said you were going to do. But these are the ones where we felt clarity or measurability, or a slight change in direction was needed.

ZARKO KECIC: [These are new recommendations based on the] [inaudible]

RUSS HOUSLEY: Correct.

ZARKO KECIC: Yeah, but that’s my question, are we going to get rid of SSR1 recommendation and put that as follow-up on recommendation [inaudible]?

RUSS HOUSLEY: Yeah, it’s an SSR2 follow-up, but it’s based on our findings from reviewing SSR1 recommendation 15 in this case. But this becomes our recommendation. Yeah, otherwise it lingers forever and just continues to grow.

UNIDENTIFIED MALE: [inaudible].

RUSS HOUSLEY: Yeah. Okay. So this one's short. Hopefully it's easy too. I wonder just for simplicity, now that we've already talked in the previous about the moratorium and everything, if we shouldn't merge these two and make recommendations 12,15 and 16. Just leave the words the same but make the categories together, because the best practices across contracted parties and then the disclosure reporting seem to be aligned, people think.

LAURIN WEISSINGER: Yes, I agree, we can probably streamline this. Also just a note, this recommendation is not particularly smart. We would have to add some words so it's actually trackable.

RUSS HOUSLEY: That's exactly what I was going to ask. You want to put a minimum frequency? Okay. At least annual?

LAURIN WEISSINGER: I believe that having a minimum frequency would help. I'm not sure what we would want, once a year, twice a year. Norm?

NORM RITCHIE: I'm not going to comment on the frequency but did want to comment on who that is reported to. Do we even need to say that this should also be reported to the board? Or is that automatic?

RUSS HOUSLEY: I thought the point of the anonymous metrics was meaning it was public. Otherwise, why did you make them anonymous if you were keeping it to the board? Okay, so I think maybe we make that clear by saying public reporting, at least annually or something like that.

NORM RITCHIE: Yeah, my point more on reporting to the board is that it implies there's a receiver on the board, rather than just generally here's a thing to the board, it's actually someone on the board that receives the security input.

RUSS HOUSLEY: I'm sorry, Laurin, then Kerry Ann.

LAURIN WEISSINGER: I think it makes more sense the other way around.

RUSS HOUSLEY: Okay.

KERRY-ANN BARRETT: Norm raises a good question, because it's a good point to [inaudible] distinguish what we think is for general information or public consumption and what is for action. And I think who the report goes to is critical, and then decide what we're recommending is a type of information where it's going for the audience that needs to digest it.

So what Norm says is when they have the report, what are they reporting? If it's critical threats that needs correcting, who's actioning it? If it's just for the public to go, "The Internet is screwed, panic!" So it's like, what are we intending? What is the action that needs to be corrected, and what is knowledge so everybody is kind of on the same page with where this is going? So the who, as Norm says, I think I would support us thinking it through, what is our intent? Once this knowledge goes to the public, then what is the intent? For academics to be able to write? I think they have their own information already. For the public to go, "Oh my god, the Internet is going to die?" Yeah, maybe. But I think thinking through as to who's the audience for this information, and if that's the case, what is the information we're trying to get? Vulnerability is a lot of information. It's many categories of vulnerabilities. Some are technical and need correcting, some is just for general trends which we already know. so I think it's a good point to start thinking through here, really, who?

LAURIN WEISSINGER: Yes, this works well this way around. I think there are two things here. One is the reaction to events, and the other one is to track this information. So the former is mainly relevant to contracted parties, players in the system. The latter however is important to essentially the ICANN community to kind of influence, inform the policymaking process.

So it both has to be in there from my point of view. And probably the former which goes to people who are actually active in the system.

That one should probably be more regular and more operational in nature, and the other one would be more like a report.

RUSS HOUSLEY: So the problem is in the sentence that begins after the page break where it says these disclosures, you're saying they shouldn't be the same disclosures?

LAURIN WEISSINGER: The form would likely have to be different. So the contracted parties, if there is something wrong, they should be informed right away, they should be told operational information so they can fix something. That, going back to previous comments, you might not want to have public right away, but then a few months later, it can be in a public report that says, "Oh, this was an issue, we informed about, it's now fixed." So it's two different types of information, I think. People might disagree with me. I can see Heather is unsure of what I'm saying, judging from her face.

HEATHER FLANAGAN: I'm trying to decide whether that brings these back to two separate recommendations or not.

RUSS HOUSLEY: I don't think so.

HEATHER FLANAGAN: Okay.

LAURIN WEISSINGER: So what I would propose is we turn the text around again. So we start with prompt disclosure to the contracted parties and then the next bit is what's currently up top to kind of say, after a while, you should then give this to the community so the people who make policy have an insight into what was going on. Works? Okay, I will try.

RUSS HOUSLEY: So that it flows in the same order as the previous, is what you're saying?

LAURIN WEISSINGER: Yeah.

KERRY-ANN BARRETT: We still haven't answered Norm’s question though. Does the board disseminate this, or who does it?

RUSS HOUSLEY: I think we’re asking Org to have processes. Is Norm happy with that? Do you think it needs to go through the board, or just the board should also be informed?

NORM RITCHIE: I'm thinking of a case where a disclosure may be significant enough for the board to want to consider whether to disclose it or not.

RUSS HOUSLEY: To disclose or not?

NORM RITCHIE: Yes.

LAURIN WEISSINGER: A quick question as I'm just writing this; you mean disclose to whom now?

NORM RITCHIE: To anybody. It should be the board’s decision.

KERRY-ANN BARRETT: For the public?

LAURIN WEISSINGER: So essentially, the board gives it to contracted parties at all times because they need to fix, or they might withhold from the contracted parties? That’s my question.

NORM RITCHIE: No, the public, I guess.

LAURIN WEISSINGER: Okay, so essentially, this is I think in line with what we said, right? You can do a report without openly saying, “Okay, this is the stuff we talked about three minutes ago.” You don't have to put technical detail in there. So that would be compatible as far as I understand.

NORM RITCHIE: Yeah. Am I happy with this yet? No, because I'm trying to think of the purpose of this, actually. It’s kind of like, decide what to do periodically on how you're going to disclose things to certain parties, is kind of how I read this. I'm not getting it as very actionable by anybody.

RUSS HOUSLEY: What I think I'm hearing is when there's some kind of a really significant vulnerability discovered, you want it to go through the board before it becomes public?

NORM RITCHIE: Yes. I think that’s what I'm saying. I’d kind of like to hear from the board on that, but ...

KERRY-ANN BARRETT: Would it be a public interest thing then? Because you have those things that are, because of the public interest and the public good, it should be disclosed, and then you have those things which are technical, operational level that just needs to be fixed. So [for me it’s like a] distinction between ...

RUSS HOUSLEY: Also, when you tie this to the previous paragraph, we're talking about after consideration for operational security, so the established moratorium could have a clause that says if it's significant enough, then go through the board first. But do you want the recommendation to require that? That's what I'm asking.

NORM RITCHIE: Yeah, that's a good point. It should be done on these bases, I guess. So I assume that people follow the correct processes.

RUSS HOUSLEY: We have to assume that.

NORM RITCHIE: Correct judgments. I guess what's in my mind is that there probably will be cases that will come up that we can't even fathom what they might be, and they might be very sensitive and there might be other things going on at the same time, such as someone wants to take over control of the domains, oversight away from ICANN, and you could have something that happened, although minor, becomes a rock that they can throw at ICANN. That's the kind of scenario I'm thinking of.

DANKO JEVTOVIC: Just a short comment, I actually don't know what will be proper thing in this case, but I believe it's also a big legal issue. We can discuss here about want to build this thing in the ICANN, but also with contracted parties, if you're talking about contracted parties, we have publicly listed companies, so [implementing] Securities and Exchange Commission, you can make a securities fraud if you don't do it in the proper, legal way, and it's something that is beyond my knowledge of the U.S. legal system, but disclosure is a complicated issue.

LAURIN WEISSINGER: Quick question. I tried to include what has been said in the changes, so if people want to have a look if this could work now, I would be interested to hear what you think.

ALAIN AINA: Russ, can I? So I'm not sure – or maybe someone need to help me understand, why are we mentioning contracted parties? Because for example, the ccTLD registries are not contracted, but I think they're also eligible to get disclosure of vulnerability. So, do we really need to mention contracted parties? I'm talking just about the term of contracted in this ICANN ecosystem.

KERRY-ANN BARRETT: Alain, could you probably think through what term would cover both? I think the issue we had was initially just said all parties, and then we put contracted to narrow down the scope. But what language you think would capture that operational grouping?

ALAIN AINA: Maybe interested parties?

KERRY-ANN BARRETT: That's too broad.

LAURIN WEISSINGER: I've put relevant now, which sounds broad, but it means – you never know, as Norm said, who might be affected. So if the party is relevant, then it should be –

RUSS HOUSLEY: But do you mean relevant, or do you mean impacted, or ...

LAURIN WEISSINGER: I'm like thinking of a technical bug, there might be relevant parties that are not contracted parties. They're also not a CC registry, for example, certain owners of resolvers. And they might be relevant to fix.

RUSS HOUSLEY: Sounds like all parties, that people objected to earlier.

LAURIN WEISSINGER: Depending on who has to take action, essentially quoting Kerry Ann right now.

RUSS HOUSLEY: Then say that, parties that need to be involved in correcting the problem.

NORM RITCHIE: Okay, so some of this stuff will fall into hosting companies. I don't know how you're going to contact all the hosting companies. Maybe there is some way of doing that, I don't know.

RUSS HOUSLEY: Well, they also use software that’s in common, so maybe you talk to the vendor of that software.

NORM RITCHIE: Vendors, yeah. I don’t want this to backfire is what I'm saying. I understand the goodness in it, but on the other hand, the greatest source of hacks is available from certs, because they publish them. What happens if people don’t correct those? Then they become vulnerable. So my concern is, especially we’re having a hard time describing what's a contracted party, what is in that ecosystem, you could have a flaw in DNS services providing, but not contact the DNS service provider. Therefore, they become vulnerable and you’ve actually caused the harm by trying to correct it. So that’s what I'm struggling with here.

LAURIN WEISSINGER: Norm, if we added “trusted,” would that help? Because then there is a choice process involved. Someone might be relevant but is untrusted so they wouldn't be informed right away. Would that help your concern?

STEVE CONTE: I agree strongly with what Norm's saying, and maybe this conversation is bigger than this room, and should be inclusive of contracted, noncontracted, relevant, impacted, whatever words we want to use, that should be inclusive of those parties to determine the level of action and disclosure and get that community feedback and buy-in to this. So maybe it's worth considering simplifying this to say that maybe just that should happen, and let the larger community decide what that is and how it should happen.

RUSS HOUSLEY: I think Negar is next.

NEGAR FARZINNIA: Just noting for the record that KC has joined us in the room. She also put a comment in the chat to say that she's here for about 15 minutes while ATRT3 is on break.

KC CLAFFY: Hi, guys.

RUSS HOUSLEY: Norm, then Kerry Ann.

NORM RITCHIE: Yeah, these recommendations don't stand alone. For instance, if you had a CSO in place, then that person would make the call. Does this go out? He's the responsible person, the buck stops there. But given that it's currently standalone, this is something that's good, so we've got to trust somebody – I'm not sure who that somebody is – to do the proper thing, and I don't know if we specify it that way or if we provide a link to, "See, we recommend getting a CSO whose job function would include this," or do we even bother with that? I don't know.

RUSS HOUSLEY: Kerry Ann?

KERRY-ANN BARRETT: Just listening to Steve at the end, is it a matter of like the recommendation above where we speak to exploring how they should work? Because there's a lot of work that would have to go in to determine the parties, the type of information, the level of information once you define the types.

So maybe as Steve said in terms of setting up the process for this to happen, recognizing we think this needs to happen, to do that, our recommendation is that you begin the dialog and discussion towards this end, but this has to be your end goal. So I don't know I that would probably help, because as you said, this is the end. There's a whole process behind getting there. And that who process, I don't think it will be done between now automatically and the next SSR team. So maybe be specific about what we're asking them to do is explore how this would look and how to get this done, because vulnerability disclosure, it's a whole tier behind – as you said, we talked about trusted parties, untrusted parties, what information is actionable, what isn't, and what is critical and what is just good to know.

NORM RITCHIE: Yeah, so I would be fine with this recommendation if it started off under the umbrella of a CSO, but there isn't one.

KERRY-ANN BARRETT: [There never was a CSO, this would always just be there.] It's the function that we're speaking of, not the person or his post.

NORM RITCHIE: Yeah.

ZARKO KECIC: I have a question about CSO. Is John Crain acting CSO, or am I wrong?

STEVE CONTE: [That's a level of definition.] John is the chief information security, stability, resiliency officer which looks at the SSR. He's not necessarily the CSO in looking at the security of ICANN Org's systems and things like that. So there is some bleed over to that, but it's not a very clear path, nor is it in his description to be that path either.

RUSS HOUSLEY: Yeah, and we have a later recommendation that recommends a C-suite person be established. And I think Norm is trying to link these two recommendations, because you want an officer to be making the judgment.

LAURIN WEISSINGER: I think what we have to do is put this position really high up and provide links in that recommendation to relevant recommendations below. So we could say we envisage this position to have authority or responsibility, whatever it is, variety of things. For example, see recommendations one, two, three, four, five, six. I think that would work and would provide the context to then explain what's coming later.

RUSS HOUSLEY: I think you're suggesting pointers in both directions.

LAURIN WEISSINGER: Yes, and particularly to have that position higher up so that it becomes before this, if at all possible.

RUSS HOUSLEY: I would say you just totally shuffled the whole report. Heather says no. Go ahead, Zarko.

ZARKO KECIC: Yeah, in regard of reporting, we will have exercise in Serbia from 11th to 15th of November and I will be late for that, but I'll join them, and I'll tell you how it's going. Plan for now is to have direction from bottom-up, so if I am disclosing a vulnerability and incident in my organization, I'll put level of security and confidentiality of that information.

So if I want to share with only high-level officials, if it is public, it will go public. So something like traffic light protocol should be established over here and let's leave this alone. We spent a lot of time, and think about exact cases and we'll come up with some resolution on this.

KERRY-ANN BARRETT: I think overall, we're all on the same page.

LAURIN WEISSINGER: Reading the new text, does it reflect our discussion? Is it functional as is, or do we need further changes? I think we have to scroll up on my screen.

HEATHER FLANAGAN: It's configurable.

RUSS HOUSLEY: It is, it's totally swappable, which is why when you use somebody else's machine, it doesn't do what you think it ought to.

NORM RITCHIE: Laurin, this is to you because I think you wrote it. Can you explain or clarify that statement there a little bit? I'm not sure I follow that one.

LAURIN WEISSINGER: The red marking?

NORM RITCHIE: The highlight.

LAURIN WEISSINGER: Okay.

NORM RITCHIE: Starting with considering operational security.

RUSS HOUSLEY: Are you saying drop the first three words?

NORM RITCHIE: My confusion is based on clear communication plan, for reports, I'm not sure where the reference is on that.

LAURIN WEISSINGER: I think this got mangled as well, reading this. Give me a second.

KERRY-ANN BARRETT: I think the intent is what we were speaking about earlier about doing the classification as even Zarko gave the example of TLP where at least there is some clear categorization of what type of information, to which audience. The communication plan is supposed to encapsulate what, who, when.

NORM RITCHIE: And do we reference that communication plan anywhere?

KERRY-ANN BARRETT: No, we haven't. So I think what we spoke about is that there needs to be some process, as you highlighted, to develop what information has been shared with whom and when. And then from that process, the communication plan would stream from it. I think that's what we wanted to articulate there.

RUSS HOUSLEY: And I think that's a pointer back to the previous paragraph which talks about the consensus document which provides those clear, measurable, trackable ... Anyway, I think those are related, which is why we merged them.

LAURIN WEISSINGER: Steve, is this better now, or should we explain what we mean by considering operational security?

RUSS HOUSLEY: Why don't we just delete that? Because then the rest of it makes sense.

LAURIN WEISSINGER: Happy to do that as well.

KERRY-ANN BARRETT: Yeah because that categorizes it further. Can we put it in the reverse though?

RUSS HOUSLEY: Couldn't hear you.

KERRY-ANN BARRETT: Sorry. The communication plan comes at the end, so I think –

RUSS HOUSLEY: Well, it's restating part of what comes in the previous paragraph.

KERRY-ANN BARRETT: So, is it that the communication plan is developed based on what's above?

RUSS HOUSLEY: Yes that's how I read it.

KERRY-ANN BARRETT: It should be a follow-on and not a new ... Somehow [inaudible] that and then based on that, establish a communication plan to be able to do these things. So based on the above, ICANN Org should establish ... So make sure that it’s correlated so they understand we want a process, then a communication.

RUSS HOUSLEY: Or the best practices should include a clear communications point.

KERRY-ANN BARRETT: Something like that, that would be very clear.

RUSS HOUSLEY: Laurin, are you typing?

LAURIN WEISSINGER: Yes. Give me a second. I'm trying. I'm just wondering, because we’re now just saying containing anonymous metrics, wouldn’t it be more appropriate to kind of – I'm not sure how to word it, to essentially say, put in these reports what can be shared as much as you can without compromising anything. Wouldn’t that make more sense than just to say, anonymous metrics?

RUSS HOUSLEY: I don't know, but I hear Eric in the back of my head going, “I want metrics.”

LAURIN WEISSINGER: Oh, yeah, I'm all for the metrics, I'm just wondering if the way we're framing this now, like we're being maybe too specific in that case. So to give you an example of what I'm thinking about, a report might contain case studies, if you want to call it that, where it's like, oh, this was the type of stuff we did. And if the report just says, "Okay, we had ten things that happened and that's all we can say," that's not particularly useful to anybody. So I'm wondering if we might want to change that slightly.

STEVE CONTE: Maybe something along the lines of establish reporting conventions as prescribed by the security community, or something like that? There are – Danko expressed it before, there are legal considerations that have to be noted, and there's also the trusted considerations too that if you disclose improperly, you won't be invited back to the table the next time something happens. It's important to maintain those parameters and stay within the norms.

LAURIN WEISSINGER: Would it be fine to say these reports should responsibly disclose information but avoid information that would be problematic for operation security, something like that?

RUSS HOUSLEY: I think Steve's suggestion was to tie it back to the community consensus, right?

LAURIN WEISSINGER: How would we write that?

RUSS HOUSLEY: Responsibility report within the norms established in the best practices. Steve, did I correctly capture what you were saying?

STEVE CONTE: I'm going to let Laurin finish.

LAURIN WEISSINGER: Yeah, the typing isn't ideal yet.

STEVE CONTE: So I think community is too broad and I think we should possibly consider security community, because it's really about the legality of disclosure and breaching the trust factor of that community, and not necessarily the ICANN community. I want to be very specific on what community best practices that this recommendation should follow.

KERRY-ANN BARRETT: And just to add, I was just suggesting to Laurin that he adds the word "as defined," because "responsibly" doesn't really add any value unless responsibility disclosure is based on what is defined as being responsible in law. It's not like an automatic thing. As defined. Not by applicable law, I don't think it has to be by legislation. It could be by agreement, it could be voluntary responsible disclosure as well. So it doesn't have to be prescriptive in law but it has to be defined by a community. Whatever the community is that's defining it, it has to be defined. But I wouldn't put "By applicable law."

LAURIN WEISSINGER: I mean that there is applicable law to this kind of stuff.

KERRY-ANN BARRETT: There is, but there's also voluntary responsible disclosure that has nothing to do with legislation.

NORM RITCHIE: Yeah, I'm thinking this whole area is not mature enough for us to say this is what you should do, because you have things – if a company is public, then have certain onus on them. Let's say they didn't disclose something, then ICANN turns around and discloses it, that would be a big mess. The laws are different in each country right now, there's no international. Most laws don't exist.

I just think this whole area is too immature for us to say thou shalt do this and have any use for it. We can report things, but I think it would be not very useful.

KERRY-ANN BARRETT: I think that’s why we’re trying to say above that we need to have some kind of categorization above. That’s what we’re asking them to do, and then based on that, the disclosure that comes out should flow from what is agreed by the community. I think that’s where we need to punch, that needs to be very clear. Then it avoids that issue that you're identifying.

NORM RITCHIE: They're regular reports so I'm not sure what the purpose of them would be. So unless I can figure out what is the purpose of this report, I don't know why we’re recommending to do it. “Here's some numbers.”

RUSS HOUSLEY: I hear Eric in the back of my head,” We don’t know until we have the numbers.” How many times has he said that? Are we done with this one? If so, I think we deserve a coffee break. Alright, let’s take ten minutes.

STEVE CONTE: Really quick, before we take the break, we’re off record and I can talk a little bit more, because we’re in budget building phase right now and there's a couple of things that are happening or going to happen that are actually going to impact and complement what you guys are talking about, but I don't want to be on record for it.

We're discussing community involvement with a DNS security facilitation center. This was tried a number of years ago with not great success. We're trying it again, we're trying to get community involvement on this. This would kind of go into the ability to talk in a trusted and secure way. We're also talking about a program called [Kindness] in collaboration with Manners in the IETF world, which is about establishing norms within – no offense – the contracted parties, the noncontracted party community about best practices and things like that.

We don't have budget for it yet, we're trying to get budget for it. I can't speak on it on the record, but please keep this in mind while you guys discuss this, because we are looking forward about these kinds of things, and these kinds of recommendations would be quite helpful to frame the need for those types of endeavors. Thank you.

RUSS HOUSLEY: Alright, let's get started. I think we're on SSR20 at this point. SSR1 recommendation 20. Yes, budget, this is what Steve was talking about. Yes, Laurin?

LAURIN WEISSINGER: [inaudible].

RUSS HOUSLEY: It's only four lines. Four and a half. You're not happy?

LAURIN WEISSINGER: [inaudible].

RUSS HOUSLEY: Go ahead, Zarko. Hopefully Laurin will figure it out while you're talking.

ZARKO KECIC: Yeah, thank you. I have a couple of suggestions over here. First, when you have fully transparent budget in regard to security, that may be problem at one point.

Another thing, I don't think that we need fully transparent budget. I would rather consider in making this positive way that the budget should be sufficient for all SSR activities that ICANN Org has, and also, I'll add enough resources to do annual plans in regard of SSR.

What we have now is that the SSR team is small, there are not enough people to do, and we are adding more functionalities and functions to them with our recommendations, and they do a lot of travel, a lot of stuff. If you think that somebody get training in Africa, Far East or somewhere, it is only one day but it is two days to get there and two days to come back. So that's the entire week. We should think about that.

So I would reshuffle this, and don't think in fully transparent budget for SSR but to make that more usable to say that budget and resources that SSR has are sufficient to fulfill their role within ICANN.

RUSS HOUSLEY: Kerry Ann.

KERRY-ANN BARRETT: I agree with Zarko, but I think we would have to, one, hit the original text, with the original textbook to transparency, and then do the [inaudible] we want to ensure with the transparency that it covers the needs that SSR would have for its functioning. So the original spoke to just transparency alone, was very simple. So if we're taking that aspect of it, either it be a part of our finance or we just do it like we did the other one where it's kind of plus from our end to make it effective. So just to consider that this was the original only spoke to transparency, so we'd have to decide if it's a new, tack on.

RUSS HOUSLEY: Laurin, do you know now?

LAURIN WEISSINGER: I don't. I will make it even more complicated. Considering that we're trying to cut down on recommendations, I'm wondering, isn't a more important part what Zarko talked about? And transparency is a kind of nice thing obviously and relevant to ICANN as a community, but first you need the money to spend. I'm wondering, do we want to change the approach, kind of say, think about the budget? And if you do, be transparent as SSR1 wanted, so the transparency becomes the addon instead of the –

RUSS HOUSLEY: Isn't that what the next recommendation says?

LAURIN WEISSINGER: Yeah, so this was the next point. That's why I was saying wait before, because I'm not sure if we need two for that.

KERRY-ANN BARRETT: But could we merge it like we did the others where we do 20 and 22, and then at least we'll hit Zarko's point, plus the transparency but let the transparency be the faded one, the less obvious, the ...

RUSS HOUSLEY: The difference was in the original SSR1 recommendation 22 the 22 was tied to the new gTLD stuff, and what Zarko's talking about is SSR budget and resource as a whole.

NORM RITCHIE: You just made the point that I was going to make, that that's tying it to the new gTLDs, which that ship has sailed because this was written seven years ago. And I agree with the other point, we should combine them, and I also agree with Zarko's point. The point was made here at the time, talking about new gTLDs, but like I say, that ship has sailed, so maybe we just kind of generalize it. Yeah.

HEATHER FLANAGAN: At least the way I had originally looked at the SSR1 recommendation 20 thing is the concern that you were expanding on is that you couldn't measure this because it wasn't granular enough, right?

RUSS HOUSLEY: Right.

HEATHER FLANAGAN: So now you're saying you're not so worried about that as you're worried about sufficiency, which sounds like its own very difficult thing to measure. What is sufficient? Are you basically asking ICANN to have an infinite budget on this? Because there's no way to figure out how much is sufficient.

KERRY-ANN BARRETT: The sufficiency component of it, how Zarko put it was I think the point that we need to make clear is when you spoke to even like Compliance and everything, everyone says they don't have enough money. There's not enough staff.

So I think what we're saying is if it has been that your inability to implement these measures have been for lack of resources, then have specific line items addressing the resources required to fulfill the recommendations that we're asking, because some of them may be encapsulated in one entity to be able to do these things. We've been talking about having the C-suite, but allocate the resources and functions necessary and put budget to fund these. It's not just sufficiency as a broad brush, but sufficiency relevant to the issues that we've identified in the recommendations to fix them.

RUSS HOUSLEY: Laurin, the way you're writing that is throwing somebody under the bus.

NORM RITCHIE: I'm going to continue with Kerry Ann's point, is that, again, with the lack of a CSO, someone at the C-suite level, there's no one at the table to fight for that budget, and that's part of the issue. So then it behooves the community to say, was it done sufficiently? Because that body is, again, missing. So I don't know if we want to bring that up here or not. Maybe not.

KERRY-ANN BARRETT: Norm, just to [inaudible] your question, I don't think we should bring it up here, but I thin kas we get back to the section that speaks to the C-suite, we can do a correlation. We're still stuck in SSR1 which we've been stuck in for two years. Once we get out of the weeds here, we can go back to the correlation to see how it will be supported by previous recommendations.

LAURIN WEISSINGER: I'm trying to find a good way to put in an element we discussed, which is Kerry Ann kind of mentioned that I think the most clearly, which is this transparency is needed so that every relevant department or function or whatever we want to call it has a given amount so that they can actually deal with it and not just a lump sum.

Do we still want to put it in? If so, what would be a good way to put it in?

RUSS HOUSLEY: Is everyone comfortable with the revised text?

STEVE CONTE: Can I ask a question for clarity?

RUSS HOUSLEY: [inaudible].

STEVE CONTE: I don't think that's going to change. The way I'm reading this, it sounds like the review team is asking for an itemized list, the transparency as an itemized list of activities and the funding around that activity for SSR.

RUSS HOUSLEY: That is what SSR1 asked for.

STEVE CONTE: So the only thing I would ask the review team to consider with the wording here is that some activities, there might be contractual considerations take place that we might not be able to – we might be in breach of a contract if we specify exactly what we're doing. I'm not the CFO, I don't know the details here, I'm not Legal, I don't know those details, but I want to be careful that we not reveal things that we legally can't reveal within a signed contract. So the level of transparency might need to be taken into consideration.

RUSS HOUSLEY: We're talking at the level of the budget. So one way to implement this would be to tag each item in the budget SSR-related or not. That would be sufficient.

STEVE CONTE: Okay. Yeah, I don't have the visibility to comment back on that, just asking for consideration around the potential of breach of contracts if we reveal the details of how much we're paying contractor X or vendor B or whatever.

RUSS HOUSLEY: No, what I mean is you already have the budget. That's already shared with the community and goes through open review and public comment. On that, you can't tell which items in that budget are SSR-related and which are not. That's what this is calling for.

STEVE CONTE: Okay.

ZARKO KECIC: We should clarify that because I didn't get that that way either. So I've raised my concern similar like Steve said, fully transparent security budget is not good idea. Having budget just to mark up what is security and stability issue, that's another thing and I agree with that.

RUSS HOUSLEY: I'm looking in the SSR1 report to make sure what I said is actually what they called for. So I just reread the section of the SSR1 report that led to the findings part that led to recommendation 20, and it’s really saying that when you look at the budget, you can't figure out which pieces of it are for implementing the SSR framework, and that’s what they're calling for.

KERRY-ANN BARRETT: How the first sentence even begins, it’s wrong, because one of the things – I think it’s very clear. When I read that, I thought there was a specific line item that was like a general statement, and it’s not. So I think it doesn’t appear either, so I think it’s more while SSR-related functions are covered under specific line items in the budget, it’s not specifically mentioned. I think that’s what we want. It’s the reverse. It’s like it could be assumed that it’s covered under different things in the line items, but there's no specific budget for SSR-related activities. I think that’s the issue.

HEATHER FLANAGAN: So while SSR-related activities may be covered under various ...

KERRY-ANN BARRETT: Under various – it's not specific as an SSR related [budget, it's specific allocations in the budget itself.] Even Laurin thought it's OCTO, but Steve said it's not OCTO, it's kind of littered throughout the budget under various things.

STEVE CONTE: In light of the conversation with Laurin, I think one of the challenges that we faced with SSR1 implementation on this was that not everything is cut and dry. This is SSR. Those that are easier, the challenge came into some of the pieces where there was aspects of SSR inside of a different project.

I think my recommendation to the team would be maybe have a conversation with Finance, with Xavier, Becky or somebody to help determine – to express the spirit, the intent of the recommendation and see if there's a way that Finance can help the Organization determine and achieve the spirit of – maybe more than the spirit, but achieve that recommendation without having incredible overhead of marking 3% of this project is SSR. And we have gone through exercises like that, and so to make it so it's – so the Org understands the intent of the recommendation, and we can try to follow that. So maybe a conversation with Finance before this recommendation is finalized may go a long way.

DENISE MICHEL: Thanks, Steve. That's, I think, a good suggestion. It would also be helpful if you could kind of more broadly give some thought to tactically and operationally why ICANN fell down on so many of the implementation of so many of the SSR1 recommendations.

and I understand the complexity of so many different teams and programs being involved, but I haven't really heard – it would be, I think, really valuable to hear your perspective, staff's perspective, on how we can support a much more robust and much better coordinated implementation plan I think coming out of SSR2.

Budget's part of it, but I think another part of it is staff coordination, operation, robust, detailed implementation plan, reporting, all of that. Thanks.

RUSS HOUSLEY: I think the discussion that started with the board is going to address a lot of that, because they are talking about dashboards for each recommendation from each review team on who's tagged with implementing and status. I think they get that that is needed in order for the community to understand how many recommendations are, each one has moving parts and all of that. So that's a conversation that's going on as a backdrop, but it's not at all clear that it's totally an Org thing. the board has clearly inserted themselves here.

Okay, do these new words resolve that concern about we're talking about the budget as opposed to – well, bot what Zarko and Steve raised earlier. Laurin, do you have to take it apart?

LAURIN WEISSINGER: Well, so, I think what we should do is put this one on ice and try to get that conversation as soon as possible. I know it's not great in terms of what we're trying to accomplish, but if this text isn't clear and doesn't work, then we have SSR1 all over again.

RUSS HOUSLEY: I totally get that. What I think we should do – that level of ice maybe is what's different, but we need to proceed with the presentation and we can certainly set up a discussion that says, hey, this is what we intended. How do we clarify the words to make it easier for you to do? Or vice versa.

So Negar, maybe we can schedule on one of the future team conferences to have the folks who put together the budget join us to have that discussion. You're still editing, Laurin.

LAURIN WEISSINGER: I added one key thing that Steve said for consideration, which is where possible and reasonable in terms of effort. Because if like 1% of something is SSR, it would be ridiculous to kind of go through this line item by line item. So just to kind of reflect that issue in this draft.

DENISE MICHEL: I have KC's voice in my head, which is mildly disturbing, where trying to measure possible and reasonable seems not possible nor reasonable.

LAURIN WEISSINGER: This could be defined. For example, we could say if SSR is greater than 10% or 20%, do list it, otherwise, don't. So I think this could be a footnote, what we mean by that. Just throwing this in the room, hope someone has comments.

RUSS HOUSLEY: So if you look back to the SSR1 report, what they're talking about is the amount of staff that are assigned to do SSR-related activities, including policy development, including the board risk committee, including SSAC, bla bla. Anyway, it basically was trying to say these are scattered all over the budget, we just want a way to understand what portion of the budget is related to this important piece of the ICANN mission. Maybe that's what we need to say.

LAURIN WEISSINGER: But I think this is exactly where Steve is coming from, if I understand him correctly. So if we have someone in policy who does ten things and security is one of them, then the question becomes, how much of that in percentage is roughly security? And this might work to some extent, but becomes really complicated if you actually try to break it down. That's why I was kind saying maybe we can kind of put in like a ceiling, say, "Okay, if it's 2-3%, forget about it, but if it's 25, you should list it." So that's the idea behind my last comment.

RUSS HOUSLEY: So instead of where possible and reasonable, say where a significant portion of the budget item is SSR-related ... I'm reluctant to move on while you're still typing.

KERRY-ANN BARRETT: Just a question. Somewhere in the document, we've defined what SSR framework is, right?

RUSS HOUSLEY: Yeah.

KERRY-ANN BARRETT: Just want to make sure there's a correlation. [inaudible]. Just to make sure that we put a pinhole that we make sure that we're very clear.

RUSS HOUSLEY: So in SSR1's recommendation, that was those things related to implementing the SSR framework.

KERRY-ANN BARRETT: So just to make sure, I know we have a definition section or references and terms, just to make sure that we're crystal clear, are we saying this is what ... So no one can ...

RUSS HOUSLEY: We do on like page two.

DENISE MICHEL: I think as we go through here, it would be great to have staff specifically create a list of items that need to be defined, that need to be footnoted, that need to be researched and referenced more clearly. Particularly those items relating to past ICANN work. So when we reference an SSR framework given the context for that, we reference the registrar accreditation agreement 2009, giving appropriate and footnotes to that. It'll require some research and things like that, but those issues will be coming up throughout our week here, and it would be great to just start a punch list so we can have a consultant take care of those. Thanks.

HEATHER FLANAGAN: That's part of what I expect to do, and I expect we'll jointly be highlighting that in here.

RUSS HOUSLEY: Are we done with this one? Okay. SSR1 recommendation 27, the last one.

DENISE MICHEL: I think it would be good just to add a couple words here. Boban isn't on the line, is he?

RUSS HOUSLEY: He's in the air.

DENISE MICHEL: I think my recollection – Norm was there as well – that when we did sort of a deep dive into the risk management framework that they had, the subteam was happy with the results and what they had actually –

ZARKO KECIC: [It was comprehensive.]

DENISE MICHEL: Yeah, it was comprehensive and seemed appropriate. I think it would be good just to note there that the risk management framework and related activities that we reviewed were comprehensive and appropriate. Just to acknowledge that. Yeah, it's positive we're suggesting more process changes than substantive.

HEATHER FLANAGAN: Is that a different thing than the ...

DENISE MICHEL: [It's actually the risk management framework.]

HEATHER FLANAGAN: Right, which is –

RUSS HOUSLEY: Which we talk about in the middle of the recommendation.

HEATHER FLANAGAN: Yeah, it's like the last two sentences of the recommendation. Are you talking about that, or something different?

DENISE MICHEL: In the middle of recommendation 27, we have a sentence that starts with "ICANN'S risk management framework." So somewhere in there, perhaps we can just insert "which the team reviewed and found to be comprehensive and appropriate" or something like that.

RUSS HOUSLEY: Does the yellow text belong in the recommendation, or is that part of the finding?

LAURIN WEISSINGER: I asked in a comment if that's a footnote.

RUSS HOUSLEY: Well, just put it in the finding is fine, right? Go ahead.

KERRY-ANN BARRETT: Just with the addition, the paragraph seems to be contradictory. With the edits, it now seems to be contradictory. We're saying that while we have assessed the framework and it seems good, it's not clearly articulated nor aligned strategically. So we just need to pull together to say that we've dug through the mires, and once we dug through and realized that it's there, just scattered, but we think it needs now to come together and be aligned strategically. So I think we need to make the sentence [inaudible] we're saying it's good, but I think the middle part that Denise highlighted, pretty much, it's not centralized, but once we have found it, what we found out there is good, it's just that it's not in one place.

So I think we need to make that – unless that's not the point we're making. IF that's the point we're making right now, the paragraph doesn't say that. It's just saying two different things.

NORM RITCHIE: Yeah, so really it's an odd recommendation because we're basically saying strut your stuff, good job but strut your stuff, which is a really unusual type of recommendation to make. So I don't know if we can phrase that some other way and say along the liens it was painful to do the gather the information and find it was a good job done. Going forward, that should be more coordinated and public.

KERRY-ANN BARRETT: Which is why I was thinking that the middle part needs to be in front, so the middle part should be that ICANN's risk management framework should be centralized strategically, the review team found that what exists in different areas is sufficient but it's just not coordinated to make it a benefit for the organization. Something like –

DENISE MICHEL: And published.

LAURIN WEISSINGER: Are you happier now after Heather and I again had a go at the same time?

KERRY-ANN BARRETT: I would include assess [inaudible] comprehensive and appropriate. However, it needs to be publicly available and show … It needs to be publicly available and in a centralized – that's where it gets more specific as to what we're asking them to do. So where you have "While risk management activities including the DNS as assessed by the team were comprehensive and appropriate …"

LAURIN WEISSINGER: Yeah, we can make this in two sentences.

KERRY-ANN BARRETT: Yeah, this needs to be publicly available and centralized, something something. But that's where you want it. So you don't need to point out it's piecemeal again because you already said it's piecemeal at the top. So it's just to make what we're asking them to do specific.

LAURIN WEISSINGER: I still don't like the language, and I think that needs some beautifying, but I think it says what we want it to say.

RUSS HOUSLEY: I'm not sweating beautified at this point. Do we have an agreement on the concepts of these words?

DENISE MICHEL: I think it’s fine.

RUSS HOUSLEY: Okay. Not hearing anything else, Heather, you want to talk about this big yellow block of text?

HEATHER FLANAGAN: Regarding the suggestion to move the intro for SSR1 general findings up in the document?

RUSS HOUSLEY: Yes.

HEATHER FLANAGAN: I think that makes perfect sense and I will do that. Good overall context before jumping in.

RUSS HOUSLEY: No, it’s really important to say the general finding ... Yeah.

DENISE MICHEL: Let me take the comment off.

HEATHER FLANAGAN: Don’t take the comment off, it’s serving as an action item for me. I'm assuming it’s just the intro text though that moves, not the whole findings.

RUSS HOUSLEY: Correct.

DENISE MICHEL: I just highlighted it so you know which one [inaudible].

HEATHER FLANAGAN: Perfect.

DENISE MICHEL: And the way we’re organizing it is SSR1 recommendations for which we have specific guidance and additional action, and then the block of SSR1 recommendations for which we say “Finish implementing this.” Right? So maybe a note to that effect so the reader can follow how it’s organized. Do we have that ?

HEATHER FLANAGAN: We have that.

DENISE MICHEL: Okay. If you're moving this text, there should be a note before SSR1 recommendation 1 that says the following SSR1 recommendations, we recommend that they be fully implemented. Yeah.

RUSS HOUSLEY: I think that brings us to page 52. In the slide bar, not the numbering.

HEATHER FLANAGAN: You will note the pages are not numbered. There's a reason for that.

RUSS HOUSLEY: Which is Work Stream 2. So the first recommendation in Work Stream 2 is the security position in the [CC.] The bottom of 52, top of 53. Let's see if we can get through Work Stream 2 and then have lunch.

HEATHER FLANAGAN: Part of the challenge we've had with page numbers is, particularly as things have jumped around, I noticed especially on our original document how the page numbers didn't actually align with the real page numbers, so it just got to be a mess. I think someone may have added them manually or something. I don't know what happened, but I just skipped that. If it gets complicated, go to the table of contents and click the link and it'll take you to it.

DENISE MICHEL: I may be misremembering, so I thought we had discussed putting all the discussion of the SSR1 recommendations for which our recommendation is fully implement those, that we would reflect that in an annex so as not to take up so much room in the front of the report. And I am still a fan of that.

RUSS HOUSLEY: I don’t remember that, but I don’t object to it.

DENISE MICHEL: It’s hard to remember what happened BH, before Heather, and I don’t think we've been really comprehensive in updating you on all the things that we have discussed, but I do recall that’s one of them and I'm a fan of saying the rest of the recommendations, we recommend you fully implement them, see Annex 1 for additional information, and park it there.

HEATHER FLANAGAN: I am more than happy to do that.

KERRY-ANN BARRETT: Denise, just to be clear, where we have that entire part we just scrolled through, that entire block will be an annex? But the parts that we’ve been going through this morning will remain and then refer to that annex?

RUSS HOUSLEY: Correct.

KERRY-ANN BARRETT: After the table, the table will say please see ... because the table will stay though. And then after the table, please see annex for further details.

DENISE MICHEL: Yeah.

KERRY-ANN BARRETT: Okay. Agreed.

RUSS HOUSLEY: Okay, somebody highlighted a block of text. I assume they're wanting to talk to us about it. I can't tell who did the highlighting.

LAURIN WEISSINGER: That was me. Following point, we recommend a CSO position – which is great – and then we go into security stuff that hasn’t been mentioned in this recommendation previously. So I'm wondering, is this part of this recommendation? If we want to leave it there, we should probably relate it to this CSO position instead of security stuff.

DENISE MICHEL: Where are you, which recommendation is this?

LAURIN WEISSINGER: On front screen and the yellow part. It’s just a slightly different topic.

KERRY-ANN BARRETT: No, I remember when that got inserted.

LAURIN WEISSINGER: Yeah, but doesn’t matter –

KERRY-ANN BARRETT: No, I remember when that got inserted though, the intent for that part was that when it comes to risk management, there was a call or something, we wanted to make sure that when they talked about risk management, they consulted with internal security staff.

LAURIN WEISSINGER: Yeah, but –

RUSS HOUSLEY: Yeah, but his point is that we’re mixing two things. Either they're separate recommendations, or this is something the CSO should be responsible for.

LAURIN WEISSINGER: Exactly.

DENISE MICHEL: I think it makes sense.

LAURIN WEISSINGER: Should we just do “ICANN Org should consult the CSO or security staff to provide guidelines?” And their staff ...

DENISE MICHEL: Why don’t you just put CSO/Security staff at the beginning of the sentence that you highlighted?

HEATHER FLANAGAN: This might sound like a weird nit. You create a position and you hire a person, so to create and hire sounds very strange to my brain.

KERRY-ANN BARRETT: I've seen many positions created [and they never] [inaudible].

RUSS HOUSLEY: Kerry Ann, can you repeat that for the mic? We have Naveed on the line.

KERRY-ANN BARRETT: I was saying I've seen many times posts are created and they never hire someone. So I think – I've seen it too many times, entire org structures created and no one is ever hired for years.

HEATHER FLANAGAN: No, I get that, it’s just that as Laurin took care of it, you create the position and then you hire for it, but it’s separate.

KERRY-ANN BARRETT: Okay. Agreed.

LAURIN WEISSINGER: Is my edit okay?

RUSS HOUSLEY: Are we done with this one?

KERRY-ANN BARRETT: I have one concern though. So taking into account the nice framework that [inaudible] is it a function that we want to fill or a post? Like a job, or ... What is the – we want someone just at the CSO level, the C-suite level? Is it that if ICANN opts to put this function on their existing role or job that they already have on this structure, do we care?

RUSS HOUSLEY: We had that discussion.

KERRY-ANN BARRETT: Yeah, I remember, but I'm trying to remember what the conclusion was.

RUSS HOUSLEY: We said we don't care whether they reorganize and pick somebody who's already employed to become this, or whether they create the position and then seek a new hire.

KERRY-ANN BARRETT: So under the new implementation, can we make that category – are we keeping that structure that we have below where we put implementation, or no?

RUSS HOUSLEY: Right now, we have a –

KERRY-ANN BARRETT: We don't know yet?

RUSS HOUSLEY: We don't have the same structure in the various parts, we're just now trying to focus on the recommendation text so that we can brief that. But Heather clearly wants to correct me.

HEATHER FLANAGAN: I don't want to correct you, I just want to clarify a little bit. Part of the reason I left that outline there was I think those are very important points that we needed to make sure were reflected in the recommendations. So if we go to this and say, alright, there's the recommendation, do we know how to implement that? Do we know what the measures are? Do we know what the impact is expected to be? We have to be able to answer those things. We don't necessarily have to have them blocked out that way.

KERRY-ANN BARRETT: I can tell you, when I'm reading it – and this is our last read of this for now- the sentence that follows I think is the punch that we need to come before a suggestion to create a position. That's the point I think I wanted to make clearly. So where the sentence says the review team considers it necessary to have an officer at the level of C-suite to coordinate security, da da, I think that is the punch.

RUSS HOUSLEY: Move that to the front.

KERRY-ANN BARRETT: Move that to the front. [I don't want them to get caught up] with us thinking that we needed to hire a CSO. No, we needed to have someone at suite level with this function. If you want to call it a CSO, [a BSO,] whatever you wanted to call it, that is ... So I just think, what is our [inaudible]

LAURIN WEISSINGER: I know I'm a terrible pain in the back of everyone. Last sentence, I am not clear what this sentence does. So I'm saying either we cut it or we edit it.

RUSS HOUSLEY: It's pointing back to the sentence that we just reworded completely, because this consultation is about the – as part of risk management, ICANN should consult ...

LAURIN WEISSINGER: I'm talking about that one.

RUSS HOUSLEY: That's the consultation. Norm, you wanted to say something.

NORM RITCHIE: [inaudible]

LAURIN WEISSINGER: I will just not come back after lunch. Sit by the pool.

RUSS HOUSLEY: I'm fine with deleting the sentence personally.

DENISE MICHEL: I like the sentence. And I'm happy to hear or think about clarifying it if you feel that it's not clear, but fundamentally, staff with security expertise and responsibilities don't have a seat at the table or even regularized input to the closed-door negotiations between Legal and contracted parties staff and the contracted parties. And as a result, you don't have the security expertise and knowledge to factor into the negotiations on what the contracts are going to say, and we've identified so many challenges that flow from a lack of clarity and really a lack of contracts even addressing some of the most critical security-related issues.

LAURIN WEISSINGER: Denise, I like completely agree. I just don't see how that sentence actually say that.

RUSS HOUSLEY: [Exaclty.]

LAURIN WEISSINGER: Let me provide an example. It's in blue, but I will need a minute to write it.

KERRY-ANN BARRETT: While Laurin writes, can we just reinstate "the equivalent of" given that we did the change with the paragraph? Because I think then everything makes sense after that, so we're not prescribing what it should be.

ALAIN AINA: I'm just wondering if we should be going down the line, because I think by saying that ICANN should have a CSO to be responsible for both strategy and tactical security, I think that for me seems to be enough. We don't need to really specify that they have to be involved in reviewing contract. So I think I don't feel comfortable giving this kind of detail.

So if a company has a CSO, then the CSO – the job description must be done internally and cover – so I'm not very comfortable saying that [inaudible] guideline for [all] negotiation for ICANN contract. So it looks like we're giving too much detail.

KERRY-ANN BARRETT: I get the point of being prescriptive with the job function, but I think what we had wanted to reflect when we had spoken about this was the disconnect as Denise described it from the security issues informing the contract. So it's however we can capture that, that function would kind of be that bridge between the person who is head of legal and the ahead of understanding what security issues [inaudible] to figure out how to let the two speak.

So the issue we found is that the negotiations are going on in one shop, and the knowledge that's needed to make sure that the contracts are tight enough that when Compliance now comes in, Compliance has the tools to be able to correct or issue corrections requests. And you're correct, prescribing that it has to be a job function, maybe not, but prescribing that the two functions need to speak, legal and security, that's what we wanted to hit.

If this is not the place, maybe we need – because we're creating a post here, so if this is not the place, maybe we need to figure out where to stick that. Probably under Compliance or something else. I don't know.

DENISE MICHEL: I agree with most of what you said. I think if it's one thing that I think we should take away from the last couple of years of due diligence is that without some degree of direction and specificity, implementation doesn’t seem to occur. And particularly given all the work we've done relating to abuse mitigation and compliance, I feel pretty strongly that we've struck a good balance on recommending the role, providing some general guidance. I could write another two pages on different activities this person should do, but I feel comfortable with the level of specificity that we have, and I think it’s really important to highlight the role in contract negotiations as well. Thanks.

RUSS HOUSLEY: Laurin, you're not ready to share text yet? You keep saying you're going to and then I see Laurin’s popping up all over the place.

LAURIN WEISSINGER: I am ready now. So one of the things we could do, I think, is what is marked as blue by me right now just gets replaced with the blue text at the bottom.

NORM RITCHIE: There's different parts of our recommendations that'll point towards the existence of a CSO, or the desire for it. So I think we’re going to probably have pointers to this one from other areas, and vice versa, are we going to take this one and point back to the others? If we’re doing that, we shouldn’t just put one point down, we should put them all. We just [inaudible] one item here and said, ”Let’s specify this” and not looked at the others. So I think we’re going to have to come back and review this one later.

LAURIN WEISSINGER: I agree we have to do that, but as we're currently talking about that bit of text, do we want to agree on that right now? At least preliminarily. So as I said, I think what I marked now could be replaced by the much shorter, like three lines below that are in blue, if everyone's happy with that.

DENISE MICHEL: I think it's fine, it's a preliminary.

RUSS HOUSLEY: It's fine except for what security function means, because we talk about security staff in what would become the sentence before. [After your delete,] "The position should oversee interactions of security staff in all relevant areas." Right? So, is the security function the staff, or is it the CSO's office?

HEATHER FLANAGAN: I think what was in your ahead is the security function as described, so that CSO role. To Norm's point about creating those bullet points of what we're crosslinking, I've made a note to myself to follow up on that and do that.

LAURIN WEISSINGER: I think there will also be a lot of [inaudible] on what the security function actually is. And this is, I don't think, something we should put too much detail in. We do not have the visibility of what in Org could fall under that and how it should be organized.

RUSS HOUSLEY: I think, to make it flow with the rest of the text, what you want to say instead of the security function is “This position.”

LAURIN WEISSINGER: Yes, this’ll be the head of the security function. Okay.

DENISE MICHEL: Sorry to extend this, but I thought we were talking about a chief security officer, which is different than a chief information security officer. My understanding, interpretation, and please correct me if you have different, CSO to me connotes an inward-looking ICANN Org’s own information systems and the security of those.

We’re talking about security as it intersects with ICANN’s Bylaw-mandated responsibilities. So the CSO in here doesn’t seem to fit for me.

KERRY-ANN BARRETT: That was a concern I had, because we mentioned both. We said the equivalent of a CISO or a CSO. So [that’s why in terms of it] gets lost as to what's the function that we want them to address, not necessarily the title of the position we want them to address. To me, there's a distinction.

RUSS HOUSLEY: Probably both.

KERRY-ANN BARRETT: Probably both, but if it's both, we need to say that, [but] we say "or." So how that's defined, sometimes depends on organization. Each organization uses the term sometimes interchangeably. For some, all the functions are subsumed [under another.] So [when I thought about mentioned the NICE framework from the US] is because it speaks to roles and functions rather than job titles. So if it's a function we want to address, we should describe the f unction as you said rather than tell them it has to be a CISO or CSO. Whatever we want them to call it, we already said C-level, so we want it to be at the executive level with these functions, someone who sits at the table at that level with these functions. So we need to specify.

RUSS HOUSLEY: My memory is that we started to have this argument and Scott said, "Well, I'll just put the 'or' in there." And we moved on.

DENISE MICHEL: May I suggest that Laurin, Kerry Ann and I just confer at lunch, come up with some text and that we come back to it? Is that okay, or do you want to just keep ...

LAURIN WEISSINGER: So I think we can do this in different ways. I made a proposal how to do the bottom [bit] of this recommendation. I hope that's okay. A question to Heather. Why did you delete the "At the C-suite level?"

KERRY-ANN BARRETT: We didn't delete it, it's moved.

LAURIN WEISSINGER: Okay. It looks like it's deleted. I'm sorry. Yes, okay. Happy to go with Denise's approach.

RUSS HOUSLEY: I'm actually even fine with deleting those words because the first stance says it. Hire or appoint a responsible.

KERRY-ANN BARRETT: Hire somebody [inaudible]. To me, that was the punch line and we've already stated it. So to describe the specific title of that person to me doesn't add value.

RUSS HOUSLEY: Yeah, giving it a name doesn't change what we're recommending.

KERRY-ANN BARRETT: The point we're making is have somebody at the C-suite level create a post and hire the person. That's the point, doing these functions. Call them John Doe, Jack [inaudible] whatever.

RUSS HOUSLEY: Okay, so I think we're moving to page 54. Laurin's through typing, right? Laurin, stop typing. Okay.

DENISE MICHEL: I was, I'm just making a note that we're going to update that text and come back to it.

RUSS HOUSLEY: Alright. Risk management. Seems to me a lot of the things we said right here, we already said previously, so I'm wondering whether we should grab that previous risk management text and just make one recommendation out of the two.

DENISE MICHEL: I think that the distinction here is in my mind was the first one is addressing broadly the approach to the risk management framework. This zeroes in on – and I think is important in that it calls out the adoption, implementation of the ISO 3100 risk management.

So, are you asking if this should be part of the other one?

RUSS HOUSLEY: I don't care which one moves, I was just thinking if you thought the – put it all in one place, which is what the other one says, and it should include these things. Makes a coherent al in one place recommendation. That's all.

HEATHER FLANAGAN: I think you're talking about merging this and the SSR1 recommendation 9?

RUSS HOUSLEY: Yes.

HEATHER FLANAGAN: Okay. As you like, but I would then question, are you still expanding upon SSR1 here, or is this a new SSR2 recommendation? Because that directs which way you go.

RUSS HOUSLEY: The answer is yes, but –

KERRY-ANN BARRETT: No, I don’t agree with [merging it.]

RUSS HOUSLEY: Okay, people disagree. I'm fine with that.

KERRY-ANN BARRETT: Yeah, because I think [inaudible] flagging, no. I think I wouldn’t want to mix apples with pears, like finish up with SSR1 and then this is a whole standalone here.

RUSS HOUSLEY: Okay, we'll leave it alone. You've shouted me down. All of you. Zarko.

ZARKO KECIC: That's what's confusing me. We have SSR1 recommendations which is saying something, and we have our own recommendation talking about same thing, and suggestions, again talking about same thing, and it is confusing me and I believe it will confuse people who will read this.

RUSS HOUSLEY: Denise?

DENISE MICHEL: Yeah, I think if we're going to have a section that provides additional guidance on implementation of SSR1 when there's a recommendation that clearly aligns with the intention of an SSR1 recommendation, that we should combine them. We continue to look for ways to streamline this report. I think that's one of them. SSR1 not only addressed risk management but it also directed ICANN to adopt an appropriate ISO-type system. So it's also in line with that.

So I would be up to looking at how to combine these, and then I would also suggest deleting the third bullet because we'll be addressing that CSO-CISO position I think up above. Is that correct?

KERRY-ANN BARRETT: Just to follow up on Zarko's point, in that context, I think I agree, but I wouldn't necessarily – I think as Denise probably described it putting it as the follow-on to the recommendation, I would support not tacking it on to the SSR1 application. But where we have the section that says to do these things, consider these things as well, I agree with Zarko that it would be confusing. But at the end when we are doing the report, we'll be doing cross-references and correlation as well, correct?

DENISE MICHEL: So one way to handle this would be to leave them as two separate things, but to say for considerable expansion upon this, see security risk management.

KERRY-ANN BARRETT: [And then you can read everything related.] Because I think the distinction that Denise made when she elaborated was the tacking it on under the SSR1 at the top, or in that extra section that we're creating, the extra section I agree it could move to there.

RUSS HOUSLEY: [inaudible].

KERRY-ANN BARRETT: What were you thinking?

RUSS HOUSLEY: I can live it the way it is, but I was not thinking it would get tucked into the appendix.

KERRY-ANN BARRETT: No. [inaudible].

RUSS HOUSLEY: Okay. I was thinking that this could move to the SSR1 recommendation 9 section that says put it all in one place and then, “And it should include …” I'm fine, but you didn't like the idea, we’re moving on.

DENISE MICHEL: I think it’s fine [here.]

RUSS HOUSLEY: Okay, and we’re going to turn the third bullet into a pointer in the previous one, right? Okay. Anything else we want to do here? I think the last bullet is actually already said in the previous recommendation, so I don’t think we need it here. And these two things become pretty straight forward.

KERRY-ANN BARRETT: Just a question, Russ, [on the] consistency. When we had the [27000] recommendations, we were bellyaching over whether it should lead to certification or not. For this, are we sufficiently happy with them just looking at it as a best practice to implement for risk management, or do we want them to ensure that it's established – Yeah, and validate appropriate –

RUSS HOUSLEY: It says you have to audit it.

KERRY-ANN BARRETT: [It just says validation.] It's not specific, it's not very clear to me.

DENISE MICHEL: Yeah, perhaps it does need to be clarified, and this wasn't my recommendation, but in recalling the conversations that we had on this, particularly driven by Scott and some prior team members, they felt very strongly that ICANN needed to officially adopt and comply with the appropriate ISO standards and that it be audited. So perhaps we need to clarify that language, and it would be good to check in with Scott on this.

LAURIN WEISSINGER: I just added "Validate and certify implementation with appropriate independent audits." If people are happy with that. Steve, do you think you can work with that? Just to make sure, because we're very specific here with the risk management, not necessarily the rest.

STEVE CONTE: As part of our previous conversation on this, it sounds like I might have missed during my absence a conversation that the review team might have had with E and IT, engineering and IT, because they're the ones who would be looking at adoption and implementation of these. So if they've expressed that this is the path that they acknowledge that they want to go down, then the wording is fine. I don't know, I wasn't involved in those conversations.

As far as the specificity of it, again, the first time we all met in LA. It sounded like the E and IT was adopting various – and I don't say it in a loose way, but various certifications and various – like NIST at the time and stuff like that. So they were taking pieces depending on the relevance of the item that they were working on. So I think some of the external functions that they did were falling under a different certification than ISO and things like that, so if NITS – if this is the way that they're going and they've expressed that, I'm fine. If not, then my recommendation, maybe have a discussion with E and IT prior to publication on this to make sure that they're aligned with this path as well.

LAURIN WEISSINGER: Okay. I personally don't see a problem to say, use of an equivalent is fine. I'm not aware of any exact equivalent of this though.

STEVE CONTE: I'm not either.

LAURIN WEISSINGER: So that’s my problem here. I don’t have a problem to be more open, it’s just I wouldn’t know what else to put.

DENISE MICHEL: I would have a problem being more open. They were very open in SSR1. At the subteam meeting in LA, we had several information security experts around the table. They were stunned at some of the information security lapses that were discussed. And from that came a very prolonged conversation about being specific and how useful the specificity would be.

So perhaps we should flag this and take this up when Scott and some other people who created this are at the table, maybe.

LAURIN WEISSINGER: I was involved in that. So essentially, the problem is for some standards, you can say, “Oh, you can do that one, you can do another one,” and there's a list of ones you can choose from, which I have no problem with. That’s what I'm trying to say here. I just don’t know which other option we can provide.

RUSS HOUSLEY: For the risk management, I understand that, but then we talk about the 27000 family, and ...

LAURIN WEISSINGER: [inaudible].

RUSS HOUSLEY: Yeah.

LAURIN WEISSINGER: And this is the thing we might want to think about if we want to do that, put in brackets, okay, say, after 27000, we can say “Or these alternatives,” colon. With [BC,] again, it’s a bit more tricky to find a good replacement.

RUSS HOUSLEY: Yeah. Okay.

LAURIN WEISSINGER: We might want to consult with IT function again. Tell them, “Look, this is what we want to do.”

KERRY-ANN BARRETT: Before making this one public.

LAURIN WEISSINGER: Before kind of going full public with this and say, “Do you have something else in mind? If you do, okay, we’ll have a look at it. If not, do these.” Because maybe they're using something we’re not aware of.

DENISE MICHEL: Steve, could you perhaps take an action item to contact your colleagues and find out what they're – if they're implementing, if they're complying with anything new? And if they have thoughts on the ones that are specifically recommended. And I wouldn't be supportive of removing this. It's been in here for a long time and came out of a fair amount of due diligence. And the purpose of floating these draft recommendations this week is to get input and then to change them if we feel that that's warranted.

LAURIN WEISSINGER: So yeah, I'm not for removing this. All I'm saying is if they're doing something already that is relevant, we might want to include that specific thing. it doesn't really change the rest. Just tying them down to something that they might have replaced by something equally useful could be a problem.

RUSS HOUSLEY: We already talk and give flexibility regarding the ISMS in the earlier recommendation. Here, we're nailing them down to the 27000. That seems wrong. The next recommendation is about business continuity. So I don't even know why that's raised here. So if we were to narrow this recommendation to the ISO 31000, to follow that, validate and certify and audit, that works great. And then I don't think we have the problem that we've been discussing now fort 20 minutes.

LAURIN WEISSINGER: Great point. Happy to go with that. Where do we move the other two? [inaudible].

RUSS HOUSLEY: We already have the 27000 in the SSR1 follow-on.

LAURIN WEISSINGER: Yes, but 22301.

RUSS HOUSLEY: 22 should be in the next recommendation, which his about disaster recovery and planning.

LAURIN WEISSINGER: Okay.

RUSS HOUSLEY: I'm now happy. Are others?

DENISE MICHEL: [inaudible].

RUSS HOUSLEY: Good luck. He hasn’t answered an e-mail from me in months. Boban is on his way. He’ll be here after lunch.

DENISE MICHEL: Okay. [inaudible].

RUSS HOUSLEY: Right, can we get through the disaster recovery planning before lunch? So Laurin, you're going to insert the 22301 here somewhere. Why don't we just say outside North America? Yeah. Sure.

DENISE MICHEL: Yeah, at which point we don't need to specify what [inaudible].

RUSS HOUSLEY: All those places that might be outside North America. You're worried about a sharpie?

LAURIN WEISSINGER: Just noting, I am totally happy to remove the i.e. The United States and North America had a specific reason, because North America is geographic in nature and the U.S. has to do with the legal system and the country per se. That is why they're both in, because there are different types of risks associated with each one.

RUSS HOUSLEY: But if it's outside North America, it is also ...

LAURIN WEISSINGER: It is covered, I agree. I'm just saying there is a reason why we did this.

RUSS HOUSLEY: [inaudible].

LAURIN WEISSINGER: Exactly, that is the point. So you could put it somewhere else that still falls under U.S. territory.

RUSS HOUSLEY: OKAY.

LAURIN WEISSINGER: So I suggest we just say United States territory.

KERRY-ANN BARRETT: Legally correct, United States and its territories.

RUSS HOUSLEY: Going once, going twice. Go, Steve.

STEVE CONTE: I'm just reading the first paragraph and you're calling out RSSAC and the root server operators. Is this disaster recovery plan – oh, it’s related to IANA. Okay, sorry. I wasn’t putting all the pieces together at that moment.

LAURIN WEISSINGER: Steve, would you propose to include SSAC as well or something? Is that where you're coming from?

STEVE CONTE: No. I was curious of why RSSAC was being invoked, but because I didn't draw the connection back to IANA at the time.

KERRY-ANN BARRETT: I was just wondering, it starts off by saying that there is an existing DR plan. That's what we're assuming; correct?

LAURIN WEISSINGER: Yeah.

KERRY-ANN BARRETT: Would we be doing a cross reference to where this DR plan is located? It starts off with "the DR plan." So it means that there is a plan somewhere. If it's not public, there needs to be a footnote about it because it starts off with "the DR." So it seems like –

RUSS HOUSLEY: But the second paragraph makes me think there's not one, or at least not a public one.

ZARKO KECIC: Yeah, the meeting in LA we had in October 2017 two years ago. Yeah, we talked about business continuity and disaster recovery plans, and [all answers] that we got is that ICANN and IANA systems are active active, fully redundant, and they're in multiple locations and that's it.

So I'm not sure, maybe Steve can help with that, I'm not sure that there is – actually, we didn't see and we didn't hear about disaster recovery and business continuity plans, but everything is based on active active and redundancy.

KERRY-ANN BARRETT: [inaudible] it's just that how the sentence starts, it should ensure that the DR plan includes, so it means it assumes that there is a plan, and we're now asking them to include these things. So if it doesn't exist, we should stat off by saying that we should ensure that there is an established DR plan that should include bla bla. The sentence is misleading.

RUSS HOUSLEY: So I think you're saying take the first sentence of the second paragraph, pull it to the front and say ICANN Org should develop ...

KERRY-ANN BARRETT: [inaudible] after, yeah, if ...

LAURIN WEISSINGER: Last comment before lunch, hopefully. We should make a note, check, we're currently only talking about disaster recovery specifically for IANA functions. Question is, what about everything else? We should check the relevant board communications and see if we did this because of that or if there are other reasons why we exclude everything else.

RUSS HOUSLEY: I guess the question is – I don't recall this – were we purposely saying let's just focus on this and leave it to a subsequent team to expand?

ZARKO KECIC: It depends on what level. And if you're talking about disaster recovery and level of ICANN Org and operations that ICANN Org are doing and overseeing, it should cover everything, not only IANA function. Or we can put key services, but that's just not good idea.

KERRY-ANN BARRETT: Just because we've moved the sentence just to make sure it starts off and it's specific, right now it's not, it just says ICANN should have an implementation plan, [basically] that we want ICANN to have a disaster recovery plan and clear measures for its implementation or something like that, but it's not very specific right now.

RUSS HOUSLEY: No, I think what we were calling for was after the board approves, they have 12 months to put the plan together.

KERRY-ANN BARRETT: Implement it within 12 months?

STEVE CONTE: It goes back to what was just said, that the first paragraph then reads that ICANN should have a disaster recovery plan. The second paragraph goes to explicitly the disaster recovery plan for PTI, and there's no connection between those two. So, are we talking about ICANN Org having a disaster recovery plan, or are we talking about PTI? Specifically the IANA function having a DR plan.

RUSS HOUSLEY: I thought Zarko just addressed that a minute ago and said both.

KERRY-ANN BARRETT: [inaudible].

RUSS HOUSLEY: Right.

LAURIN WEISSINGER: I just put in brackets essentially ICANN Org should establish their plan for their own systems, again based on ISO 22301. Does that make sense? We should consider if we want to put it in or not. Sorry, Russ, didn't hear that .

RUSS HOUSLEY: That’s already imposed on the IANA in one of the previous paragraphs.

LAURIN WEISSINGER: There is a difference between IANA and ICANN Org.

RUSS HOUSLEY: I understand. All [we're] trying to do is apply that same level of specificity to both. Okay. Thank you.

LAURIN WEISSINGER: And there are other issues, right? So the disaster recovery would include the operators while ICANN Org systems that only they own is a different deal.

HEATHER FLANAGAN: So it should be ICANN Org should also establish?

KERRY-ANN BARRETT: [inaudible].

RUSS HOUSLEY: Yeah. Anything else? Yes?

KERRY-ANN BARRETT: [It says, should publish evidence.] I know different writers have been writing. What is evidence? Is it a report, a website?

LAURIN WEISSINGER: It says ...

KERRY-ANN BARRETT: It says example, but a summary doesn't still tell me if it's a report. A summary could be one page or two sentences. A summary of what? A summary of its report on this? So the example doesn't clarify what the evidence is. Is it that we want them to publish a summary of the audit results above?

RUSS HOUSLEY: The auditors won't let you do that.

KERRY-ANN BARRETT: Right, so I'm just saying, what is it? It says show evidence. Evidence for me would be the audit results. And is it a summary of the audit results? Well, no. What is the evidence? The clarification doesn't help, if I had to implement it. I'm just looking at it as a point blank. I wouldn't know what you want me to I would just publish a sentence to say I did it.

RUSS HOUSLEY: So, what do you want?

KERRY-ANN BARRETT: I don't know what was intended. That's why I'm saying, there have been different authors. I don't know what evidence, what were we looking for when we said evidence. This is just an outsider looking in.

RUSS HOUSLEY: What we have done with IANA and the protocol parameters registries is when thy do their audit, they send a summary of that to a group of nine people to review, but the auditors will not let them make it public. So I think evidence is kind of probably the best we're going to get.

NORM RITCHIE: To what you just said, Russ, would the last line in that paragraph on the next page inform the first line on that paragraph? Would that be sufficient enough for the team?

RUSS HOUSLEY: Works for me.

KERRY-ANN BARRETT: [inaudible] ICANN should to improve transparency and worthiness, bla bla, and then going to getting an external auditor. I don't know. But I know Zarko was trying to ...

ZARKO KECIC: Yeah, I would like to address something else. I believe this is mixing two different things. Business continuity management and disaster recovery are connected, but they are not the same thing. And I believe that we should cover business continuity as well in a separate part and keep disaster recovery what it is.

RUSS HOUSLEY: So you're just asking that the first sentence be expanded to include both, or something more?

ZARKO KECIC: I would rather have another recommendation talking about business continuity. We can add them up because risk management, because and disaster recovery are interconnected, but they are separate things. [We should do] what I'm thinking, without risk assessment you cannot do good business continuity plan, and when you have business continuity plan, you figure out what key roles and key services are so you can recover them in certain period of time. So either to make recommendation this way or to have three different, but we need risk management, business continuity and disaster recovery as separate things.

LAURIN WEISSINGER: Agree.

RUSS HOUSLEY: That adds a recommendation to this section, right? it basically breaks apart the DR and the CM, that's the plan?

ZARKO KECIC: it would.

KERRY-ANN BARRETT: But I think the logic flow is what – Heather, I don't know if you'll be able to write it, I think it's the logic flow if I'm not wrong that Zarko is speaking of. One is embedded ad nested into the other in order for any of them to be effective as a whole. So everything is contained, I think, in the recommendation, but it's to ensure that the logic flow is incldued as well.

HEATHER FLANAGAN: [inaudible] I'll be able to write for you.

KERRY-ANN BARRETT: We will have to do it.

RUSS HOUSLEY: Yeah, it should all flow from the risk management in the previous section, right? So the three are bundled together in that.

LAURIN WEISSINGER: How long is the lunch break?

RUSS HOUSLEY: Alright, let's eat and maybe a team can figure out how to pull the continuity management part after they get some sustenance.

NEGAR FARZINNIA: Russ, are we breaking for an hour? I need to put a note in the Zoom room for [inaudible].

RUSS HOUSLEY: Why don't we try and do this in 45 minutes? At the pace we're going, we're going to need the time.

KERRY-ANN BARRETT: You deleted the last one?

LAURIN WEISSINGER: No, I copied.

KERRY-ANN BARRETT: [inaudible].

RUSS HOUSLEY: Okay, this is the three-minute warning. We're going to start in three minutes.

NEGAR FARZINNIA: Russ, are you ready to get started?

RUSS HOUSLEY: We are. We are resuming. Okay, where's Laurin? He ran out of the room.

DENISE MICHEL: No, he's back there.

LAURIN WEISSINGER: I have fled the room.

NORM RITCHIE: I was going to say now is your chance to move on without edits.

RUSS HOUSLEY: Okay, so before the break, we had a section on risk management and a section on disaster recovery which actually talked about disaster recovery and continuity management. We now have three sections that flow security management, continuity management, disaster recovery.

And I think that right before, it looks like Laurin put his last edits in. So please take a look at those three sections, how they fit together to give a consistent message, and let's start with the security risk management section. I think it now hangs together as a flow. That would be on page 54. I don't know if Ram's still with us.

NEGAR FARZINNIA: No.

RUSS HOUSLEY: Okay. Any concerns with the risk management? Alright, moving on to the new continuity management words. Any concerns here? The whole text is blue.

KERRY-ANN BARRETT: So now we move the paragraph around, so we say they should establish of IANA for the PTI operations, and then for all systems owned under the previous – are there two different recommendations unrelated?

RUSS HOUSLEY: The way I read it, we're saying develop one for IANA, develop one for your own systems. It's a two-part and then have them both audited.

KERRY-ANN BARRETT: Okay. Is there any way to restructure it?

RUSS HOUSLEY: You want to make it six recommendations?

KERRY-ANN BARRETT: No.

RUSS HOUSLEY: Please no. Good.

LAURIN WEISSINGER: I just noticed we should put both in to make sure it's clear it's both points.

RUSS HOUSLEY: What are you talking about both?

LAURIN WEISSINGER: Because there are two different plans.

RUSS HOUSLEY: Yes.

LAURIN WEISSINGER: So I just added both.

STEVE CONTE: Laurin, just to confirm that or to talk about that, there might actually be more than two plans, because if we look at IMRS, L-root services, that might have a completely separate continuity plan. So I would avoid both and you have, like you're saying, these or – there's a minimum of two.

LAURIN WEISSINGER: Yeah, that’s true. So both alone doesn’t work, like its related to both these points.

RUSS HOUSLEY: But an S after “plan.”

KERRY-ANN BARRETT: No, so Steve, just to be clear then, should it be, “Should establish a business continuity for each of“ instead of “all of?” Since it could be a different plan for each of the systems. It could be one master – is that what we’re saying, to have one master plan for all the systems or have a business continuity for each of the systems owned by them? Because [inaudible] they may have several. I don’t want them to try and just do like one general brush. Does that make sense? So instead of “all,” put “each.”

NORM RITCHIE: [Can we just delete the word?]

KERRY-ANN BARRETT: Which one of the words?

NORM RITCHIE: I would actually follow Russ’ example there because “each” kind of implies that there’ll be a separate plan for every system. I hear what you're saying with intent, but I think if we just say for the system’s own, just like Russ mentioned, I agree with that.

LAURIN WEISSINGER: Yeah.

KERRY-ANN BARRETT: Thank you.

LAURIN WEISSINGER: So you usually have an overarching thing and then you have specifics.

KERRY-ANN BARRETT: The [subsets.]

LAURIN WEISSINGER: And the “both” I put in was kind of more related to IANA and the systems owned, not if there are multiple documents.

KERRY-ANN BARRETT: So just leave it as is.

LAURIN WEISSINGER: Yeah.

UNIDENTIFIED MALE: It’s fixed.

RUSS HOUSLEY: Okay, are we happy with the business continuity part? Disaster recovery.

LAURIN WEISSINGER: I just added the name of 27031. That was ISO site, that wasn’t me.

RUSS HOUSLEY: Okay, Zarko, you asked for these changes. Are you satisfied?

ZARKO KECIC: I'm just reading business continuity management, and first paragraph is talking about business continuity plan for PTI operations. I cannot find correct wording, but PTI, it is important to have disaster recovery for PTI. Business continuity should be for whole entire ICANN Org and all organizations attached to it.

RUSS HOUSLEY: That’s the next paragraph. We decided because DR says IANA and then all ICANN, they did the same here. You're saying merge them?

ZARKO KECIC: I'm saying we don’t need IANA function over here for business continuity. Steve, IANA and ICANN share offices, am I right?

STEVE CONTE: In its current state, yes, you are right.

ZARKO KECIC: So I would propose to remove IANA from business continuity.

RUSS HOUSLEY: Does anyone want to argue against? [Go ahead.] You're thinking about it.

NORM RITCHIE: So what if PTI and the rest of ICANN separated physically? Would then the same still apply?

ZARKO KECIC: It depends who is managing all that stuff. If it is under the same management – and it doesn't matter of physical location of people but who is managing all that stuff, because business continuity is planning from where will people work if some disaster happened, fire or earthquake or whatever. So that plan applies to IANA, to ICANN Org, to all other organizations which are under same management.

LAURIN WEISSINGER: Yes. I don't disagree with that in practice, but the question is, will this stay exactly the same as it is right now? And there is this kind of coordination issue that has to do with RSSAC and root server operators which we don't have for the other systems because they're not involved. I think that's why we broke it up. So I'm wondering how we would do this, because the disaster recovery and the business continuity in terms of [– you do this] according to the standards we're putting in here, intersect, interact, whatever you want to call it.

ZARKO KECIC: Yeah, agree, they interact, but for disaster recovery, both business continuity and disaster recovery will manage similar things. But when you talk about business continuity, you're talking about day-to-day operations of something. Disaster recovery says that if you have IANA function, you have to recover that in certain amount of time from the systems and offices which are located somewhere, which is described in business continuity plan.

So they interact, but disaster recovery talks about how fast should critical operations be recovered.

LAURIN WEISSINGER: Yes, so I'm just wondering what's your specific problem with not having this BC plan for the PTI operations. I understand you're saying they're housed in the same building, but it involves parties that are not in that building for example.

So in terms of continuity, having multiple nodes involved is relevant, which is not relevant for the other systems owned or under purview of ICANN Org.

ZARKO KECIC: Again, I wouldn't mix disaster recovery and business continuity. Business continuity is higher level than disaster recovery. So in that case, talking about PTI, there should be a disaster recovery plan for PTI. So we should think about systems, people who are involved in that, what if something happened to those people? who will continue?

LAURIN WEISSINGER: Now I'm confused. I do not understand anymore what you want to remove.

KERRY-ANN BARRETT: I understand what Zarko is saying. I think if that's the case, what Zarko wants is that if it is that you do the business continuity plan, we don't need to specify in the first sentence the IANA functions and PTI because it would be part of all the relevant systems generally, and then the specific recovery plan, the [inaudible] system that we want to ensure that the uptime is like this, the downtime is minimized, it needs to have a specific reference to disaster recovery.

So if that’s the case, I'm wondering, do we need both sentences then for business continuity? Since as a part of it, we already say it’s for all systems under the purview of ICANN Org that we want the business continuity plan. So we may not need both, just the second one. That’s what I understood, and there's a logic to it. It makes sense.

LAURIN WEISSINGER: I understand now. However, PTI operations, all systems [relevant to contributing to] security, stability of the DNS and root zone management – that’s the sentence – not all of the relevant things are specifically under ICANN’s purview.

KERRY-ANN BARRETT: So?

LAURIN WEISSINGER: Which means that the business continuity plan is different because it doesn’t just involve ICANN systems but other parties.

ZARKO KECIC: That's part of disaster recovery, not about business continuity. Verisign is managing root zone, and you cannot write business continuity plan which will cover Verisign. Verisign should have their own business continuity plan and should be part of disaster recovery plan of IANA in regard of root zone management.

LAURIN WEISSINGER: Yeah, I can see where you're coming from, and I think we need to rephrase it. I do not think completely removing it would be appropriate though.

UNIDENTIFIED MALE: Let's move on.

LAURIN WEISSINGER: Yeah, let's think about how we could do this.

RUSS HOUSLEY: Okay, the other lunchtime discussion we were going to have was regarding the C-suite. The title, there was a suggestion we just remove it and let the first sentence, the C-suite level sentence, do this, and then there was another suggestion that we leave the CSO-CISO alone and leave it in there. So, did that during lunch conversation happen? Yes.

KERRY-ANN BARRETT: Laurin suggested using the term instead of – we could keep the two descriptions, [inaudible] fulfilling the function of a [CSO or a CISO.] And I think that would fix the pain for all of us, "Fulfilling the function of."

RUSS HOUSLEY: So he didn't type it.

KERRY-ANN BARRETT: He didn't type it yet because we needed to make sure –

LAURIN WEISSINGER: I did.

KERRY-ANN BARRETT: It's not there though.

LAURIN WEISSINGER: Yes, it is.

RUSS HOUSLEY: Oh, he said, would have the responsibilities of a ... Okay.

KERRY-ANN BARRETT: No, fulfilling the responsibilities is what you told me.

LAURIN WEISSINGER: Yes, that is what I have.

KERRY-ANN BARRETT: That's not what you have. It says, "This would have the responsibilities of ..."

LAURIN WEISSINGER: Would have, yeah.

KERRY-ANN BARRETT: That's different. This position would fulfill ...

LAURIN WEISSINGER: Would fulfill. Yeah, sorry.

KERRY-ANN BARRETT: He's like, "No, that's what I have, fulfilled."

LAURIN WEISSINGER: As I always say, someone else can do all this.

RUSS HOUSLEY: Okay, so it has "and," so inward-facing and outward–facing, which I think is the comment that got us here, and saying both. Any concerns with this approach? Hearing none, moving on.

Okay, page 57, the abuse and compliance section.

ZARKO KECIC: I have one concern and question over here, and I wrote a little bit about that in an e-mail a month ago. I don't believe that we can order doing anything in a certain amount of time. We're a review team and we should just find out what is a security threat, and definitely, abuse should be addressed by ICANN, but saying that community [inaudible] abuse definition, action based on current community [inaudible] abuse, without delay but not later than 2020.

That's something that board and ICANN should decide when and how.

RUSS HOUSLEY: If I remember the discussion on this, it was they've been told this by two other review teams. We're just trying to say, "Get on with it."

ZARKO KECIC: Yeah, but those are recommendations they can accept or not, and that's up to them. It's similar to risk management. You get risk and you decide if you're going to mitigate that and to do something, or to just accept risk and do nothing. So same thing is with recommendations. If it is very hard to implement or you have some other obstacles, like legal or community approach to that stuff, that's very difficult to know how it is going to be addressed.

I would rather here put wording that abuse is really important and that ICANN and ICANN board and ICANN community should work on it, and as soon as possible, try to mitigate [inaudible] so it is as soon as possible. It depends.

RUSS HOUSLEY: There was a whole subteam that worked on this. One of them should defend it. Or ... No later than 2020? So, are you happy with the "without delay" part? Yeah? Okay. Kerry Ann.

KERRY-ANN BARRETT: I think reading the doc that the first sentence again is a bit sensationalized by using overhaul, like someone sees that overhaul means like completely [dig through it throughout] and start again. So, is it that we want them to revisit their approach, or is it that we want them to revisit the definitions that they use? Is it that we want them to examine all the definitions across the board and then ... Overhauling makes it seems as if there's an existing system that we want them to reexamine and do a new one. So I don't think overhaul is – that's the first sentence, and the first sentence is what they'll grab as a highlight.

NORM RITCHIE: [So we turn heads.]

KERRY-ANN BARRETT: Yeah, so is it overhaul that we want?

RUSS HOUSLEY: [inaudible].

KERRY-ANN BARRETT: You want to turn heads? I just wanted to make sure because it's saying that what you have is rubbish, start over. And if that's what we want, it's fine, but I'm trying to avoid the statements in the first sentence that will hit and then persons will get caught up by that just that word instead of seeing our purpose. And I think our purpose is that there's no clear definition of DNS abuse. So before overhauling, let's hit the problem. So for me, it's a very emotional first sentence based on our frustration.

NORM RITCHIE: I get it. So what you're saying is "overhaul" is an emotional word, triggers an emotion and we want to avoid that? I like your word "revisit."

KERRY-ANN BARRETT: [I'd] start off with the fact that – isn't our problem that there's no concrete – is it the approach we want them to revisit, or do we want them to have clear definitions? We speak about definitions. Definitions come up three times in the same paragraph. So if I was the recipient and I read it, it's like telling me "Your definition, you have no approach for definitions." What exactly are we saying, revisit it? They have no process or nothing, there's nothing to revisit overall. We're not saying it. Like punch them, Norm.

DENISE MICHEL: So you find the first paragraph here just confusing?

KERRY-ANN BARRETT: Not confusing, just not direct. We're saying overhaul means that –

DENISE MICHEL: [inaudible].

KERRY-ANN BARRETT: Yeah, no, the whole thing, I get – so for me, if I look away, [inaudible] definition three times. "Overhaul your approach. So change your attitude towards it." Right?

DENISE MICHEL: Yeah.

KERRY-ANN BARRETT: You need to talk to people, you need to use international conventions to make your definition evolve, you need to create a complaints mechanism. So, are we saying to them "We want your attitude to change towards this process?" Or are we saying that "You need to establish clear definitions and engage the community to make sure that this is very clear?" Or are we saying that, "You don't like this attitude?" That's what I'm getting, "We don't like your attitude in terms of how you engage on DNS definitions."

DENISE MICHEL: Yeah. So it’s saying that ICANN should overhaul its abuse to DNS definitions, tracking and reporting, including implementing review recommendations. Yeah, I think it should be clarified. The point I think the subgroup was making is that there is, I think, an e-mail to the list, a well-vetted through the community and well-established definitions, there are well-established definitions of DNS abuse.

This team looked at this issue not once but twice, and unanimously decided that a tabula rasa new definition of DNS abuse is not needed and should not be the focus of our activity. The board used the excuse of, “We need to have a brand-new definition of DNS abuse” as a reason not to implement some of the CCT review recommendations.

So the heart of this recommendation is to fulfill your obligations, move forward with CCT review-related – CCT review recommendations now, based on the current DNS abuse definition. In parallel, the Internet and abuse evolves, so ICANN should have a process to evolve in parallel its definition of DNS abuse. And then we have some specific suggestions of how to rely on outside experts’ work in this area to augment what ICANN is doing.

So I’d have to look at the first paragraph to make that clear, but is that – go ahead.

NORM RITCHIE: Yeah, [I'm going to have to] side with Kerry’s view on this. If something is soliciting an emotional response to the reader, then we need to look at that again because that will destroy our message. So if Kerry is saying that's an emotional word, the word "overhaul," I think we should change that to "revisit." And I think that first sentence is a bit run-on. If we could break it into chunks, I think [inaudible].

DENISE MICHEL: Yeah.

RUSS HOUSLEY: But I think it's merging t ow ideas. One is we want them to in parallel do the two ideas. The first idea is get on with the definition, and the second –

DENISE MICHEL: [inaudible]

RUSS HOUSLEY: I understand that.

DENISE MICHEL: [And the second is evolving.]

RUSS HOUSLEY: One's definition and one's reporting. We want the two things to progress, and either it needs to be written so that there's two thing, or there need to be two recommendations.

DENISE MICHEL: Yeah. Can I suggest that I take that paragraph and fiddle with it and come back with an update for you guys to look at?

KERRY-ANN BARRETT: Don’t get me wrong, [it’s not a matter –] because I don’t think we need to – all the points are there. But it’s just a matter of –

DENISE MICHEL: [inaudible].

KERRY-ANN BARRETT: It’s just to be clear that you are not taking the fact that you have resources of DNS definitions out there already and just doing what you need to do. That’s just it. So it could just be – as I said, for me it was just that “overhaul” was emotive. So the “revisit” could fix it, and as Russ said, separate the two ideas [in the end.] But yeah.

RUSS HOUSLEY: So one of the things that the board was sharing with the review team chairs is the teams should share what the dependencies are so that if one recommendation depends on another, well, obviously you can't do the implementation of the second one until the first one’s done. Here, we’re clearly saying there is no dependency, get on with it. So that message needs to come through.

So let’s move down to the compliance part while Denise is wordsmithing.

HEATHER FLANAGAN: But we're going to need Denise for the compliance part since she's [sort of the lead of the] compliance subteam. Is she not?

RUSS HOUSLEY: No. Compliance is about the contracts.

HEATHER FLANAGAN: [inaudible].

RUSS HOUSLEY: Oh, it's the same team. I see what your point is. Alright, Heather raised the point that, Denise, if you're focused here when we talk about compliance, we won't make progress. So either we need to wait for you or you need to be involved in that discussion. Which would you prefer?

DENISE MICHEL: [inaudible].

HEATHER FLANAGAN: That's my point.

DENISE MICHEL: Sorry, I won't let it happen again.

RUSS HOUSLEY: Yes, you will.

DENISE MICHEL: Can you repeat your question for me?

RUSS HOUSLEY: Heather made the point that the next section we would move on to, you were heavily involved in, which is compliance. So either you should move with us –

DENISE MICHEL: I will move with you.

RUSS HOUSLEY: Okay. Thank you.

DENISE MICHEL: Sorry, trying to [inaudible]

RUSS HOUSLEY: I understand. Three things at once just didn't work. Alright, let’s move to the compliance section.

KERRY-ANN BARRETT: Just because all the other recommendations, we were very directive, the “fundamentally” is the emotive word. So “should change the compliance regime” is different from “fundamentally [inaudible].”

RUSS HOUSLEY: Adjust?

KERRY-ANN BARRETT: No, just “fundamentally.” It’s just the extra layer. Everything else was very direct. “Should do this.” So once the “fundamentally” is gone. See, Norm gets the mind – we had a mind meld.

RUSS HOUSLEY: We have avoided the word “must” everywhere, because the board is the one that has to do it, not us.

ZARKO KECIC: I again have a problem with giving orders to ICANN and that to move compliance activities to independent compliance office, outsourced. How we are going to defend this part to hire external compliance auditor?

NORM RITCHIE: Well, if it’s internal, it’s conflicted because its source of revenue comes from the very people it’s looking at compliance over. So the money comes from the registries and registrars for ICANN, and the compliance function – so they basically pay their salaries.

KERRY-ANN BARRETT: So Zarko, one of the things we were trying to get at is make it independent and third-party. It may not be prescriptive to say "Get a ..." The only other way to do it is like how we've done it on the others, to suggest to them how this could be implemented. But our idea was it has to be a third-party independent, and there's no other way to describe it than to suggest an external audit first.

NORM RITCHIE: [I'll give a for instance] because you have a registry, and if you see 100,000 abusive registrations, that's a source of revenue, but then you stop them and delete them and lose the revenue. So it's the same situation here on a grander scale.

DENISE MICHEL: Compliance already uses third-party auditors now, so it's not as big a leap as it sounds, I think. Changing the "must" to a "should," right?

ZARKO KECIC: Yeah, but I would change this "outsourced." So, is it outsourced or internal? It is up to ICANN.

DENISE MICHEL: Yeah, so the recommendation is outsourced. And I think that was unanimous among the subgroup on abuse and compliance.

KERRY-ANN BARRETT: Our focus was just to make sure it’s third-party. Third-party removed from, because I don't know how – would third-party removed from be better than outsourced? Our idea was not to tell them –

DENISE MICHEL: [inaudible].

KERRY-ANN BARRETT: Yeah, it’s like how to capture that we want it to be an independent third party.

RUSS HOUSLEY: I think that Zarko is making a higher-level comment, which is tell them what you want to happen, not tell them how to implement it.

KERRY-ANN BARRETT: So my first comment when he said it is wondering if we should actually move it –

RUSS HOUSLEY: [inaudible].

KERRY-ANN BARRETT: Yeah, if we should actually move that then to where we had the suggestions as to how this could be done. Maybe that would fix that part of it. I don’t think there's anything wrong with that, because we also had another section where we spoke about audits several times.

NORM RITCHIE: Okay, so I get what you're saying. What if we put "possibly outsource to an established auditing firm?"

KERRY-ANN BARRETT: Can I rephrase it?

NORM RITCHIE: Sure.

KERRY-ANN BARRETT: Negar, can you scroll up a little bit? My computer is still restarting for the past half an hour. Go to the sentence that we're fixing. Just to show both pages. Maybe we could say something like "Move its registry and registrar compliance activities to be independently audit." If we say, "To be independently audited," it would capture without being prescriptive. Yeah, so it's very specific, what we want is that it needs to be independently audit, full stop. And instead of probably move to probably say something [inaudible]. "And ensure that its registrar and registry compliance activities are independently audited." Probably change it around that way. I think that would, without being prescriptive that it needs to be to an external audit firm, da da. Would that help? Zarko?

HEATHER FLANAGAN: We have another place then to change that, down in the second bullet.

KERRY-ANN BARRETT: So it’s a separate point, right, Denise? Norm? This was a separate point though, us wanting a compliance office. This was a different point because one of the issues we had found in the subgroup is that it seemed as if Compliance did not have the power and authority it needed to do its job because of where it was subsumed, so we wanted Compliance to be a properly established, functioning office, not just have – I think that’s one of the – Norm, you could correct me.

NORM RITCHIE: Yeah.

KERRY-ANN BARRETT: It was a completely separate issue. Yeah.

ALAIN AINA: Maybe I also need help here. It looks like we’re talking about two different things here from what I could see. One is make sure your compliance offices get audited by independent party, but the second thing I'm seeing here is we are saying that the compliance activity itself be outsourced or something to an independent – so it looks like there are two different things we’re talking about.

One thing is that, okay, ICANN still have internal compliance office, but get this activity to be audited by independent part. But it looks like we are now talking about the whole compliance offices to be ...

DENISE MICHEL: That is correct, the edits in the first paragraph fundamentally change the recommendation of the group. The recommendation of the group was move this to an independent party, not be audited by an independent party, which ... Yeah, it is to move it to an independent party. Yeah, you're right.

So we should discuss the first paragraph edit because it's not in line –

KERRY-ANN BARRETT: [inaudible].

DENISE MICHEL: It's not in line with what the group recommended. So I think more discussion is in order. Yeah, I don't agree with all the edits up there, personally.

RUSS HOUSLEY: That's kind of good because I couldn't figure out how to reconcile it with the second bullets.

DENISE MICHEL: [Yeah, it can't be.]

RUSS HOUSLEY: Right. So we need to figure out –

KERRY-ANN BARRETT: Denise, I agree with you, it has fundamentally changed it, but it's probably how we had it drafted then, because what it's saying is that we want a compliance office within an established auditing firm. So would that auditing firm be hired by ICANN for life? If what we're speaking of is – how it's worded there, if the explanation we have is that we want an established compliance office, which is – when I was taking part in the subgroup, that's what I understood, there was the external auditing function and there was the compliance office that we wanted established.

But if it's to be how the sentence read before was an independent compliance office outsourced to an established auditing firm, that means that it's not the function. We said office. So if we said office outsourced to an auditing firm, that's a permanent move. That means that auditing firm will be there for life.

So I generally thought, even during the call, that we wanted two separate things happening in one. We wanted an established compliance office and we wanted the oversight of an independent auditing firm to make sure that everything runs – so unless I misunderstood as well. Because [inaudible] we can't recommend for an independent compliance office into an external private sector body for life. That's how it would – when you read it, without me being like – when you read it as is, that's what it would look like.

DENISE MICHEL: So if you read the second bullet, the group was trying to get at the fundamental conflict inherent in ICANN to come up with a structure that hopefully yields much more effective compliance activities.

If the compliance activities were fully outsourced, what would an internal compliance office do, do you think, in what you're describing?

KERRY-ANN BARRETT: I could answer that question, but that’s not the issue I was highlighting. How we have it worded was a compliance office embedded in an external auditing firm. Is it that it would be a firm that goes out to tender every year? Is it that it would be a compliance office function that is going to sit in any auditing firm that’s renewed every year, every two years, every five years?

DENISE MICHEL: We didn't address the RFP and –

KERRY-ANN BARRETT: No, that’s fine, it’s just that how –

DENISE MICHEL: Renewals and things like that. [inaudible].

KERRY-ANN BARRETT: Just remember I was part of the group too, so [I want to see] where we’re going.

DENISE MICHEL: No, you're right, we didn't get into that level of detail of how this would be outsourced. The time period for the contract and whether it would be rotated and all that stuff. We didn't get into any of that.

KERRY-ANN BARRETT: Which is fine, but I'm saying if you look at how Zarko read it, because of how it's written, it just says that the office is going to go to an external auditing company. That's a full stop. We have not said a compliance office that would be outsourced on whatever basis, like a competitive basis, da da. But it's –

DENISE MICHEL: So, would it be easier to understand to talk about the compliance function?

KERRY-ANN BARRETT: Function rather than an office, because an office is an established thing.

DENISE MICHEL: Being moved to a neutral third party?

KERRY-ANN BARRETT: Yeah, because how it's written, just looking at the words, it just says compliance office, so you're now thinking of a body of people being seated in an external auditing firm for life. I don’t think that was our intent. So everything that you said, I agree with. I understood. [Like I said, I was] part of the subgroup. But just Zarko as a person outside reading it and just hearing his reaction to it, I'm seeing where that one sentence could be misleading in terms of what the ultimate purpose is. And I agree with you, the edit that we made doesn’t address it, so it’s just to backpedal and fix it.

DENISE MICHEL: [Does that work?]

KERRY-ANN BARRETT: I can't see it, my computer is still [booting.]

DENISE MICHEL: Okay, so I'll read it for you. “Should change the compliance regime by taking the necessary steps as described below to amend the RAA and the RAs, establish procedures to address systemic abuse involving contracted parties, and ensure that its registrar and registry compliance activities are outsourced to an established auditing firm.

ZARKO KECIC: Denise, I understand what we are trying to do, but I wouldn’t and I don’t think that it will be accepted to recommend to have external firm. It is up to ICANN and –

DENISE MICHEL: How do you know?

ZARKO KECIC: I don't know, but I'm afraid that it wouldn't be accepted. And then another thing, our remit is not to recommend establishment of – actually, not establishment but hiring external firm to do permanent job.

DENISE MICHEL: I'm sorry, it's not our job to recommend it? [I didn't understand this part.]

ZARKO KECIC: Hiring external firm to do permanent job which is now within ICANN. We can say if we are afraid that there is a not independent and not biased compliance team right now, we should say establish independent and not biased compliance office. Where, I don't care. Within ICANN, outside ICANN, somebody else will decide, not we.

DENISE MICHEL: Yeah. Okay. The part of the concern – and other people on the subgroup should jump in as well – is that there's been a number of tweaks over the years, going back decades, to ICANN Compliance, and many declarations that it's neutral and independent, etc.

And after a lot of due diligence, what the subgroup found is that a significant change in this direction is needed. Simply telling them, as has happened many times in the past, to be independent, to carry out its obligations, to be neutral, simply has not worked.

So I think that's part of what got the subgroup to this recommendation, which I think the way I'm looking at it is that it's a good time and a reasonable draft recommendation to raise with the community and see what people think. And it may be that we'll want to then modify it as we go forward with the draft report. But I don't know, Norm or Kerry Ann or Laurin, did you have anything you want to add to that?

KERRY-ANN BARRETT: I think we'll probably have to regroup for a second, like together as a subgroup, because what I understood, and if that wasn't the intent when we came up [inaudible] what I understood – because it was something I had a problem with from day one, was there needed to be enough power given to a compliance entity within ICANN but have that oversight of an external auditing firm to make sure that they're following what they're supposed to follow and do.

So I think we probably have to regroup, because to permanently outsource the compliance function, I'm not sure how sustainable that would be or how … The need for an external auditing oversight is critical, but to permanently outsource it? I thought we were doing an institutional strengthening and not outsourcing an entire function. I didn't understand we were trying to understand the entire function.

So it was probably a misunderstanding on my part.

NORM RITCHIE: I've been [inaudible] dealing with some other models that kind of fall in the same area, and some of them are regulated. even in those cases though, the entities that regulate it have watchdogs looking over them all the time so that they correct the problem before it hits the regulators.

What I'm saying is there's different models that might work here, and we've jumped to one to say it’s either inside or jump outside. And even amongst ourselves, we’re not resolving that, so it’s not likely to get far outside of this room. So I wonder if we should look at some of these other models and perhaps – having oversight for instance, that is, [where the results of the audit are] public, that might work.

DENISE MICHEL: Can I propose then that we have the subgroup discuss this a little further? And we can trade e-mails with KC and Scott and Eric I think is who’s missing, and perhaps come up with –

NORM RITCHIE: [We have until tomorrow.]

DENISE MICHEL: Broader language that notes that we think a significant change should be made so ICANN can move forward with an independent, neutral, effective, compliance function, not be specific about in, out, auditing, etc., and then keep talking and working on that. Would something like that general approach be acceptable at this point?

NORM RITCHIE: AS long as we can come up with it by tomorrow.

DENISE MICHEL: I mean, [but Zarko, I want to hear your opinion.]

NORM RITCHIE: I do think it's very important that this is discussed, the recommendation comes forth [inaudible]

DENISE MICHEL: Yeah, we should all understand and agree on what we're recommending.

RUSS HOUSLEY: Okay, so what I did is I inserted a comment, "Come back to this one." By that, I mean not later than tomorrow morning.

DENISE MICHEL: It'd be good to do it today. Zarko, did you have more thoughts?

RUSS HOUSLEY: [inaudible].

DENISE MICHEL: Yeah.

ZARKO KECIC: It is not question will I accept or not.

DENISE MICHEL: No, I want to hear your opinion.

ZARKO KECIC: Will community and board and ICANN accept this this way, or other way? I wouldn't accept if I have some Implementation Review Team coming to my office saying you should hire somebody instead. You have a compliance team but you should hire somebody outside your organization to do that job because they are biased, they are not doing good stuff. Probably, you have some result of that review you did.

But another question is, will that external office be still independent? If I am big registry with 90% of domain names doing abuse, I believe I have enough money to buy that office.

DENISE MICHEL: Yeah, if only our job was simply to review one ccTLD. It would be much easier, and have less global impact. But we clearly need to do some more discussing about the approach and the model, so we'll do that and come back with some suggested wording by tomorrow morning. How's that?

RUSS HOUSLEY: Okay. I don’t like putting anything on hold because we've got a very short deadline here, but I get why we have to do that. Okay, I think the next one is policies and agreements with contracted parties, which is at the top of page 60.

NORM RITCHIE: [Do we] need to say in this one that having revised contracts/agreements are a prerequisite for Compliance to be able to do a better job handling abuse, etc.?

DENISE MICHEL: I think that’s a third bullet.

NORM RITCHIE: [Oh, I need to scroll then.] Got it.

RUSS HOUSLEY: Are you saying that that’s the motivation for the whole thing and so it should [inaudible] at the top? We’ll let Heather fix that.

NORM RITCHIE: Sorry, Zarko and I had a side conversation. The very first sentence says adopt new policies and procedures. ICANN cannot adopt things. They have to be ...

ZARKO KECIC: PDP process.

NORM RITCHIE: Yeah, has to go through the process.

DENISE MICHEL: Well, they can adopt it after a new ... Some of them. But some of them they don't. For example, they don't need a PDP to change the fee structure, of the fees they collect from registrars and registries. They can actually use the fees to incentivize DNS abuse mitigation. That doesn't require a policy change.

Some may, some do, and some don't. But if a recommended change involves a policy development process, it's the board's responsibility to accept or reject a recommendation, send it to the GNSO and say this is a recommendation, please address it. And then it's the GNSO's job to run a PDP, or I guess not, is how I'm looking at this workflow.

ZARKO KECIC: There is another thing. okay, looking at all reports, the most abuse comes from new gTLDs and from gTLDs.

DENISE MICHEL: [Not really.] .com has the highest.

ZARKO KECIC: Okay. There is no big difference between – actually, there are more ccTLD domain names than gTLD domain names. It changed in past ten years. And ICANN cannot do anything with ccTLDs.

DENISE MICHEL: That's not the case.

ZARKO KECIC: What do you mean that's no the case?

DENISE MICHEL: Are you saying there's more new gTLDs than ccTLDs?

ZARKO KECIC: No, what I'm saying, there is more ccTLD domain names than gTLDs.

DENISE MICHEL: I don't have the statistics off the top of my head, but [inaudible]

ZARKO KECIC: It is some 160 million ccTLDs and 150-something gTLDs.

RUSS HOUSLEY: [inaudible].

DENISE MICHEL: Are you recommending different text or a different point?

ZARKO KECIC: No, but we should think about ccTLDs as well and abuse in ccTLDs, and especially, we have a couple which are – not couple, but few of them which are acting as gTLDs, and they are heavily abused.

DENISE MICHEL: Yeah, absolutely. And I think the CCT review demonstrated that in its research report. So, what additional text would you recommend?

ZARKO KECIC: Right now, I don't have anything in my head, but what I'm trying to say is we are here talking about policies and agreements, and no ccTLD has agreement and no policy is [trending towards] ccTLDs. So somehow, we have to cover entire domain name space.

DENISE MICHEL: So, do you want to come back with some text on that?

ZARKO KECIC: I'll try to think, and all of us will come up. I really do not have solution.

DENISE MICHEL: Yeah, I think we're at the point where we need writing, so I take your point for sure, and I realize ICANN's limitations when it comes to influencing ccTLD behavior. And of course, some of the ccTLDs, as you know, are at the forefront of tools and processes that mitigate abuse. We would be lucky if some of the new gTLDs adopted some of the things that some of the ccTLDs are doing, but I take your point. We sohudl also acknowledge the abuse in some – high levels of abuse in some ccTLDs and recommend something there if you feel it's appropriate.

RUSS HOUSLEY: As you well know, we have different ways to deal with the divided space between the ccTLDs and the gTLDs. These clubs and carrots, however you want to think about them, don't apply there. We'd love to have the ability to write a section to deal with one space and one to deal with the other, but we don't have the same levers to pull.

ZARKO KECIC: Yeah, I know, that's the reason why I'm saying that I don't know how to do that. But I would rather see here – because this is a really important part, and, okay, talking about compliance, there are no ccTLDs, but talking about abuse, that's really important and I would rather see some more general recommendation which will cover entire domain space, and after that, coming to Compliance to address gTLDs with agreements with ICANN.

RUSS HOUSLEY: I know the abuse subteam didn't get there, but I don't think anyone in the room disagrees with you.

HEATHER FLANAGAN: With regards to the specifics, 3% of registration and 10% of something else, are those hard and fast rules, or are those examples?

RUSS HOUSLEY: The now first paragraph, the one that was the first bullet and got moved up at your suggestion. On the screen, the highlighted text.

DENISE MICHEL: Well, based on the CCT review, I don't know that there's a large chance that any of our recommendations will be accepted, but I take your point. We should craft them in a way that's as palatable as possible.

At the same time, I think we need to keep in mind that a certain level of specificity and direct guidance is needed to really convey and try and build in some accountability to what –

KERRY-ANN BARRETT: And measurability.

DENISE MICHEL: And measurability of what we're suggesting.

RUSS HOUSLEY: Okay, so I see us fragmenting into several side discussions. What I think we need to do is press forward to figure out how many of these recommendations need the kind of wordsmithing that we've now identified two. So let's move forward to the abuse of naming section, which is on page 69, and we'll then figure out how many groups we need to break into to do that rewording and use the balance of the day to do that.

Let’s see if we can get through abuse of naming, and then take a short break and then come back. Okay, I'm not hearing anyone have concerns with the two paragraphs in the recommendation section for abusive naming. Heather made an e.g. Anything else? Cool. Alright, let’s take a five-minute break, please. And then we’ll come back and resume.

Okay, our five minutes are long ago. The next one we’re going to look at is page 70, DNS testbed. I'm sorry Eric isn't here, but oh well. I think my first comment is this should be [Org.]

HEATHER FLANAGAN: And for the record, having learned there is an ICANN style guide that I can get my hands on, I will fix all of the Orgs to be appropriate to ICANN style.

RUSS HOUSLEY: So Zarko, do you want to remove the one year?

ZARKO KECIC: I didn't get to that recommendation yet, but I have a lot of questions about this issue.

RUSS HOUSLEY: About the one year, or about the whole thing?

ZARKO KECIC: About whole thing.

RUSS HOUSLEY: Well, then I'm really sorry Eric isn't here, because he's the one who really is best able to defend it.

DENISE MICHEL: I just texted [inaudible].

ZARKO KECIC: Just to explain my point here and to some other recommendations that we have, there are a lot of things that are related to SSR but they're not that important, and if we want to comply with request from ICANN board to have fewer recommendations which will do [higher] impact to the community and security and stability and resilience of DNS and unique identifier, we should consider having only that stuff, not to have some recommendation which are related but not that important.

RUSS HOUSLEY: So I'm putting a comment in that says come back to this one question about lowering its priority. I don't know if that’s – but I certainly don’t want to have that discussion without Eric if he's actually going to be here.

so other than the – I think timely completion and whacking the one year doesn’t hurt, but ...

NORM RITCHIE: On the testbed one, kind of remember that conversation, that was actually started by a skunkworks project that wasn't completed.

RUSS HOUSLEY: Yes, I know.

NORM RITCHIE: Yeah, so part of this is actually [inaudible]

RUSS HOUSLEY: It says it was started and not completed, and basically, it says ...

NORM RITCHIE: because of lack of funding, right? Lack of funding and resources. So part of the reason for putting this recommendation there was to make sure it got the funding and resources to be completed.

I disagree with the one year. That's already been stricken. Perfect. Thank you.

RUSS HOUSLEY: I think Heather's in the process of fixing that.

NORM RITCHIE: As you said [earlier,] that's budget time, that's why I think having that recommendation out in the open now is timely.

STEVE CONTE: I think timely is reasonable. I think this, in some ways, will go to the future discussion on prioritization as you guys look and prioritize your recommendations, because I'm not saying that this isn't a good idea. I do think this is a good idea, but it comes down to a question of resources, manpower, funding and everything else, and determining where that should be slotted in with the rest of the recommendations.

RUSS HOUSLEY: We'll just assign Steve Conte to this full time and it'll be taken care of.

STEVE CONTE: Russ, I'm getting a taxi after this, you wan to join me?

RUSS HOUSLEY: Okay, IANA portal, which is on page 71. We're going to revisit its priority but not until Eric's here.

KERRY-ANN BARRETT: [inaudible].

RUSS HOUSLEY: We're going to revisit, where the lowest priority would be "delete." So page 71, IANA portal.

ZARKO KECIC: I have a comment on this, because Norm and I had talked to Kim Davies in Marrakech in regard of IANA way of doing changes and how portal is developed and how it works. So I would change a few things here, because I believe they're different. I'll read this again. I've read it a month ago and I don't know what has changed, but I would also put importance of having new software, because IANA is developing new software for a few years now and it is still not done. And it can be done in half a year if it is really priority for ICANN. It is done within ICANN ...

STEVE CONTE: [I don't know, we'd have to ask the question.]

ZARKO KECIC: What Kim told us, it is internal development of ICANN, so that's the reason why it is slow. And Laurin, you were working on this.

LAURIN WEISSINGER: Yes. Essentially, this came out of discussions between Zarko, Boban and myself in Kobe, and then we did some edits. I wasn't privy to the conversation you had with him. I don't think I was there. If I was, I forgot.

ZARKO KECIC: You were not there, and [inaudible].

LAURIN WEISSINGER: So I would just say, Zarko, just propose the changes you would recommend to this based on that conversation, and then we could look at it.

ZARKO KECIC: Yeah, let's find some sometime, because –

LAURIN WEISSINGER: Okay, yeah, we can do it [again.]

ZARKO KECIC: I want to do it with you guys, because we had talked to Kim, and I did several changes for my TLD recently, and I found out some differences that I thought before.

LAURIN WEISSINGER: Okay. So I think we have to have an edit session for compliance already, so during that time, we can do that.

RUSS HOUSLEY: Okay. So that's at least three of them that need some editing. Key rollover on page 72.

NORM RITCHIE: This seems to go into a fair amount of detail on what specifically should be included in the tabletop. Do we want to go that level of detail?

RUSS HOUSLEY: Do you want to suggest some deletions?

NORM RITCHIE: I'm thinking we should say there should be a tabletop exercise and kind of leave it at that. This goes into quite a bit of detail into what specifically needs to be done, although it is probably not wrong. I'd hate to change [inaudible]

RUSS HOUSLEY: I don't know, etc. twice in one sentence is kind of egregious.

KERRY-ANN BARRETT: Just to delete the sentence that says "These tabletops must follow ..." Just to delete that sentence would fix it? Because everything else was kind of suggestive in terms of the kind of things we would want to see happening. That's the only one that's very, "They must ..." So if we delete that entire sentence, would that work?

NORM RITCHIE: I'd like to actually [leave it until] Eric's around for this one. I actually think if you just left that sentence and deleted everything else, it'd work.

KERRY-ANN BARRETT: I kind of like how it goes, unless we give ideas, but it kind of outlines very specific areas that we wanted them to address, which is part of the stakeholder engagement and the clarity. Like it would just be tabletops and I don't know if that would be sufficient.

ZARKO KECIC: Nobody understands what is tabletop exercise.

KERRY-ANN BARRETT: It says periodically run tabletop exercise, follow the root – nobody understands what tabletop exercise is?

ZARKO KECIC: Yeah, I know what it is, but what it should cover, I don’t understand in this case.

KERRY-ANN BARRETT: Okay. Yeah, so probably tabletop exercise should run [inaudible] that follow the procedure for the specified [key rollover.] Would that make sense then?

NORM RITCHIE: [inaudible].

KERRY-ANN BARRETT: Who’s editing? I'm seeing movement. That’s Heather?

HEATHER FLANAGAN: [inaudible]

KERRY-ANN BARRETT: [inaudible] Tell me, Zarko, it’s like it would be periodically run tabletop exercises that follow ... But we have that follow the root KSK rollover process. That’s the tabletop, I think, that they want to do.

RUSS HOUSLEY: Good enough?

UNIDENTIFIED MALE: Yeah.

RUSS HOUSLEY: Okay. Root server ops, page 73.

LAURIN WEISSINGER: I think this is mainly going to Steve. I'm not sure if this is not something that’s already being done. It’s mainly a question for later prioritization of recommendations. If you could say something about what's being done right now on that front.

STEVE CONTE: I do know that there's been tabletop exercises in conjunction with RSSAC on some of the root ops stuff. I don't know the details behind what took place on that. So if you’d like more information or if it'll help inform this dialog, we can ask RSSAC or someone from OCTO, John Crain or so, or Terry Manderson from E and IT to comment on what has taken place around this.

RUSS HOUSLEY: Could you just fire this text off to Terri and ask him whether he already does it?

NEGAR FARZINNIA: We'll take an action item and send a note.

RUSS HOUSLEY: Thanks.

LAURIN WEISSINGER: So apart from being unsure about priority, I'm okay.

RUSS HOUSLEY: Alright, root zone data. Boy, this is a long one. Page 74.

KERRY-ANN BARRETT: Just a question, what's the difference between "should create" and "bring into existence?" Is that creation?

RUSS HOUSLEY: SOmeobdy else can do it. If I recall, Eric said like they could pay a university to do it.

KERRY-ANN BARRETT: But that's creating. The means by which they create is irrelevant [inaudible].

RUSS HOUSLEY: I'm fine –

KERRY-ANN BARRETT: There was a debate on that?

RUSS HOUSLEY: There was. I'm fine with ...

KERRY-ANN BARRETT: Should create?

RUSS HOUSLEY: Create.

LAURIN WEISSINGER: [As somehow this wasn't seen,] I'm wondering, can we somehow reduce the length of this recommendation to about a third of its current length without removing too much detail?

RUSS HOUSLEY: Well, you could do that by moving the bullets to the findings. You know, "Examples of information that would be very helpful are ..." Or something. But this is small compared to the compliance one.

LAURIN WEISSINGER: So my problem essentially is this is a page-long recommendation.

RUSS HOUSLEY: Laurin just said, can't we reduce this to one paragraph? Please get settled, but you will be in the thick of this one.

KERRY-ANN BARRETT: I think for some of it, it's prescriptive as to what we're recommending them to do, which is very specific, like they should create. Boom. The rest of it, unless it's critical, that's what we could move if we want to reduce it. Like the end result, what it would cause to happen. So what we're hoping is the outcome is what could be removed, and specific actions could remain, because it starts off each time with a specific action and then it's followed on by what we expect to be the end result.

LAURIN WEISSINGER: So again, I have no complaint about the content per se, it's just I think a lot of this should be moved to the findings.

KERRY-ANN BARRETT: [inaudible].

RUSS HOUSLEY: Right, so just leaving the highlighted text as the recommendation, would that work for you?

KERRY-ANN BARRETT: I can't say specifically, but the second bullet for example, for me it's very specific, and it's different ... The second bullet, the first bullet says about the creation of formal KPIs, while the top speaks about the metrics. [inaudible] the KPI was really the solution, like one of the options for the metrics, [inaudible] not?

RUSS HOUSLEY: Yeah?

KERRY-ANN BARRETT: It is? Well, if it is, then I guess you're right, the rest could be moved. I agree.

RUSS HOUSLEY: Yes, Heather?

HEATHER FLANAGAN: Perfectly happy for stuff to move down into findings, but one of the points I'd noted earlier is that when the text says that ICANN should do a thing, that reads to me as a recommendation, not a finding, so this would have to be rejigged a little bit more than just cutting and pasting, I think.

RUSS HOUSLEY: Right, it would be these kinds of things would be useful and why, would be a finding.

LAURIN WEISSINGER: I think this is – there is a lot of parallels, so I think it is doable, it'll just require 15 minutes or so of rewriting.

KERRY-ANN BARRETT: Just to make it simple, because I don’t think it’s something we have to necessarily come back to, because of the rest of it, the only part that says specific again, it’s just that sentence, ICANN should create the KPIs. Everything else reads like findings. That’s the only one that’s a direct action. You found another one?

DENISE MICHEL: There's the one you noted in the first bullet. In the third bullet, “ICANN should create or commission the creation of a framework for assessing and measures that codify a propagation delay of root zone changes to instances.” And the bullet after that is the third or so sentence, ICANN should create a set of measures that demonstrate the size, growth and composition of IANA registries.

ERIC OSTERWEIL: Just so I feel like I contributed. Maybe I missed this because I probably missed a lot of stuff, but I think I remember somebody taking exception or bringing up an issue with KPIs and how they would be measured. Did we talk about that again today? Did I just ...

KERRY-ANN BARRETT: [inaudible].

RUSS HOUSLEY: No, but if the higher level recommendation is taken, the discussion of KPIs will move to the findings, so therefore, we won't have to have that argument.

KERRY-ANN BARRETT: So I have [a fear.] There's nobody taking ownership to fix it, so I'm just trying to figure out who’s fixing it.

RUSS HOUSLEY: I’ve put a comment in there that said reword these to state the benefit of that particular thing to the community and then put the whole thing in the findings, leaving only the first paragraph as the recommendation.

HEATHER FLANAGAN: And that’s probably something I can take a stab at when we’re not otherwise engaged in the document.

RUSS HOUSLEY: Yeah, I definitely want you to stay engaged [inaudible].

KERRY-ANN BARRETT: Okay. Perfect. I was trying to figure out the who.

RUSS HOUSLEY: Okay, cool. Of course Alain ran out of the room, we're on his recommendation. It's alright. Page 75, cryptography.

ZARKO KECIC: I'll ask that question again, if we leave just this first paragraph, CZDS, I really don't see that that's any priority in regard of SSR. CZDS is database of zone files for gTLDs, for domainers and researchers, and I don't know who else to access easily those zone files. And if they don't exist, I don't see any threat to SSR.

ERIC OSTERWEIL: So how do you know there's no threat to SSR if you don't measure it?

ZARKO KECIC: [SSR measure in CZDS.]

ERIC OSTERWEIL: I guess I was responding to your comment that – I thought I understood you say that there was no reason to put the measurements of the CZDS in, because what's the threat to SSR?

ZARKO KECIC: No, I just said they're not that important.

ERIC OSTERWEIL: The measurements or the CZDS? I can say I find it to be very important personally. Could certainly espouse my own perspective as a measurements person, but I'm not sure if that's what you're talking about or not.

ZARKO KECIC: [inaudible] we talk about personal issues, that's one thing. If we are talking about global threat, I don't see CZDS as something which is really important to be in our report.

ERIC OSTERWEIL: Okay, that's a fair comment. [inaudible] a little bit more pedantic. So my perspective researching security, stability and resiliency threats is that it's useful data. I personally found it useful as I've researched those particular things. That doesn't mean I'm always right or anything, but I could certainly describe how looking for for example abuse is something that's very greatly benefited by access to CZDS. And I can say as a user of CZDS, I've been dismayed is probably the nicest thing I can think to say about the ways in which my access has been curtailed, denied, revoked, [inaudible], etc.

So I think it winds up being if you're going to actually use it to do DNS abuse analysis, which I think it's very good for, then its ability to actually serve the role, the function that it's been given, is really important. And my anecdotal evidence suggests that it's at times very lacking, so I think a more structured analysis and more structured measurements are critical.

DENISE MICHEL: Yeah, that's been my experience as well, and there's been several writeups of failings of the central zone file data system, and particularly its impact on cybersecurity and cybersecurity researchers. It's been a problem consistently since the system was launched.

LAURIN WEISSINGER: Not to go into this, but there are a variety of issues that people struggle with. We can talk offline about this. I'm not talking about just you, Eric. I'm talking generally. So I also support that there is a problem and that there is a point in having it.

ZARKO KECIC: That's my question. If we can discuss later on, I'm happy to discuss. Right now, I really don't see – I understand that we have for example DNS over HTTPS just mentioned n one sentence and we don't have any recommendation on biggest threat to DNS today. And we have a lot of measurements which are somehow related to SSR but are not our biggest priority right now.

ERIC OSTERWEIL: I'm trying to home in on the disconnect, because I feel like there's probably a disconnect. Maybe I found it. So when you say the biggest threat, right after saying DNS over HTTPS, do you mean DNS over

HTTPS, you're considering as the biggest threat? Just to make sure I understand.

Okay, so while I personally don't take exception to that at all, what I would say is the more fundamental measurements are what enable us to have discussions about those sorts of things. But I think there is a bit of a difficult role if we want to talk about DNS over HTTPS, because there it gets maybe difficult to figure out what ICANN's role in that system is.

So while I may not disagree with you at all, I may find it difficult to figure out how we can structure a recommendation. But I would also use that as a great strawman to say fundamental measurements of these underlying substrates enables us to do research and to do the second order effects and to actually hanging that around ICANN and identifying if it's in its remit.

So I agree with you, but I'm not sure how close we can get in the report, but these other measurements, especially like CZDS and of KPIs, they help us actually do analysis that leads to that in my opinion.

ZARKO KECIC: If DOH gets broader use, there'll be no measurements.

ERIC OSTERWEIL: I agree, and I'd love to hcat with you more, probably offline just because of our focus in the group, because I totally agree with you. So my pushback is not in the sense of I disagree with what you said, it's just I'm not sure how to frame it inside of the work we have in front of us. But I'm just kind of throwing out the perspective that some of these other things actually become very useful in those discussions too, like having these measurements, doing these substrate analyses, but I can chat offline if you'd rather.

ZARKO KECIC: I'm not saying that measurements are not important, but we should focus on most important stuff, because we are asked to have just few recommendations and not hundreds. A couple of times. And probably board will repeat that and community will repeat that. That's my point. And I would really like to see HTTPS. I don't see what we should recommend to ICANN right now, but I believe that ICANN should take leading role in solving that problem, because it'll become huge problem when it is adopted by many software developers and vendors.

RUSS HOUSLEY: Okay.

KERRY-ANN BARRETT: This is not my area so I can't jump in on the technical side, on the benefits, I just wanted to throw in two considerations. Is it a nice to have or a must have? I think I would probably ask you to think about. So we have the CZDS as the only example. We could put other examples to show that it's not just that alone but others, and hit the point, what you're saying, that in order to do the things that we've recommended, which is having DNS definitions, having this, having that, the research is what would be good to underpin the other things that we're asking ICANN Org to do for the community, because that's what I'm hearing, is that this is not just a nice to have, but it's more that this critical information can feed into long-term threat analysis.

So, can we say that? Because we're specifying a specific, just one thing, and I know you said it's one of the critical things and it has helped, and Denise has validated that. But can we get to the specific, which is for us as a more general observation, we've recognized that for all the other things that we've spoken about in our recommendations, it addresses Zarko's point of not having more recommendation is that research underpins all of this in order to get effective definitions. Effective methodologies, effective metrics, etc., research underpins it and we need to ensure that the community has access to the data needed to do this, such as ... But to rephrase and restructure it as probably more general conclusion rathen than, as probably you said, another recommendation, because it is a specific thing, but I think it underpins a lot of our other recommendations. That's just one approach we could – I can't speak to the technical benefit, but just listening to the discussion, that would be my ...

LAURIN WEISSINGER: One thing, I'm looking at the text outside the document right now, trying to figure out if we can do something. That's one. The other thing is I totally agree with Zarko, we should think about the problems he describes and consider it. we haven't considered it before deeply enough, I think. So totally agree on that.

On that one though, it is very important for measurement, and there are a lot of people who can talk to that. And as I said, let’s do that later and not spend group time on this.

ERIC OSTERWEIL: I’d like to back up to something that I thought of while Zarko was talking, and then maybe jump back to what Kerry Ann brought up. I don't know if we talked about this earlier today before I was in transit or if we have a plan to talk about it tomorrow or not, but I do think at some point we might want to actually circle up on where we stand with the numbers of recommendations, the concern that here's too many recommendations, and the impedance mismatch that gives us whereby we try to do early optimization without realizing what our recommendations actually are. We’re just cutting down numbers. We can't help but loser some important information from ourselves even before we decide what the best recommendations are and what we’re trying to say.

And I think there's a longer discussion to be had there amongst the team that I think if successful, we would then want to have with the board caucus group, whomever else. So I don't know if we've talked about that yet or we’re planning to, but if we aren't planning to, I’d like us to plan to talk about it.

RUSS HOUSLEY: We're going to talk about the prioritization in another pass. We thought it was important to go through all of them so they were all kind of in our cache in order to have that discussion. We had not had a discussion about the [ADOT] or any of those things, or DOH. I don't think we have any text that anyone knows how to address to ICANN regarding those yet.

ZARKO KECIC: We should think about text, because I really think that's important, and it must be in our recommendations right now. And there is one question. Is ICANN responsible for domain space that ICANN delegated to TLDs, or ICANN is responsible for entire domain space? With DOH, we'll have more and more domain space outside the ICANN part, and also, we'll have some fancy resolutions in [that domains.]

Not only that, but in existing domain space, and we don't know how it is going to end up.

RUSS HOUSLEY: So at a minimum, I think we should write something for the future section that says, watch what's happening here but maybe we need to go further and even say actively work against the adoption of that technology.

We probably should talk about that – I'm not sure we're ready to put words on paper yet.

ERIC OSTERWEIL: I'll just finish up real quick then. My perspective on the multiple recommendations and there being too many is that it's important for us to express what we think is important, and if someone then comes back and says that there's too many of those, then I think there's still an important data point there that we still have a lot of work to do.

If on the other hand we get the news that we should only come up with five things and we only come up with five things, then we've missed a data protection of there was a lot of work to do. Someone can always reject a whole bunch of the things that we say, but I think even just down the road, this is part of the transition. How much work was left to do after the transition? If we come up with a lot of recommendations, it suggests that the review teams thought there was a lot of work to do. If the review teams are all kept to five recommendations each, then there's no data point there about how much work there was to do, regardless of what's picked up. That's the broader discussion that I'd like to see if anyone has appetite to have.

To Zarko's point, or to one of the things that came up just a second ago, we may want to come up with some framing text. I would say one of the starting point is that maybe there should not be active energy expended by ICANN Organization furthering the development of these standards, which is the case right now.

I think the biggest proponents of DOH are actually ICANN Org. So I think if we have a problem with DOH, and we as the community think that there should be a statement made about it, then I think maybe at the very least, stop funding people to further it.

ZARKO KECIC: A lot of measurements are done by universities, by research groups, by different organizations, even some of measurements which are proposed here, you can get out of RIPE and Atlas, not to have your own measurements but you have root zone measurements over there. So propagation stuff and other things are already there. And for research purposes, I believe that's enough for some researchers to do that. And I'm not against general recommendations that ICANN should encourage and support different type of measurements which will give more data in establishing [ground-based] SSR for DNS.

And just string this, as Laurin says, into some general stuff, and maybe put examples what we're looking for.

ERIC OSTERWEIL: A couple things. Yeah, I think you're right, there's a lot of people that do measurements, and universities are among them, but certainly not just universities, and lots of people do it.

I think the observation that I felt was coming from this was that someone should be responsible for that happening. Because if a university researcher is collecting a corpus of data and then they just decide to stop one day, and then years later, somebody else says "I really wish I had access to that data," it's gone. Whatever would have been collected after they stopped is gone. And maybe even the old stuff is gone, it's not really clear.

I think the idea of these recommendations was someone should be in charge of making sure that happens and that it’s archived, because it should then become a public resource. And I think that right now isn't really anywhere. You're right, you could go to RIPE and you could commission Atlas to do a bunch of measurements, and then you could collect that data or drop it.

But Atlas is a measurement infrastructure, it’s not a data archiving infrastructure. You could build that on top of it.

ZARKO KECIC: There is DNSMON.

ERIC OSTERWEIL: Yeah, so who’s to say that that’s going to be around next year or ten or four years from now? My point is there are a lot of people who do a lot of long-term measurements, but nobody is required to do it. They could all just disappear.

RIPE is a little bit different because it’s a community of its own, so it’s not going to be flippant with that, but I think the idea here was ICANN could also say there are certain elements of the unique identifier space that they could be in charge of tracking, just to make sure they're always around. Doesn’t mean they have to do the work, doesn’t even mean they have to host the data, although I think we say something about ODI in there. But it just means your job is to make sure those archives exist and they're accessible. I think that was the gist of it.

ZARKO KECIC: Can we say it that way?

ERIC OSTERWEIL: Yeah, I think that's totally fine. I was sensing there was a disconnect, so I have no objection to saying it that way. And then something else you said, but I forgot what it was.

ZARKO KECIC: [inaudible].

ERIC OSTERWEIL: Yeah, you and I are totally in violent agreement about DOH.

LAURIN WEISSINGER: There is now a text called Laurin proposal. Have a look, and maybe it fixes some of the problems. It is definitely shorter.

RUSS HOUSLEY: You brought back the "or bring into existence."

LAURIN WEISSINGER: This stupid copy and paste. I'm sorry. I want to note at the bottom I put a specific point on CZDS to kind of speak to why it is in here.

RUSS HOUSLEY: Why do you think this addresses Zarko's high-level point?

LAURIN WEISSINGER: I'm not sure it does. I really want to hear from Zarko if he thinks this makes more sense now. And to add, if it doesn't, he can say what else.

NORM RITCHIE: As it's written, your first paragraph you have there at the bottom, it says currently no such reporting exists, but this paragraph was talking about having a list of data sources and indicators. So that sentence doesn't apply. I'd just delete it.

LAURIN WEISSINGER: Happy to do that.

ERIC OSTERWEIL: I'm just kind of skimming it now. I'm not a big fan of rewriting things over and over again from scratch, because we've missed a lot of what we've put in the first one.

Part of what we were trying to say in the first one I think was that someone should actually come up with what these are, because you can't just say "DNS is important and I'll measure it, and that's the same as somebody else's measurement of it." It was to come up with a set of things that were important, that coming up with a set of measures is actually a task by itself.

The conducting the measures is a task by itself. The maintaining of corpus is a task in and of itself. I think what we just came to with Zarko was it doesn’t have to be ICANN staff doing all this work. It doesn’t even have to be inside ICANN’s shop if they can point at something somewhere and they can just ensure it'll always be there.

But I think making a very general statement without a lot of the specifics that were in the previous recommendation, it just runs afoul of my measurement perspective. You have to be specific, and I know you're trying to make it short, but I worry that making it short might make it too vague.

LAURIN WEISSINGER: Eric, I completely understand your point, it’s just that the previous recommendation is over a page long. I'm wondering if we can't somehow refer to that text in the report or something like that, make this a little bit shorter and kind of provide more information elsewhere. I see where you're coming from though.

ERIC OSTERWEIL: Yeah, I could strawman a couple of things that I think maybe some of which I probably said before, but probably a lot of them I haven't, which is there r lots of ways to skin this cat. Coming up with a set of – I think I heard people talk about findings, structure, prioritization, also talking about proposals on how to implement just as advisory statement.

There's lots of ways we can put stuff in there, and we could certainly excise things that say it’s really important to measure bla, and here's one way you could measure it and this is why it would be really important to measure it that way. That could be completely separate from "See section N that has the recommendation for this," and that way recommendation N could be like "Go do blah. If you want backstory, go to section C." We could do it that way, it's a lot more structured. But I think it's important for us to say why we're saying things. Where we do it, I think I'm not sure, but yeah, writing can be tough.

ZARKO KECIC: May I ask two questions? First, I totally agree that previous measurements should be accessible even after whoever is doing those measurements stops measuring that. But I don't know how. In that case, ICANN or somebody else should make repository of those measurements, which is also acceptable, but we should try that to be clear.

Another question, you're with RSSAC, and they're proposing a lot of measurements. Can you brief us what RSSAC is doing and how?

ERIC OSTERWEIL: I was appointed by RSSAC but I'm not actually on RSSAC. So I can't.

ZARKO KECIC: Can we ask RSSAC, use this meeting and ask them what they are doing and how? Because they have a huge list of measurements that will be proposed, I believe on this meeting, what I heard, and we should talk to them.

ERIC OSTERWEIL: Yeah, I think we can. And they also have a document series and we can read the RSSAC documents that they have as well.

ZARKO KECIC: it is available because it was under development in Marrakech and previous ICANN meetings, and we should sit with them and check. If it is available, that's fine. If it is not, just get information from them.

ERIC OSTERWEIL: Yeah, Russ, we want to try to get facetime with RSSAC. Do we have that on the calendar? Maybe we should have an engagement session with RSSAC. I think I hear a motion on the floor.

RUSS HOUSLEY: They have a 2016 document, RSSAC advisory on measurements of the root.

ZARKO KECIC: No, there is new, and there is measurement group within RSSAC and those are people we should talk to.

RUSS HOUSLEY: Go ahead.

STEVE CONTE: Thank you. I apologize if I lost where we landed on the conversation around the alternate roots.

RUSS HOUSLEY: We took it out.

STEVE CONTE: Okay, so it's in point two, and also the second bullet on the text below. It's the same information just reworded.

RUSS HOUSLEY: Laurin put it back.

STEVE CONTE: No, it's in the yellow section below that too.

LAURIN WEISSINGER: Yeah, so the yellow section and what I pasted on top is essentially the same. It's not the same, but what's on top is the stuff I tried to shorten in a functional way. This is why it's repeated.

RUSS HOUSLEY: We had originally said we didn't want to measure that because it wasn't ICANN's job.

LAURIN WEISSINGER: So this was still in there, so I assumed this was agreed.

RUSS HOUSLEY: That was a mistake. Take it out. Okay, we know we have to come back to this reprioritization. Is there anything we need to do now?

ZARKO KECIC: To agree if we are going to put recommendation in regard of DOH and maybe mention DOT, but DOH is more important.

RUSS HOUSLEY: So we do have one in the future section that talks about them. I don't know if that will satisfy you when we get there. I suspect not. Okay, page 76, cryptography. Seeing no hands, this one's good? Yes.

ZARKO KECIC: The first paragraph I see useless. That's normal, like telling somebody they should breathe.

RUSS HOUSLEY: Right now, the [DPS] includes, as I remember it, the steps for transitioning from one key to another, but only staying with RSA. It doesn't accommodate the transition between algorithms presently. We're saying go back and do the rest of the job.

ZARKO KECIC: Okay, let me think about that.

ALAIN AINA: That was the point, the DPS means mechanism on the algorithm rollover.

ZARKO KECIC: DPS should cover what is existing situation, and if you plan change, you should put how you're going to change from one algorithm to another. And since I'm n to aware that ICANN is planning to do that anytime soon ...

RUSS HOUSLEY: They've been talking about it for a long time.

ZARKO KECIC: Okay, but not actual work done over there. And what I'm trying to say when I said mention to somebody don't forget to breathe, it is normal procedure that before you do any practical change, you'll update DPS and provide how you're going to move from one type of algorithm to another type of algorithm.

RUSS HOUSLEY: I guess we're telling them to do it now. That's the recommendation.

NORM RITCHIE: Are the keys substantially longer?

RUSS HOUSLEY: Shorter, in the case of EC, much longer in the case of post quantum.

ZARKO KECIC: No, but your question is, what will be impact of key change?

NORM RITCHIE: Yeah, and it’s not just at the root level, it’s also going to impact [inaudible].

ZARKO KECIC: Exactly, and we come up with measurements and we’ll know what will happen at root.

ALAIN AINA: So as we said in the second paragraph, Zarko, I think maybe actually trying to say that there are two things. The DPS has a provision for key rollover. DPS will have a provision for algorithm rollover. But now, how do you proceed when you want to do algorithm rollover? That will be like saying that like we did for the key rollover, it requires some studies, developing the plan, etc. before you can implement the algorithm rollover.

So you will not put in the DPS that this is what you do in detail, but you should have a provision that for the key management here, it may happen that we change the algorithm and then when you're ready to go, like for the KSK rollover, there needs to be more work to be done, produce a plan with the community involvement, etc. This kind of thing. But there must be a provision on the DPS for that so that if you want to do that, you can organize, develop a plan, all these things before you can do that, because [inaudible] we are saying that the algorithm rollover is more tricky than the key rollover. So we need more and more analysis before we do that.

ZARKO KECIC: I'm aware of that, but if you have DPS, you are also aware that 8u have to change that and to put new stuff when you start working on something before you do exact change.

So you have to plan that change in advance and to put in DPS. And what we are saying here is, please plan, don't do change without planning, and please put in DPS, not change without updating DPS.

ERIC OSTERWEIL: Can I ask a clarifying question? Because maybe everyone's in agreement. Or maybe I'm misunderstanding. But isn't this just saying – yeah, I think what you're saying is, of course you'd have to change the DPS to do something, and I think Alain is saying you don't have to say it –

ZARKO KECIC: [inaudible].

ERIC OSTERWEIL: Right, and Russ said they've been talking about it for years. And I guess, is this maybe just trying to be a forcing function to say it's time to get out of bed and do it? Because you're right, someone should say it before they do it, and Russ said they've been saying it but they haven't been doing it. Maybe this is meant to be a forcing function. That's maybe what's going on.

ZARKO KECIC: I believe that there was more important forcing function, but old key signing key existed for ten years. What was in DPS, how long it will last?

ERIC OSTERWEIL: I would be very happy to have a root KSK rollover conversation, but I think everyone else would probably fall asleep or pull their eyes out or something. So yeah.

RUSS HOUSLEY: So, are we going to leave it this way, or what? Zarko, are you happy, or not?

KERRY-ANN BARRETT: [inaudible].

RUSS HOUSLEY: Okay. Alright, name collisions, page 77.I keep thinking we're getting closer to the goal line, and Laurin keeps adding text. It's like the document actually gets longer.

UNIDENTIFIED MALE: [inaudible].

RUSS HOUSLEY: There is discussions.

UNIDENTIFIED MALE: [inaudible].

RUSS HOUSLEY: You quit what? You mean you're going off to form a company to put your proposals together. No.

LAURIN WEISSINGER: So I did not change that bit, and I'm wondering about that, because this might involve policy, which means community. And I think it makes sense because the next thing is then us saying ICANN Org should do something to facilitate that. So you might want to add the facilitate somewhere.

KERRY-ANN BARRETT: I'm John Public for this one. ICANN Org should produce [inaudible] that characterize the nature and incidence? With a c?

DENISE MICHEL: As in peridocity, as in frequency, as in how often it happens, as opposed to the noun of the number of things that happened, as opposed to how often they happen.

KERRY-ANN BARRETT: I don’t understand this sentence.

DENISE MICHEL: Yeah. Trust me, I struggled with this one too. I had a lecture.

KERRY-ANN BARRETT: [inaudible] sentence isn't correct.

LAURIN WEISSINGER: I think this was Eric and myself said it’s –

NORM RITCHIE: I'm struggling with this one. I've read it three times now, I think, and it basically says, yes, name collision is an issue, SSAC’s looking into it, we should support them doing it. That’s kind of how I'm reading this.

RUSS HOUSLEY: My interpretation of this is don’t go forward with creating more gTLDs until that work finishes.

NORM RITCHIE: That would be a nice, short recommendation. I agree with that one.

RUSS HOUSLEY: That’s how I read it.

NORM RITCHIE: Too many words for that. I like what you said.

RUSS HOUSLEY: Yeah, it's at the end.

KERRY-ANN BARRETT: Norm, just confirming that your issue was resolved.

NORM RITCHIE: I still don't understand why we have that second paragraph then.

KERRY-ANN BARRETT: Can incidence be replaced with frequency if that's what we want to say? If the editor was confused and I was confused, anyone else reading it will be.

UNIDENTIFIED MALE: [Maybe the whole board's confused except the author.]

KERRY-ANN BARRETT: Except the two authors who are like, "It's a word!"

LAURIN WEISSINGER: I just say let's just go with frequency. I made a small change to the sentence so now frequency should make exactly the same sense.

DENISE MICHEL: We can have a discussion about language and the concept of communication over drinks later.

RUSS HOUSLEY: If we move the part about NCAP up, can we – otherwise, what's happening in the second paragraph is mostly a repeat of the first.

LAURIN WEISSINGER: I mostly agree, it’s just that ICANN community should implement a solution, and then we’re kind of saying ICANN Org should support or facilitate this, I would say through an independent study, that might make sense and then we can get rid of the rest.

RUSS HOUSLEY: That actually is a way to implement what I was suggesting.

LAURIN WEISSINGER: I wasn’t sure how much the team wants [to delay it.]

RUSS HOUSLEY: Eric, is there any chance you have a citable reference to shove in there?

ERIC OSTERWEIL: For name collisions?

RUSS HOUSLEY: [Dollar, citable reference.]

ERIC OSTERWEIL: Yes, I do. It was a peer reviewed paper that actually said the rise in name collisions in the new gTLD era [inaudible] right now.

RUSS HOUSLEY: Since you had something to do with that, I'm pretty sure, I bet you might be able to find it. Okay, is there anything else we need to do to this one? Heads up, Zarko, this is where DOT and DOH get talked about. Privacy section.

ZARKO KECIC: [inaudible].

RUSS HOUSLEY: I told you it was coming. I didn't say it was adequate.

ZARKO KECIC: Yeah, when I mentioned DOH, I didn't mean privacy, I meant different resolution of DNS.

RUSS HOUSLEY: I'm aware. That’s why I suspected you’d want to make a significant change here.

ERIC OSTERWEIL: Russ, would you like me to paste my citable reference in any particular document? I found 7354 of them and I just want to make sure I get the right one.

RUSS HOUSLEY: Yes, the one that's on the screen. If when you past it, it doesn't appear up there, you did it in the wrong one. Okay, privacy. Come on, Zarko.

DENISE MICHEL: He's reading.

ZARKO KECIC: I would just add, in privacy, name shortening, DNS shortening, we omitted that.

NORM RITCHIE: I'm a bit confused on this one. If we as a group have an issue with DNS over HTTPS, reading this recommendation doesn't convey that. It's kind of like saying it's okay.

RUSS HOUSLEY: Really, it just says that there is a privacy impact and it should be monitored and reported. That's all it says.

ERIC OSTERWEIL: Because I think we were struggling with how to make a statement that would fall within ICANN's remit. So I think that's why it may seem a little [inaudible].

RUSS HOUSLEY: What do you want to do here, Zarko? Zarko, are you letting this one go? Are you happy?

NORM RITCHIE: What if we put a line in there saying, "Without advocating for ..." We're saying ICANN should monitor these, but also without advocating for anything ICANN should monitor these. Suggestion.

RUSS HOUSLEY: My guess is that Eric wants the data so he can say why it's good or bad.

ZARKO KECIC: There is no anything good in DOH. Advocates are saying it is for privacy, ISPs still can follow where customers are going, even it is HTTPS, because of address in the header. And bad thing is if applications can do their own DNS on unknown DNS resolvers, entire DNS system will go down and we'll have huge mess.

ERIC OSTERWEIL: I guess it comes back to where I think we were a while ago, which is, how do we put something about that in a recommendation that's relevant to what we're supposed to be doing? And I think we struggled with how to say something that was sort of within our purview as SSR2. But just in talking today, one of the things that we're talking about is we have a concern about an initiative, and we at the very least don't want our community pushing forward on the development of it.

So I don't know how we could come up with a set of comments about – I don't know, we have a bunch of meta concerns that I totally agree with, I just don't know how to put it in this report.

ZARKO KECIC: I'll repeat what I said today before you came. We're a review team. we should raise concern and ask ICANN to do something. We are not here to propose how to do that. But our findings are that this is dangerous, this will change entire DNS system, which we have hierarchical root servers and we have TLD level, and we have second-level domain names. With DOH, everything will change.

ERIC OSTERWEIL: Yeah, I agree. And I could even pile on and come up with a bunch of other things in addition to what you said which I think are concerns about DOH. But one of the big problems I'm having wrapping my head around this is that for example, DOH is a resolver-side function. The authority, those managing the unique identifier space, don't get much say, if any at all, in whether clients are using DOH. That's why it's really hard for us to put a recommendation in place about it, because ICANN isn't in charge of anything about resolvers, validators or anything like that. They're all in the authority side, and DOH is very much a resolver-side function.

So I'm not sure how we put something in there except that there is a standards process that's being pushed forward by ICANN Org and we could at least – so maybe what we'd say is maybe we need a section that says here are some general concerns and we want to make sure that our community is not adding fuel to any of these fires, and then we could put DOH in there. But I'm not sure if that makes sense.

I hear your point, as review team we should raise concerns, but they do kind of have to be scoped, like within ICANN's remit. And I'm not sure resolution is.

LAURIN WEISSINGER: I think this is one where a lot can be said in the analysis section of our report, which should be in there and which should address these concerns. My problem is the same as Eric's, what do we recommend within the scope that's we can recommend things in?

So I'm totally for putting a lot of stuff on DOH and the analysis. I think that's really important. It's just I'm not sure what to recommend, like Eric.

ZARKO KECIC: I have no idea what to recommend, how to approach that, but ICANN is only maybe we can talk about few organization, but I believe ICANN is the organization which should work here. Yeah, Eric, you're right, that's resolver-side. But if application is doing – if I'm ordinary user and I don't know what application is doing, and that application is doing DNS resolving, not my operating system and resolver that I put over there, I don't have control. And I don't know where that application will end up. Nobody can track that because of HTTPS and there are a lot of dangerous stuff that may happen and will happen.

ERIC OSTERWEIL: I am thinking while we're talking. One thing we could do, and we talked a lot in the DNS abuse section about some of these second order effects and how they do relate to the management of the namespace. So maybe we could do something like that here too and say that we could suggest that the organization commission and publish analyses on exactly what you're talking about, the ways in which the use of the namespace is being damaged by this and we could sort of make it something that they have to do some analysis on, I guess. I don't know. It feels like that's the kind of thing maybe you've been telling us we shouldn't be putting in the recommendations. But that'd be one way we could address it.

ZARKO KECIC: In that recommendation, I would like to see what Russ is proposing: kill it.

LAURIN WEISSINGER: I would propose the following: let's think – not today, because we're nearly out of time, but tomorrow, about what we would write in the report about DOH, and maybe then with something on the page, with some analysis done, and some scenarios laid out, think of something to recommend which is a bit more than commission a report. Hopefully. Just my proposal how to kind of go ahead with this topic.

RUSS HOUSLEY: I'm pretty sure we haven't reached the bottom of this one, but I think it'd be good to move on. This one we're going to have a bloodbath on, I'm pretty sure. but at least it's short and concise. We'll see. Go ahead, Kerry Ann.

KERRY-ANN BARRETT: The only problem I have with it is "ICANN Org should summarize potential harms to individual consumers or infrastructure presented at DNS workshops that it hosts." Isn't that why they have these workshops, to present that kind of information? And we're already asking them above to do reports that would be publicly available. So that's the only part of the paragraph that's, to me, nonspecific, that doesn't add value to what's above.

Unless I'm wrong, what I gathered from that section was that we want them to start doing more specific engagement and topics which they do sometimes, but have it more structured, and ensure that that kind of engagement actually benefits what they're doing and the public at large. But that last sentence, I'm not sure them summarizing potential harms to individual consumers, business, or infrastructure, we've not used the kind of language before. So that sentence sticks out to me like a sore thumb.

RUSS HOUSLEY: [inaudible].

KERRY-ANN BARRETT: Just the last sentence. Everything else, I'm ...

ERIC OSTERWEIL: Yeah, I can't remember. It may have, but when I read it – I don't know if this clarifies, but when I read that, it's basically saying go and do the review of the above venues and present it at your own workshops to your constituents. Yeah, I'm not sure if that's what people are getting from it either, and just looking at it from your comments, it just occurs to me the recommendation's suggesting a review of these venues for their literature, and then focusing the reviews that they're done and presenting them at the DNS workshop or something like that. I think that's what it's trying to say.

KERRY-ANN BARRETT: If I was ICANN Org, this would be one of them I'd probably not do, [depending,] because we've given them specific actions related to getting data of public consumption, reports, etc. The academic research and stuff, that is good and needed. We spoke about it as a part of – like above where we said we need to reword, where you had the CZDS.

So to me, who from ICANN Org would be visiting these things, then sit down to summarize, then sit down to put it in the workshop? I can't picture a person within ICANN Org that would be doing that kind of shopping, sitting down and summarizing, unless they hire a researcher that that's their sole function. But I'm just wondering, it's not very specific for me to say, okay, what does this look like? Because there's so many I could be part of, there's so many I could not be part of, there's so much data I could then specifically identify as relevant for public summary. Is it every workshop they should attend?

So I'm just trying to visualize, is the benefit we want them to do is to ensure that they are part of the academic research [and stay abreast of] cutting edge findings from academia for the public and themselves, or is it that we want them to just attend these things and make sure that people know that they attend? What do we want from it?

ERIC OSTERWEIL: Look at this year's IMC proceedings, and you'll see that almost half the entire conference was about DNS [inaudible], and some of that stuff is very familiar, very well-known to people here, like there [was the best paper was given to a paper] about the KSK roll. So obviously, there's people here who know about that. But the point is, aside from that one paper, it's possible that a lot of these DNS papers would have been below the radar for a lot of the folks here.

But at the same time, the people that publish these works aren't always doing things that are relevant to this community. But if somebody is looking at that to see if it is the case, then for many years, people have been saying – there have been random papers [admitted] about DNSSEC and stuff like that, and some of them have been a little less palatable than others, and they certainly don't all warrant getting a lot of daylight put on them. But some of them do, and it'd just be nice to know that somebody from OCTO or something like that is looking at the proceedings to say, "Oh, by the way, there was a finding, it is relevant to us, maybe we should reach out to that researcher," or, "Nothing to see there this year."

This year was a bit of an anomaly with how many DNS papers were at IMC for example. It just happens that way.

KERRY-ANN BARRETT: That's why I'm asking, is our recommendation specific that we want ICANN to stay abreast of academic research?

ERIC OSTERWEIL: Just those venues.

KERRY-ANN BARRETT: What if the venues change tomorrow? [inaudible] I'm trying to say, we want them to go to just these five places for example and follow what's happening in these five spaces, for example.

ERIC OSTERWEIL: My two cents is that those are the top three venues for security and network – between measurement, etc. There's like maybe one or two we could add to that, and I think we can certainly add "And others" if you want. It doesn't have to be presumed to be this is the only list, but certainly any of those – CCR is a bit of an interesting one, but any of those are basically at the top of the tier. So that doesn't tend to change very frequently or very quickly, so sigcomm isn't likely to fall off the top of the tree, but this is sort of like picking the usual suspects.

KERRY-ANN BARRETT: I get that, but are we asking them to assign – so let's be specific. Are we saying ICANN should assign someone with the specific responsibility to follow the trends arising from these specific conferences? Like be very specific because for me, it's still – ICANN should track, and then these reports should include, and then we're having them summarize the potential harms. So for me, it's not very ...

ERIC OSTERWEIL: So once a year with the exception of CCR. Once a year, each of these has a proceedings published, and they have a meeting. And at that meeting, people present the works that are in the proceedings. So once a year, someone has to look at what the proceedings were, go and read the papers, the ones that are relevant, and decide if they're worth summarizing.

For example, probably just pick a number, like two years ago, sigcomm probably had nothing about DNS in it. So it would be a real quick [No op] there. And IMC is not about [inaudible] so lots of years, it has no DNS. So it's just like once a year, each of those venues publishes their proceedings, and there are a bunch of independent papers.

I'm not hard and fast, we're just fulfilling Russ' desire to have a bloodbath. But you did bring up a fair point, it's like in the grand scheme of things, this one might get ...

KERRY-ANN BARRETT: No, I agree that it's needed, don't get me wrong. So I agree, I'm seeing what's there, I'm hearing you, but what I'm not seeing on the paper is a very specific thing that can be delivered upon. So, to me, just [that's] how you explained it. Given that these institutions have X amount of reputation, bla bla, it is, "We recommend that ICANN ensures that someone is assigned ..." Be very to the point that first, the premise is that these are the standing workshops and the must-attend ones that have the top leading research on these things. We think that learning from that is important, and ICANN should ensure that it is ...

ERIC OSTERWEIL: So that's in the first sentence at the end, "And publish to the ICANN community an action report about any publications that are relevant. These reports should include either recommendations or situational awareness for the SSR-impacting changes, and contracted parties and other ICANN. So that seems like it's what you're asking about.

KERRY-ANN BARRETT: Am I the only one who – I get the point, but the rest of the sentence [inaudible] am I the only one? I get it, Eric explained it, but if I was to implement it, I'm just trying to make sure that when anyone else sees it ... If I was to see it on paper by itself without you talking about like this, I just want to make sure that when someone else reads it, it’s as clear as you’ve explained it. Maybe the last two sentences need to drop off and separate from the point above, because I don't know if that’s what's – I think if we do that, it may be better. The other two, I'm not sure if they're as relevant as the first. I think the first, you have – like that’s the point. But when I put the other two with it, it seems like a run on and I'm not sure what's the run on.

I think if the last two comes off, it would make the point that he's making more clear. When [they're read] together, I think every time I listen to what he said, read the first sentence and then read the last two, it gets muddled to me again. If it’s just me, it’s fine. I'm not the best ...

STEVE CONTE: From an implementation perspective, whether or not this has a value, we’ll get to that in a second. From an implementation perspective, this is kind of scary. I know you said this is once a year, but there's at least six of them here once a year, plus reading I don't know how many papers on each of them. and right now, it’s explicit that there's an action report about publications that are relevant, which means there needs to be a review of each of those publications. That sounds like a lot of work to somebody. Is there value? Sure. There's value, and so I guess my question back to the review team, is this something that ICANN Org should be doing, or is this something that can be crowdsourced and ICANN community could be doing? Because we have industry professionals and leaders throughout the community, and if they're already at these or if they're writing or something like that, would it make sense to consider maybe a repository of something or some kind of – I'm going to stay with repository, where people from the community can contribute to the crowdsourced knowledge of this and flag instead of making the onus specifically on ICANN.

ERIC OSTERWEIL: Thanks, Steve. Those are helpful observations. This is exactly why I think it could potentially be very helpful for us to have strawman implementation advice, because it’s in there a little bit, but maybe it’s not explicit enough. But one thing you could do is for example say, hey, let’s reach out to NextGen and let’s pick one of those students and say, “Hey, it’s your job this year. You get a free ride to the ICANN community if you summarize sigcomm.”

And it even says in there, reach out to the program committees. They would probably love to come here if they knew this community existed. So that suggestion isn't necessarily to say someone from OCTO needs to read every paper from all those venues every year, but it’s like if we get too directive in our re cs, then it cuts the wrong way, like, why are you telling us how to do our job?

So if we have the ability to say, for example, you could do this. Like NextGen, get a student to do it. That's what I would do. Or B, go out to the program committee, the general chair for each of those and say, "Do you have any interest in sending someone to give us a sort of ..." Because like sigcomm, every year, has a summary of, "This is what is at this conference this year." It's like one or two presentations, they already have it. So you could reach out to them and they could come and do it. They might love it. And therefore, nobody spends any extra effort to do it.

But for us to say this is how you should implement this recommendation feels like that would get flagged as [dirty pool.]

STEVE CONTE: That's actually really interesting in an interesting way. Two things around that is we're looking for things that are relevant and SSR impacting. So if we're asking a student to do that, would they have the capacity to flag that level of impactfulness or relevance? And I'm not saying they won't.

And that leads me to the next point of, to me, this sounds like an experimental recommendation, to see how it works or if it works, and if so ... So if we look at this from an experimental perspective, can it be worded as such that if it's tried and isn't successful, then that's the result of the experiment and yet the recommendation has still been implemented for the next SSR review team? Does that make sense, what I'm saying?

ERIC OSTERWEIL: I guess I'm a big fan of experimentation so I want to agree, but at the same time, I think this is really just about ensuring that the community has enough situational awareness, especially in places it may not normally be used to looking. That’s it. But yeah, I get your point. So I'm not going to go anymore on the [map] for this.

DENISE MICHEL: I think we can address that more specific idea in the next iteration of these and when we get into filling out implementation, metrics and things like that.

KERRY-ANN BARRETT: But I think it’s important to note the examples that Eric cited, because that is far more clear, because I think every time I saw this, [I just said,] “Okay, who in the world they're going to hire to sit in ICANN to do all of this?” Because some of them are either happening at the same time, not happening at the same time. It’s something to track. So just to make sure that whoever is doing it – I think the examples would help. We can put it as a public comment, and when we clarify, we can go back and fix it.

ERIC OSTERWEIL: Yeah, and a lot of the measurement stuff they were talking about before, it’s the same thing. They probably sound a lot heavier than at least I was imagining a lot of them being, but it’s hard to not seem directive when you're giving an example of what you mean. So I don't know if we want to figure out a way to say examples –

KERRY-ANN BARRETT: [inaudible].

ERIC OSTERWEIL: Yeah, because this one, to your question about students, honestly, I think you try different students and some of them do a good job, some don't. You hope that good work gets around on its own anyway, and just the prospect of students talking about it is enough to just get it in the water. And then it basically evens out over time, would be my response. And also, we could lean on the NextGen pool if we don't like something, but I'm getting used to student labor.

RUSS HOUSLEY: Okay, I'm not seeing any more hands.

NORM RITCHIE: Well, one comment. This to me seems like something that should go in the suggestion box, not in the recommendations.

RUSS HOUSLEY: Move the whole thing?

NORM RITCHIE: Yeah, that'd be my take on it. I understand the benefit of this, but there's things like Google Scholar, you can use it to do searches on papers. You type in one keyword, boom, done. So I'm not seeing this as in the same class as our other recommendations.

ALAIN AINA: Yeah, I agree with Norm, and I think this goes back to Laurin's suggestion that when we are writing the report, we find places for some of these things.

DENISE MICHEL: I think there's some important impetus behind the suggestion. Part of it comes out of what we've seen as quite a big disconnect between the circles that ICANN and ICANN staff are moving in and what's happening in different places in the real world with some important impacts on DNS and areas of ICANN's responsibility without ICANN engagement. And I think we can all come up with different examples.

So this very much fits into trying to instill in a number of different places within ICANN a stronger connection and awareness and understanding of current real-world SSR problems and potential solutions.

KERRY-ANN BARRETT: I understand what Norm's saying but I agree with Denise that bringing in the perspective of relying on research to see what is coming – it's in future challenges right now, so I think when we look at prioritization and where we reallocate the recommendations, it should probably flow and follow close after the metrics just to kind of show that there's a relation in not just measuring what exists but actually looking at some of the future topics coming up and what the trends are that persons are actually observing from the industry. I don't know if that – because for me, that's how I can see them benefiting from making a reiterative process as they go forward.

ERIC OSTERWEIL: Yeah, I think the idea when we get to prioritization of what's more important than something else could wind up being beauty is in the eyes of the beholder. I think we could wind up with a difficult task trying to come up with a prioritization scheme when we're not going to be doing the implementation or even know what the implementation is going to be.

The other way to look at it is shortest job first scheduling. Yeah, this is low priority but we can bang it out by just putting a student on it, so we adopt it. Or that's so low priority we won't even look at it, is where you get a priority inversion. The lower priority things that are totally doable and would contribute a lot by being done are at the lower priority, so they never so that's priority inversion.

And I'm just sort of speaking generally, putting these thoughts out there as we're starting to think about the final report. Some sections about strawmen, direction, maybe pushing back against outright prioritization. I certainly am concerned about early optimization and shrinking the number of recommendations based on the corpus size before we know what we're actually recommending.

DENISE MICHEL: So Norm, how strongly do you feel about this? And Alain, do you feel like it meets the ...

NORM RITCHIE: No, I don't feel strong. Like I said, it's not a hill I'll die on, but it just doesn't seem like in the same category as some of the other recommendations, and some things are probably not there, like future in challenges such as a discussion on DOT and DOH and stuff. So I'm just ...

DENISE MICHEL: Yeah, so we haven't really addressed the prioritization of all of these recommendations, and I think that's an important next step for our work. And I think some additional conversations and suggestions will hopefully come out of this week that will cause us to make changes as well.

Do you think it's worth moving forward as a draft recommendation just for discussion with the community? Some of the other recommendations that we had in there, I also feel are much more important than this, but I certainly see the value of this long-term.

RUSS HOUSLEY: I'm trying to figure out a way forward given what we just said. I'm hearing a recommendation to move this to the suggestions. That's seems a way to reduce its priority even more so than putting it in whatever lowest priority bucket we come up with. Is that really what people want? That's what I'm trying to understand.

NORM RITCHIE: Okay, so if we're going to prioritize these, leave it there for now and we'll decide at that point.

RUSS HOUSLEY: Okay, so for tomorrow, we found several of these had writing assignments that needed to happen in order for the group to make progress tomorrow. My memory is that they were in the compliance section. You took notes? Great.

HEATHER FLANAGAN: I took them in one place so I could see that.

RUSS HOUSLEY: Thank you.

HEATHER FLANAGAN: The biggest one was the compliance and contracts, working on that, the subteam or whatever subteam members could be gathered were going to work on that one. We needed to come back to DNS testbed. Zarko and Laurin were going to talk about IANA portal. Root zone data, that seemed to still need some work where we wanted to pull the findings out, and that was up to me. And a question about writing something for the DOH and DOT workspace and whether that goes in the future section.

RUSS HOUSLEY: That was five.

DENISE MICHEL: Are compliance and contracts one or two?

RUSS HOUSLEY: Two. Six. I kind of like to self-select, but at this point I think what we should do is adjourn the meeting and then pick the teams that you want to work on to have that so that we have the raw materials we need for the morning. Does that make sense? Anyone have a better idea? Okay. Yes, Negar.

NEGAR FARZINNIA: Just want to note for everyone's attention tomorrow the meeting is in a different room. It's not in this same room here. The meeting will be in room 517C.

RUSS HOUSLEY: The agenda that was sent out, so it's 512G. Did it move?

NEGAR FARZINNIA: The agenda that I have has a different room, but we are checking right now to verify, because on the schedule, it's also a different room.

DENISE MICHEL: Because we're in E, and that says G, and that says something else?

RUSS HOUSLEY: Yeah, that's what she's saying.

NEGAR FARZINNIA: Okay, so we've confirmed with the main agenda is in 512G, so next door.

RUSS HOUSLEY: Good, because I was like, wait.

NEGAR FARZINNIA: Still a different room, just next door, not all the way ...

RUSS HOUSLEY: The last thing we need is to be in two different places.

UNIDENTIFIED FEMALE: It's correct in the calendar invite in your schedule.

RUSS HOUSLEY: Okay. Steve, you look like you want to say something.

STEVE CONTE: No.

RUSS HOUSLEY: Okay. Alright, so let's adjourn, and break into the groups to work on the text we need for morning. Thank you.

NORM RITCHIE: I had Archer quotes floating in my head, Russ. M as in Mancy.

[END OF TRANSCRIPTION]