EMILY TAYLOR:	Good morning. We're going to start in a couple of minutes. I'm sensing that some people haven't finished their homework from last night, and we've got some issues with the Google Doc. So we could just use a couple of minutes to finish that off, speaking personally.
	So good morning, everybody. I'm not sure whether we've got – who have we got on the Adobe Connect who is dialing in? Ram Krishna, Matogoro. We've actually got the Adobe Connect up on the screen, so I hope that we'll be able to spot your interventions a little bit earlier in real time. Just a request to the team members: if you do see anyone waiting to make a comment and I haven't noticed this morning, please just draw my attention to it.
	You've got me this morning, Eric this afternoon. It's kind of down to business day today. We've had a lot of listening. We've had a lot of briefings. This is I hope, and speaking to many of you after and during yesterday, I think a lot of people are hoping that we will come away from today's session with concrete outputs and concrete product which will give us confidence to move forward.
	This morning, James is going to lead a suggested approach to how we get our work into manageable chunks, I would say. Thank you very much, James, for volunteering to do that. After the break, we will then develop that into a work plan and timeline. My suggestion for that is that we break into two smaller groups and just hammer away at it and then come back into the Plenary and share the product of our work.

After lunch, we will continue again with planning, looking at discussions around subgroups. I think now having discussed with the co-Chairs and several of you yesterday, I think although this is subgroup discussions, we should also have a thought, look around the room today, look how many people are in here. How feasible is it to have many subgroups? We should be thinking about whether this is a good idea and whether we can go into subgroups. For sure, that's a very tried and tested way of moving forward. There are also other things, and I think that we're not a big team if I can say that. I think we should think about what is going to be feasible to move our work forward without everybody doing everything but equally maintaining some sort of manageability.

Then another very important aspect that we will be thinking about this afternoon after the break is about our outreach. All of our proceedings – these meetings, our mailing list – are available to the community. We have and we welcome observers, but there are also aspects of the community that need to be more consistently engaged in our work. And this is an opportunity to look at what we're currently doing but also identify who we're going to reach out to, why, and when, I think.

Then we've got some wrap-up time later in the day where we will just sort of nail it. But my personal hope is that we will come out of today with a work plan that we can all understand what is expected of us in the next week, in the next few months, and the next level of deliverables. I think that if we can leave Madrid with that, we will really have set ourselves up for success.

With that, James, I'd like to invite you to take the floor and lead the next session. You've got until – I think we have – Jennifer pointed out that

there's a ghost half hour in the agenda, so although this says 8:30-10:00, we're not due to break until 10:30. Let's see how we go, James. We could aim to stop at about 10:00. If you need a little bit more time, we can take that. Okay, thank you.

JAMES GANNON: Thanks. I'm going to preface my entire thing with I was up working until 3:30 a.m., so please forgive me if I'm unintelligible at times. Next slide.

Probably a week or two ago now, I was looking at where we stood and I've been around a lot of working groups when they're in their start-off phase and it can be a little bit difficult I think to get out of the admin and into the substance. It's a pretty big wall to climb over at times. We have a huge amount of work ahead of us in a lot of different areas, and we have a lot of different experiences around the table. I think it's important that we get to a point where we start scoping out our work and bundling it up into sets of tasks that we can start working toward.

The project manager in my head has a process that I go through when there's a piece of work before me. For me, I start off with scoping the work and move on to assessing it. Then you do some design or development, and then you implement it. So in my mind, what we're doing now and what we've been doing over the last few days I think as a team is that scoping piece. We've had discussions about where we fit inside ICANN's mission and everything else, but I think we're coming to conclusions on, which is excellent. So we need to start moving into that assessment piece where we start actually writing down on paper: what is it that our goals are, what topics do we need to address, what do we

feel are the burning threats to ICANN that we need to start looking at as a Review Team?

With that, I started off with let's go back to the Bylaws. This is something that we're pretty familiar with at this stage. We have a couple of key areas that the Bylaws actually give to us. Within our discussions, we've touched on more narrow issues, and I think it's an important piece to then map then back to where they fit into the Bylaws. Because at the end of the day, we are bound by them. We can look at gathering information outside of those, but within the regards of what recommendations we make that's our key mapping that we need to do.

I'm not going to go through these. I hope everybody has read them at this stage. We have our "shalls" that we have no choice over. That is our mandate to do. Then we have a couple of "mays" as well that I think a lot of us think are very important and we also need to spend our time on.

Then that brought me along to – and I'm sure you're all sick of me talking about it now – the CWG and CCWG work that I was involved in. It has been the primary thing I've done at ICANN for the last three years or so, so I've taken a lot of learnings from that.

What I did was I went back and looked at the method by which we broke into sub-teams or design teams. We had various different naming for them in those two groups. I took the framework that we did and mashed the two of them together and came up with a bit of a subgroup structure that we might consider.

First of all with those is you need to lay out the principles of how you're going to structure those subgroups. As Emily said earlier today, we're a very small team. If you compare us to a standard ICANN working group or the CCWG or many of the activities that go on in ICANN, we're a quarter or a fifth of the size but we still have a huge amount of work to do. So if we allow ourselves just to go off and Kaveh thinks that this subgroup should be done with [arenas] of one narrow thing and Emily thinks that there's another one that should have just this focus because that's what she's interested in, then we'll quickly become very unmanageable.

I want to go through these. And as we go through, I would appreciate if people gave me feedback on what they feel about these principles. Because these are my strawman, and strawmen are there to be pecked at and to be torn apart where necessary.

First of all, I've proposed some subgroups. They are primarily my own areas of interest and what I think the team should be working on. So the very first principle that I wanted to put down there was that we can have additional subgroups. Also, I wanted to give us some flexibility in the future that if Subgroup 2 or 3 as they're progressing through their work discover something that they feel is a very important topic that needs to have more focus on it, then at some point there must be a process there to bring back the subgroup to the Plenary and say we found this issue that needs a lot more focus, "Can we have an additional subgroup to go look at that more narrow niche issue because it's actually something that we think is more important than we may have thought of at the start."

To give a bit of time bounding to our starting on the substantial work, I put in a line saying that at least the structures and the broad activities of the subgroups, I would hope that we can agree on those here in Madrid. We don't get much face-to-face time, and breaking out work into this type of thing can be a little bit contentious sometimes because different people have different areas of interest and what should be focused on. What topics need to be mapped up into subgroups can be something that is much easier to [back it] face-to-face. Here where we can look at people and interact properly is a very valuable time to do this type of work. So I wanted to give us a goal of getting this done with regards to structure, maybe not finalized but very progressed along these lines, by the end of this meeting.

"Sub-teams will be populated by a call for volunteers." Once we have the structure and the topics of the subgroups, the members of the Review Team will need to sit down and work out based on, number one, their interests they feel they have an ability to contribute to and their own personal schedule and everything else. Then they can decide, "Okay, I'm going to start off with these three subgroups that I'm going to try and participate in." It's important to note that, obviously, participating in more than one subgroup is not just encouraged but I think will be required for us to get through our work in a timely fashion.

"Sub-teams will be comprised of a minimum of three members." That is to give a little bit of balance. We want to avoid situations where we have one or two people running an entire subtopic by themselves, both from a balance of viewpoints point of view and also from a workload point of view. We are supposed to work collaboratively here. Again, we're a small group. We all need to be really picking up the pen and

doing work here. Every single one of us will need to put in hours on this. We all knew that when we signed up for the call for volunteers. This is the point I think where we're really going to start kicking off on getting that workload and getting some work done.

Please stop me at any point if anybody has feedback.

"Sub-teams will be required to appoint a rapporteur who will act as the penholder and guide the sub-team through their work." I want to spend a little bit of time on this. When we break up into a sub-team structure – again, this is based on my previous experience – even in a smaller group of four or five people you will still need somebody to sit there and hold the pen for the drafting. Usually what these subgroups will come up with will be some text to hopefully eventually be presented to the Plenary and to be brought back into our final document. But even within those small groups, you will need somebody to sit there and act as a mediator and act as somebody who is collating all of the feedback from the members into the contribution document which will come back up to the Plenary.

That person will also be responsible for reporting to the Plenary on behalf of the subgroup. So that's an important point to note. These subgroups will not be, I suppose, empowered to finalize their own decisions. So everything that a subgroup does will be brought back to the Plenary to be read by the Plenary and to be confirmed by the Plenary as the opinion of the Review Team as a whole entity. That gives those of us that might not participate in certain subgroups the ability to have that second set of eyes on the work and make sure that we're all on the same page.

Because at the end of the day, the final work product which will be our set of recommendations on our report is a report of all of us. It's not just an amalgamation of the subgroups. It's something that we will all be representing and we all need to be behind. It's an important part of the process of when we break down into any type of smaller groups – be it subgroups, be it design teams, be it just smaller groups of people working on things – we will always need to make sure that we bring those work products back to the Plenary for confirmation that, yes, we all agree on this.

The next one is pretty self-evident. Once the sub-teams have been convened, the onus will be on the rapporteur to get that work kicked off and to really drive that sub-team to completion of that as quickly as possible. The idea would be that potentially we may have some rapporteurs appointed during this meeting, and they are then empowered to go off and start that work as soon as the members involved are available.

I'm going to take a note to take out "report back to the full CWG" because that's obviously where I've copied and pasted this. And then the reporting back of the sub-teams: particularly for some of these topics, the sub-teams are going to be working for a while. We're talking month-long processes here. It's important that we define a callback process for those sub-teams to be reporting back, even if it's just on progress. Not necessarily on presenting stuff to the Plenary to be confirmed but saying, "We have met with X, Y, and Z stakeholders, we've met with this person from ICANN staff. Here is our current progress. We're on track, on time for delivery by the date that we have agreed within the work plan."

It also gives the Plenary an ability to see where we may be stepping on timelines. Again, coming back into the project manager in my head, if we have ten subgroups, all ten of them will not necessarily deliver on time. We need a mechanism to be able to track and make sure that one subgroup may need additional assistance, it may need additional members. If we see something is holding that subgroup up, we need to be able to remove those blockers from its progress. So that reporting piece is going to also be very important.

And we should have a mechanism somewhere maybe on the wiki or some other method of tracking where the subgroups are keeping their status up-to-date so that the co-Chairs and staff and anybody that's interested in making sure out timelines and everything are tight are able to keep track of the progress of the substantial work that the subgroups will be doing.

And then the very last thing is if accepted by the Plenary, the agreed language that the subgroups will come up and potentially the recommendations or potentially any suggestions for comments to go into the report that the subgroups will be agreed. And hopefully, that will be the structure by which we build our report and our recommendations. That these subgroups will be able to focus in on the [quite ordinary and narrow] issues that we need to address. We also have broad strategic issues that we'll be looking at as well, which may span multiple subgroups, for example. But a lot of the heavy lifting can be done by these subgroups and then brought back to the Plenary in a cohesive fashion that will then build a document that we as the Plenary for the final period of our work will then be able to tweak and edit and make it into a bit more of a narrative to bring everything together.

EMILY TAYLOR: James, you're going on to the next slide, but I just wanted to pause there and ask for reflections back from the team on what we've heard so far.

As you said, James, these methods have been developed successfully in other contexts, so we should adopt things that have been learned by the community at large where they're going to work for us. But as you said right at the beginning, we're a small team compared to the very, very large teams.

I've got Alain asking for the floor. Anybody else like to contribute at this stage? Raise your [hand]. Any questions. Anything that's not clear. Anything that you would like to comment on. And that goes for those joining remotely as well. Alain, please go ahead.

ALAIN PATRICK AINA: Thank you. For the sub-team work methods, I'm just thinking of when you have a sub-team or subgroup during the group's work they may need some document or they may need some briefing from staff or from another community. When this is needed, shall we keep it at the subgroup level or open for the team at large?

This sub-team says, "We want to hear from the SSAC because it impacts what we are doing." But we allow the whole team to follow this [session]. Same thing for documentation. A group may request a document for a specific work. One aspect of doing it: keep it for this group. Do not disturb the other people. But it may also be good to share

the document for everybody to have the [inaudible]. So where are we headed? Do we keep everything at the group, or do we when possible make sure the group at large is aware?

EMILY TAYLOR: Thanks, Alain. I think you raise a very important prior issue that when you split into smaller teams and groups there's a very important piece about keeping the larger group connected and in touch with your work without overburdening everybody. Rather than effectively creating a bazillion smaller little teams that are just independent and go off and do their own thing, it's that sort of keeping in touch.

James, do you want to respond? Then I have Cathy. Anyone else? Please go ahead, James.

JAMES GANNON: Thanks. Yes, it's a fantastic point. On the fly in my head, yes and no. For normal day-to-day requests to staff or requests for basic non-confidential documents from ICANN or anything like that, I personally would suggest that that can be rolled up into the reporting mechanism. If we're using the wiki or whatever else for a weekly or a monthly update, we can have a section in that for documents requested or staff resources, staff briefings requested. Basic, normal, day-to-day things that will come up in the course of the work of the subgroup.

If, however, there is – I have three potential scenarios that I can think in my head that I would like as a Plenary member another subgroup is bringing up that I would like to know about. Number one, if a subgroup

was requesting a document under the confidential disclosure framework. Something that is known as confidential [internal in] ICANN, I think that would be something that the Plenary would need to know about.

If the subgroup was requesting work to be done at cost by ICANN – for example research or contacting an external provider to give data into the work of the subgroup, something like that that there is a budgetary implication for – that's something else I as a Plenary member would like to know about.

The third situation would be if there was a blocking situation within the subgroup where there is a resource or a document – let's take a hypothetical that the subgroup wants to talk to David Conrad, but David for six weeks is super busy and isn't able to make the time – then that would be something that I would think needs to come back to the Plenary for that reporting piece of here is a resource or a document or something that we need but we're unable to progress our work. We're going to an amber status now as our subgroup and here is why.

Yes, I am a project manager.

EMILY TAYLOR: Very good. I've got Cathy and then Boban.

CATHY HANDLEY: Since you are a project manager, you probably will be able to answer this. In the past, have you tried standing up sub-teams at different times? Like you have the immediate need and a long-term need and

perhaps activity on sub-teams comes and goes. Does that work out pretty well?

JAMES GANNON: Thanks. Yes, on CWG – and Bernie can give some feedback on this – with the design teams we kind of ended up doing that. We had ones that started, and then there was a bit of a rolling period where there were new applications, and then we had ones that started later on in the process. I will admit, it's not the most efficient way to work. If you can do your scoping in advance and work out what your sub-teams need to be at the start, if you frontload that work, you can do your scheduling much easier and you're much [more] likely to keep it under control. But I would suggest we still would need a little bit of flexibility where there is a genuine substantial issue found by another sub-team after they've started that needs its own set of focus.

EMILY TAYLOR: Cathy, did you want to follow up?

CATHY HANDLEY: Thanks. I'm thinking more along the lines of the list that you put out. Maybe in order to get some things done, there are sub-teams that need to go immediately to address some things. There are other sub-teams that maybe we need to make some progress [in] other areas because it's not as urgent given that maybe you'll be going from a lot of different places for information. So you're just accumulating things. The sub-team isn't actually doing much.

JAMES GANNON: If I can come back on that. You will notice that there is nothing in my proposal that says when they have to start. Bearing in mind the resource constraints we have as a small team, I've intentionally not really put that in so that if there are items, and if there are entire subgroups, that we feel can wait a period of time before starting so that we can focus on other issues, I would hope that – I had intended to write in that amount of flexibility into the structure there.

EMILY TAYLOR: I have Boban, and then Ram Krishna has raised something on the chat.

BOBAN KRSIC: Thank you, Emily. James, I like and appreciate your approach because I have a lot of experience in different working groups also with [ten to three] people who were working there and we'd produce a lot of documents in the working groups. And at the end, it's always the same. You will have two, three volunteering people who have the drive and to push the whole thing forward to finish it.

We have five sub-teams [inaudible] and I found my domain at the second sub-team, so I said, "Okay, let's do my homework and finish it." I think we will need at the end three people at the minimum per sub-team. So 5 sub-teams, 15 people – we are 15 – so it's a tough goal here. Maybe we can split it only in three sub-teams to put some topics together and maybe our co-Chairs can at the end put the [inaudible] together and bring it to the plenum. Because I think it's a lot of

administrative work which we have to do if we have a structure with five teams and there are some who have the pen and to report it and then we have co-Chairs, and we are only 15 people. So I would propose maybe to split it at the end in three teams, to put topics together, and hope that everybody finds himself on one sub-team.

EMILY TAYLOR: Thank you, Boban. James, did you want to come back? Can I also add to your comment? Let's also be realistic here. We have 15 people, and at any one time maybe a third of us will be so busy with our other jobs that we will be unable to give this project the time that we would like to. So I think that's something to factor into our five sub-teams thought experiment. James?

JAMES GANNON: It's a lot of food for thought, and my brain is starting to churn now. Totally on the fly, there is nothing stopping us from, for example, choosing three – we're going to get very clichéd now – thematic areas. For example, we could have a strategy group, a technical group, and a policy group. Then within those groups, we could have focus on what I currently have as sub-teams, we could focus on those areas within those groups.

I still think we need some concrete mechanism to map the issues that we need to investigate to people. What way we do that and how we structure that from an administrative side to be honest for me as long as there is some structure, I would be pretty ambiguous as to which one we would go for as long as we have something concrete there that says

Person A, B, and C are responsible for delivering this piece of paper to the Plenary.

EMILY TAYLOR: That's great. Thank you, James. I'm going to read out Ram and Matogoro's comments if I may for the record. Ram Krishna has said, "Subgroup concept is good. My recommendation is that we include at last one member from each region so that it will be easy to outreach with community and it covers all five RIR issues also."

So that's one piece. That is an alternative proposal to your thematic groupings, James, is a sort of geographical groupings. Or maybe they're both together. Would you like to take that first? Alain?

ALAIN PATRICK AINA: No, [inaudible]. James go first.

EMILY TAYLOR: Why don't you go ahead, Alain? And then we'll come to James.

ALAIN PATRICK AINA: Okay. I can see, Matogoro, what you want to achieve. I don't think this is a good idea to do geographic representation.

EMILY TAYLOR: It was Ram Krishna, just for the record.

JAMES GANNON: I understand the drive, but I would flip it on its head. We are not going to be appointing people to subgroups. The co-Chairs or any of us, I'm not going to turn around and say, "Kaveh, you're going to work on SSR1 Implementation Review." It will be the other way around. The members will put themselves onto the subgroups. I would challenge all of us that if there is a topic that we feel that there is a regional component to and we want to make sure that our regions are represented within those subgroups, the onus is on us as members from those regions to join those subgroups and make sure that our regional views are included in the work of that subgroup.

That will mean there is a lot of work for some people if we want to make that a requirement. I don't think it's feasible for us to make it a requirement. But for those of us, particularly the members from underserved regions and, yeah, there are topics of regional diversity and regional input into these sub-teams and, unfortunately, those members from the underserved regions will have a lot of work ahead of them to make sure that those views are incorporated.

EMILY TAYLOR: Can I also read Matogoro's comments for the record? "I would not recommend subgroup, rather have topics that may be divided to some members and report back to the team once deemed important. Maybe James can tell us how many members were in the CWG. We might adopt something that worked very well for a certain community which might not necessarily work for this group." That's a question. Thank you.

JAMES GANNON: I'll go first, and then I think Bernie will probably follow up. To the first comment on dividing topics up into members, that's essentially what the proposal is. We are calling it subgroups, but the naming of how we do it is not very important to me. The goal here is to map those topic areas to people and to start working.

On the second point, I will let Bernie do the exact [push]. On the design team that I led and on a number of the other ones, we usually had I think seven to eight people sign up and on that usually three to four were pretty active. I know there were some larger ones, particularly on the CWG, due to some of the bigger issues. But I think the majority of them were under 15. I'll let Bernie follow up though.

EMILY TAYLOR: That's a number, not age, right? Okay, Bernie?

BERNIE TURCOTTE: Thank you, Emily. Yeah, I designed that methodology for the CWG. But one thing to keep in mind, probably the effective comment here, is that we had sliced up that work into very, very clear chunks. Very precise, very small, very focused, and we used that approach because of that.

We were a much larger group. The CWG at a regular meeting had at least 50 people showing up, and on its list it probably had closer to 100. So different times, different spaces. Uncertain how we would clearly map that out to here, but one thing that is certain is when we were using that for the CWG – I'll hammer this again – it was very, very boxed

in, very clear what we were looking at, what the interest was, and what was to be delivered. From A to Z, it was spec'd out very clearly. I think that's one of the reasons that that approach with the very small groups worked out.

To get back to James' point, there's always someone that starts writing the first draft. That's the reality of it. If you're going down that path, and I'm not saying the group has to, but if the group goes down that path – and I subscribe to Cathy's point that given our approach here we probably don't have the resources to start all groups all at once – and that if you're going to join a group we have to have in some terminologies we call it a champion but someone who is actually going to carry that water to get that first draft done.

Two final comments. The first one is staff is not there to write the documents for you, but we can really help. So there's a line in between there, and we are there to help and assist in a lot of ways.

The second thing I think is maybe let's not forget there is a budget. We talked yesterday about maybe spec'ing out some writers, but you may want to consider overall in your budget spending how you want to approach that because there may be areas where it may make sense for you to use some of those resources to get a specialized resource to look and deal with some points. Thank you.

EMILY TAYLOR: Thank you very much, Bernie. And also thank you to you and other members of the staff for sharing your experiences in other groups and what works and what doesn't work. It's really, really valuable.

You touch on a point that's been going around in my head, which is that we did decide yesterday that we would generate an RFP for one or I would suggest "or more" writers who can support our work. Eric? Thank you.

ERIC OSTERWEIL: Just in that one point just to interject, we shouldn't necessarily assume that we won't be doing any of the writing either though. Just to clarify because that presumption is to assist, but there will be places where we need to hold the pen ourselves.

EMILY TAYLOR: That's right. I think that we also have to be realistic about our capacity. When the page is blank, you have to get started somehow. Bernie is also suggesting that staff can and has in the terms of reference just get us started, we then pile on. There are different ways to do that.

James, you want to take us forward now?

BERNIE TURCOTTE: Thank you, Emily. It's Bernie. Just one caveat: we've had some experience with hiring writers to do some work. In theory, it's nice. In practice, it's something else. People who write for a living write at a certain level. I would say that finding people who understand our environment, understand what we're doing, how we're doing it, and what we want to get as an outside product at best is a mixed bag for the result. It's really, really hard.

We had a few people helping us out at some point on the CCWG Accountability, and basically it just didn't work out. That's the reality. It's not because they weren't good. They were really good writers. But they took a much higher level approach to it versus what the group was looking to accomplish. So just that warning, if you will.

The learning curve to get people up to speed so they can actually do that is not small. You may end up spending more time trying to get someone up to speed and in the frame that you want them to get to write versus what they will actually contribute to you. Just some warnings.

EMILY TAYLOR: Thank you. Margie? And then, James, I'd like you to continue.

MARGIE MILAM: I'd like to echo what Bernie said and share a perspective from the CCT Review Team. They invoked it's more of a copyreader/proofreader kind of thing at the end right before they published the report about a month ago, and that seemed to work okay. But the actual writing itself really did come from the team itself.

The other thing I wanted to remind you is that there is a budget associated with this Review Team, and obviously it's not unlimited. It has a defined scope, and there are procedures that need to be followed if we exceed that. So the question you might want to talk about is what kinds of other work might you want to use that money for.

For example, the CCT group did a lot of surveys to get a lot of data to be able to produce the report. I don't know how comfortable you feel with the data that, for example, you saw yesterday. Or you might find areas that you do want to actually do a survey or commission a study. That's the kind of thing that you'd have to balance the need for a writer versus additional data.

EMILY TAYLOR: Thank you. Cathy has just asked for the mic. Anybody else want to respond to that? Okay. So my list is Cathy, Boban, and James in the order that I saw people.

CATHY HANDLEY: This just kind of popped into my head. Going to work with James, Denise on something, but I'm assuming there are some sort of prerequisites that ICANN has and rules about sending out RFPs and all of that. Before we launch down this path of putting something together, would it be possible – I don't know who would do it – to throw up some place a direction? If you can get us the directions on what your parameters are for issuing an RFP so that we know while we're doing this what kind of challenges or what we're looking for please. Thank you.

EMILY TAYLOR: Thank you, Cathy. Could I just say on that I don't want to – we made a decision yesterday, so I don't want to – I think that's a very valuable

thing to do as long as we don't take it as "let's not do the RFP because we're going to do this" because it will take its own time.

CATHY HANDLEY: No. Simultaneous.

EMILY TAYLOR: Simultaneous.

CATHY HANDLEY: They can get the information.

EMILY TAYLOR: Thank you.

UNIDENTIFIED FEMALE: The other thing I wanted to point out just to follow up on that is that we don't need an RFP for everything. I have to check back with the finance team, but it's a certain threshold before it gets to an RFP. And I would think if you're going to engage with a writer, it's probably not going to rise to the level that you would even need an RFP. Certainly, you can do that if you want solicit people, but chances are you guys probably already know technical writers from your various backgrounds that you would just refer and go through a process to identify whether it would work out.

EMILY TAYLOR: Perfect. Thank you very much. That's really helpful. Boban and then James.

BOBAN KRSIC: To the [inaudible], if you had to provide [inaudible] documents or so on, it depends on the content. We have a structure. We have five topics in James's proposal. I would say for the first one, maybe it's enough to [ready] the documentation what we have. For the second one, we have to provide [interviews]. So it depends on the topic.

EMILY TAYLOR: Thank you. James?

JAMES GANNON: A couple of different points. First of all, I would hope that compared to maybe some other groups, particularly the big CCWGs or even potentially the CCT, our remit is a little bit more narrow so I would hope that we can work in a relatively structured manner. In my head, a lot of what we're doing here is risk management and [auditing] to an extent. These are defined things that are out there in the larger community as part of the world of ICANN. As long as we approach our work in a relatively structured manner, I would hope that a tech writer for us compared to a tech writer for example for the CCWG would have a much shorter learning curve. As long as we can present our own work in a structured manner, I would hope that we could guide a tech writer to be able to assist us.

Again we have to remember, a tech writer – and it was an important point that Eric made – they're not going to be doing our substantial work. They are going to be fleshing out our inputs, putting them into a more structured manner, making sure that the narrative flows within the document. They're going to be assisting us, not leading. That will never be the case.

EMILY TAYLOR:
And it would not be appropriate for that to be the case, however, I've also been involved in different contexts in teams of stakeholders who are busy, who meet, who work out the substantive issues and are supported by a team of writers. So there are different ways of doing it.

James, with that, why don't you continue? If you have other material, take us to it and we'll continue our discussions. Thank you.

JAMES GANNON:
Thanks. First of all, there's a really high-pitched whine from the speakers that I would appreciate if we could get rid of because it's actually giving me a headache at this point.

What I'm going to do now is I'm going to walk through the subgroups that I've identified and how I would like to structure at least the identification of our areas. Take the topics as suggestions, but for the format that you will see I'll bring you through which is linking topics back to the Bylaws, for example, let's make sure that we put some structure around whichever way we decide to go down. Whether it be many small subgroups, one or two big subgroups, let's try and put some

structure around why we present the realities of why we are building these subgroups.

I will go to this one, which let's take this one as pretty much a given. We will have some form of group that is going to review the implementation of SSR1. This is the type of way that I would like just to approach breaking down our work and making sure that we have a clear link to why we are identifying this set of work. What type of area it fits in, in this I put it down as "Skillset."

Particularly for the newer members to the ICANN world that even if you don't know what this specific topic is – we could go down some route to do with the DNSSEC implementation within PTI – you might not know exactly what that is, but at least if we lay out that it's related to PKI and risk management and cybersecurity, you as a newer member or somebody who might not be familiar with the specifics can look at it and go, "Okay, well, if it's in that topic area, I can probably have something to contribute."

So I'd like to make sure that even when we start breaking down into smaller, more narrow areas that perhaps some of us around the table are much more familiar with than others that there is still a link back to the broader area that it sits under.

Then we clear "Description of Activity" that the subgroup is going to work on. For this one, again, this is a pretty good example of something that we can clearly take from the Bylaws and this is pretty much a copy/paste I believe that I did.

Then the next part under it is the "Work Items." This is where there is some discussion to be had on how we identify the specific work items that a subgroup will take under a topic. There are two ways that this could be approached.

This could be done by the Plenary in a session like this where we say, "Okay, what do we feel as the Plenary the subgroup SSR1 Implementation should be looking at?" and break down some specific work items that this group will then take away and work at.

Or you can flip it on the other side and say, "Who is interested in working on the SSR1 Implementation review? Okay, you guys go have your first meeting and work out your sub-items and then bring that back to the Plenary for, yes, we all agree that that's what you should be working at."

That's something that if people have opinions on, I would really like to hear some feedback on. I think that regardless of what structure we go to break our work down in, there will be a level that we will get to as we go down the chain that the day-to-day work items will need to be agreed. And we would need to make a decision which side of the fence that falls on. Is that something that the subgroup agrees themselves, or is that something that the Plenary instructs the subgroup to go work on?

If anybody has feedback on that, that would be interesting to hear. I'm ambiguous either way, just for the record.

EN

EMILY TAYLOR: Does anybody have any feedback that you'd like to share? Alain?

ALAIN PATRICK AINA: First thing I have with what you presented is I see the [method], the approach you are using, but as you just said it, it is [of] looking at the topic directly by a sub-team. It may be good to look at the topic like review of the SSR1 implementation and then we decide if the whole matter is going to be for a subgroup or is this a subset of it which needs to be delegated to a subgroup. But here, it is presented as it's going to be for a sub-team. So this is the first thing.

The second thing is I think I agree [inaudible] said on the "Description of Activity," but I think one thing I would want to add is that from this work we should also work at what are the implications from this SSR1 implementation to the SSR2 review. I think this might be very important. Not just look at the effectiveness of the [certain] implementation but also tell us what are the implications from the implementation of the recommendations for the SSR2.

EMILY TAYLOR: James, did you want to respond?

JAMES GANNON: Yes. I believe that a large chunk of that has been volunteered or "volun-told" to Zarko to a bit of a mapping exercise of the SSR1 actions onto our potential future subgroups to make sure that even in a situation where we are potentially revisiting SSR1 recommendations, that we map the two together.

EMILY TAYLOR: Zarko?

ZARKO KECIC: I just wanted to comment what we are doing today because it looks like we are doing an exercise of project management, but it is very difficult to do at this point. Because there are a lot of different topics that we have to cover, and we cannot have one of those do all of them. SSR1 recommendations review is one of the examples. We have 28 recommendations which are different, so we cannot say we have a subgroup which will do all 28 recommendations. Same thing with other topics that we have to do.

So I would propose to start as soon as possible to work on a real work plan, what we are going to do. To start from that because working on something between right now, maybe some other thing will show up in a month or two so we'll expand that and we'll have different people to jump in. So just talking about models here is very difficult and I think we will have to change that during a period of time.

EMILY TAYLOR: Thank you, Zarko. James, do you want to?

JAMES GANNON: Yes, excellent. For those not in the room, I'm up and wandering around. This was precisely why we had homework last night. One of the things that we have to do, and I'm hoping that we can at least make a start on

it today, is we need a funnel. Up here, we have all of the ideas and areas that the Review Team is going to come up with. We have started that last night, and hopefully people will continue to work on that and basically pull out the topics that we need to look at.

This is too much for us to do as individual work items, so we need to funnel these down into sets of buckets, essentially. At the moment, my proposal was that these buckets that all of these items are going to come down and be put into were the subgroups. Now we're not bound to [do this] in subgroups.

What I believe we are bound to do is to structure it some way. That's key. We need to structure it in a manner. We need to take all of these ideas that we started writing last night and all of the areas that were mandated by the Bylaws which we should be mapping all of these back to. So this is the implementation of DNSSEC. This goes back to Bylaw 4(c)(i). This is the ICANN internal security framework. That goes back to 4(c)(iii).

Then we need some way to bundle these together. Whether that is literally just tagging them, whether that is breaking up into subgroups, whether it's putting them into thematic areas – what way we approach breaking down our work into a manageable chunk where we are then able to actually start working on it is something that we really need to do today.

I'm hearing some concern about potentially moving it into subgroups. If there is another proposal on the table, let's get it out there. Let's come to an agreement. But we really need to start identifying our work items,

we need to start grouping them, and we need to start mapping people to those groups of work items. Because once we get to that point, then we can actually start refining things.

This doesn't need to be perfect at the start. We need a structure here that we can start working on, and then we can refine it as we go along. We can add tweaks to it. We can say, "Okay, well, we identified three areas today. We actually need a fourth one because we have this new [set] that we're actually going to break the ones that we put into bucket three to go into bucket four now.

But what's important for me and is really a goal for me of coming to Madrid this week is that we have this structure in place. It doesn't need to be final, but we need a structure in place that we start mapping those work items to groups of some sort and then mapping people to those groups so that we can start working.

EMILY TAYLOR: Thank you very much, James. I have quite a list emerging. I've got Steve, Alain, Zarko back again. And there's also maybe, Steve, are you conveying comments from Matogoro on the list? But I'd like to also highlight that.

STEVE CONTE: No, [I'm not].

EMILY TAYLOR:	Okay, so can I? I'll just use the chair's privilege of having the microphone on to just read out Matogoro's comments on this. He says, "Sure. I agree there a lot of topics to be covered with this team. We should be careful in not narrowing topics that may require our attention." So very much within the theme we've been discussing. "However, James has come up with something that we can build on. I'm taking this as a strawman for this team," which I think, James, is very much what your intention is.
	I always find when displaying potential models to clients or to people that they always go to the data rather than the framework and the comments are rather on the data. Actually, my understanding of what you've put forward to us for our comment is look at the blue boxes in these slides. Is this a rational way to divide up different topics or teams, whatever we decide to do? My opinion, if I may, is that this is a rational way to do it. Whether we actually use this for teams or topics or great big chunks or littler chunks, it seems to be quite a nice way of doing it.
	On my list, I have Steve, Alain, Zarko. Anybody else asking for the floor? Okay, please go ahead, Steve.
STEVE CONTE:	Thanks. James, I'm being ruled by physics with the microphone, so I'm speaking to you but looking this way. Please, I apologize. I like the ideas in the funnel idea. I'm curious if you have or where you thought a litmus test or filter for relevancy of whether these ideas – and this is with no reflection on what ideas are already posted. I'm just speaking in general.

When you look at the relevancy of an idea, if it applies to the remit of ICANN and the applicability of the SSR review itself?

JAMES GANNON: Yes. That is a really, really good point, and it's specifically why any of these items that we identify, the very first thing that we need to do is map it back to SSR Bylaw. Because we need to be able to show exactly what you're saying, that it's both relevant to the SSR Review Team, first of all, because we have a narrow remit and then even, again, that it's within ICANN's relevance and is something that we have the authority to look at.

STEVE CONTE: Then just as a quick follow up, that's at the Plenary level and not at the subgroup level?

JAMES GANNON: Exactly. The Plenary.

STEVE CONTE: Thank you.

EMILY TAYLOR: Alain?

ALAIN PATRICK AINA: Yes, James, I think I agree with you that at the end of this day we must have the focus area and the sub-teams before we leave this place. But as I said in my previous interventions, maybe let's focus first on the focus area, then we come to group or [inaudible]. First [as you said], let's focus on the first rule, what are the focus areas and how do we match them to the Bylaws, etc. first. Then we will come back to subgroups, etc.

EMILY TAYLOR: Alain, if I may, I think we have to start somewhere. We asked James to lead this session, which we're all really grateful for him doing. I think you're right that always with a complex thing there's a bit of what we would call "cart before the horse" in that we haven't quite organized our chunks of priorities. But imagine that we have done. Okay? Imagine that we have a priority and that that white space is blank. For any priority that you think is important, is the way that James is proposing that we organize it rational to you? Or are there any things that you would add or take away?

ALAIN PATRICK AINA: [inaudible] to be added to what he has proposed, but I'm just trying to fix the approach right now. Saying let's focus on the focus areas: 1) SSR1 Review, 2) what are we doing, 3) focus area first. Then we [inaudible] before. So then if we open this discussion, I have something to add.

EMILY TAYLOR: Thank you very much.

ALAIN PATRICK AINA: And I sent an e-mail this morning.

EMILY TAYLOR: That's great. And it's great to see how many people have contributed their ideas. We're going to come on to this very, very imminently. James, did you want a quick follow up? Yes? And then I have Zarko on the list.

JAMES GANNON: I'm going to go back to my lovely drawing. I usually like doing these on whiteboards. I think there is a little bit of a piece of work that we need to do before we can get to that stage.

Если we take my funnel analogy, and I've added something from Steve and now I've added something from you, we have all of these ideas. All of our Review Team members are up here coming up with these ideas. So first of all we have a sieve at the top of our funnel, a colander, where we make sure that the idea is relevant to the Review Team and is relevant to ICANN. That's our first sieve. It doesn't even get into the funnel if it doesn't pass that litmus test.

Once it's in the funnel, the Plenary is here to make a decision on funneling those into groups. However, these buckets that we have at the bottom of the funnel, at the moment we haven't agreed on having any buckets under the funnel. If we're to funnel them into idea buckets, the very first thing we need to do is agree on what those buckets are.

My very much strawman that I've put together is these five areas. If we want to decide to change those, keep the same framework, change them and change the framework, any of these things are okay. This is literally what was in my head the morning that I wrote this document. There's no formal structure to it or anything else that we have to do this because of this reason. This is literally my idea kicking off a discussion of it.

So we are doing exactly what I had hoped we would do, but I think it is important that we agree with our thematic areas or our subgroups or our topic areas or whatever we want to call them so that we can start taking these items and pushing them down through that funnel. Then the piece that comes after that is then who works on this, who works on this, who works on this, and who works on this.

EMILY TAYLOR: Okay, Zarko?

ZARKO KECIC: I agree that we have to divide our work in groups, and not all of us can do everything. But just dividing into groups is not good at this moment because unless we have what we have to do, you have here SSR1 recommendations review, there are 28 of them. They are different. Maybe five recommendations you can do by yourself. Maybe you will need 15 minutes talk to Eric or Boban, whatever, about some recommendations. That's not a group. That's work to do. Maybe we'll have some tasks that ten of us should work on them for two months.

So having groups like this like you are proposing will not get us [anywhere]. We have to have work plan what we have to do. How to do SSR1. There are other topics that are proposed. So we should have groups now to divide that into tasks. This brainstorming is good. We'll add brainstorming after those groups are finished their job. Then we can add can we do this, can we do this, can we do this.

Because at this moment, I'm still not familiar. The past two days were helpful for me, but I'm still not familiar what ICANN is doing and what ICANN can do. I don't want to get into area where ICANN doesn't have any stuff that can help. So I believe to go back to terms of reference is best thing to see what our scope. To have groups now working on those scopes and have fine tuning of tasks that we have to do. Then we can jump on groups and people who will do [real] work.

EMILY TAYLOR: Before you respond James, I actually think what we're hearing around the room is all different versions of similar things, which is this is good and let's come back to it when we have got our work plan sorted and we are simultaneously at the same time we are working on identifying major themes. This is a good thing for us to do. We may not be able to populate all of these right now.

I have Ameen. Do you prefer to be called Ameen or Noorul?

NOORUL AMEEN: Noorul. There's one more Ameen in the [inaudible]. I'm normally called that [inaudible].

EMILY TAYLOR: Okay, well, he's not here at the moment, so I'm going to call you Ameen. Then we'll go to Alain.

NOORUL AMEEN: I totally agree with Zarko's point. First of all, I'm totally interested in what are the key points that we need to address. Let's decide that first. That is a key area that I'm looking for.

EMILY TAYLOR: Alain?

ALAIN PATRICK AINA: As you said, we're just saying the same thing using different words. But I think the understanding here is let's not focus on groups right now. Let's focus on the scope, no the key focus areas first. Then we will – but I agree we must leave this place with groups and a clear work plan. But where are we starting from? What we are getting here is let's look at, again, the terms of reference. Let's look at the terms of reference and see what are the main focus points. [We need] three or four focus points before we then move on. I think this is where we are. So I hope the co-chairs will be able from now to take us to this destination or [inaudible] will crash.

EMILY TAYLOR: Thank you. No. Don't panic. We're not. I have got Cathy and Boban. And I'm not hearing this is a rubbish solution. I'm hearing [inaudible]. I'll put you on the list, James. Let's think about constructive ways forward now. Okay, we've got just a bit less than 15 minutes booked for this session, so let's start to think about drawing things to conclusion and how we move forward. Okay, Cathy, Boban, James.

CATHY HANDLEY: Thank you, Emily. This is mostly for my benefit, but I'm listening to the group and what I'm hearing is the first step is we have to agree on something. Do we agree on having sub-teams first off? It's a real simple question. It's not what's in the sub-teams or anything else, but the proposal that James has put out there?

UNIDENTIFIED MALE: [There is no question about it.]

CATHY HANDLEY: Okay, so that's good. That's step one that we have universal agreement in this room that we need this. I can't read the board, but perhaps next what we need to do is go through, identify all the bits and bytes that have been thrown out. The step after that will be too categorize in lumps where those bits and bytes fit. At that point, it will be extremely easy to slap this [on there].

If we can get that done today, we'd be miles ahead of where we are right now. I don't really think it's going to be that hard, and I think a lot of the things that have come up will just automatically fall in and not be

an issue at that point – I have high hopes – at least once we've identified the things. Thanks.

EMILY TAYLOR: Thank you very much. I've got Boban next. Matogoro in the chat has said, "This is a key responsibility of SSR Review Team members" I think. Hi, Kerry. Kerry from the airport has said she agrees with Cathy and agrees that we should shortlist the large wish list and then put it into buckets as a way forward. Boban, please take the floor. I know that this is stimulating lots of thoughts, but Zarko, Cathy, could we keep the comments into the mic so that we all have our focus? Thank you.

BOBAN KRSIC: Okay, thanks, Emily. [inaudible] follow up slide number, I don't know, 10. The topic is Review of Implementation of SSR1 Report. Is this in our scope or not?

UNIDENTIFIED FEMALE: Yes.

BOBAN KRSIC: Okay, next slide, James. Okay, thank you. James' proposal: ICANN Internal Security Processes. Is this in our scope or not?

UNIDENTIFIED FEMALE: Yes.

UNIDENTIFIED MALE: Yes.

BOBAN KRSIC: Okay, we identified the second topic. Third?

UNIDENTIFIED FEMALE: May I?

UNIDENTIFIED MALE: It is [inaudible] topic.

BOBAN KRSIC: Yes, it is. The question was only, is that topic in our scope? Nothing else. That's a topic and a description.

UNIDENTIFIED MALE: [inaudible]

EMILY TAYLOR: Okay, hang on a sec. We'll observe the line. Denise, did you want to come in at this stage?

DENISE MICHEL: I like the forward movement. Just a quick question. So you're running through the initial or strawman subgroups just to identify whether or

not they're within scope, and then we'll go back and ask additional questions?

BOBAN KRSIC: Yes.

DENISE MICHEL: Yes? Okay, good.

EMILY TAYLOR: Okay.

BOBAN KRSIC: Okay, DNS Security.

EMILY TAYLOR: Everybody comfortable? Anybody freaking out? Okay, go ahead.

BOBAN KRSIC: Next slide, topic number three, DNS Security. Is that topic in our scope of work or not?

EMILY TAYLOR: Yes.

UNIDENTIFIED FEMALE: Yes.

ZARKO KECIC: Can I [inaudible]?

BOBAN KRSIC: Yes, you can.

EMILY TAYLOR: Yes. Please use the mic, Zarko.

ZARKO KECIC: Excuse me. I just [said Cathy] when Emily intervened that James did good job and we should start from there. So let's not go through all the topics that he has. We'll agree. But we have to divide those topics into subtopics and then decide who will do that work. Actually, which [inaudible] team will do.

UNIDENTIFIED MALE: Agreed. First step, let's identify the topics. If you are [convinced] [inaudible] topics, we can go forward to structure it, to group it, or something else. The only proposal was we have five topics, we identified five topics, and let's take it from [inaudible] and then start to structure it and break it down [inaudible] sub-teams and go forward with the work to identify the work items and maybe its members. That would be great if we have this as the output at the end of the day.

EMILY TAYLOR: This is great. Also, if I can highlight that going back to our homework from last night, I think that our homework last night also has a role in identifying particularly our priorities because we are going to have to prioritize what we're doing because we have limited numbers and time. So, James, you are on the list and you're next. Unless, Boban, have you finished your remarks?

BOBAN KRSIC: Yes, my only two topics, and [inaudible] agreed they are also in scope.

EMILY TAYLOR: Thank you very much.   And thanks for that. Thanks for also advancing the slides.

JAMES GANNON: There are three things here that we need to, in my mind, make clear. These are not consecutive processes. In parallel, we can identify the items, which is now into a little box at the top of the funnel. We can keep identifying those items. That was our homework for last night. That is going to go on for a few days and possibly even a few weeks. We can also identify the framework by which we're going to funnel and identify what buckets they're going to go into.

We can agree on that framework without agreeing on what the actual subgroups are. We can then agree on what the subgroups will be labeled, what their areas are going to be, what they'll be focusing on.

But those can be three parallel processes: we can be identifying and putting the items into a bucket at the top ready to go into our funnel which is our framework which we can agree on, which will then go into the buckets at the end.

So, the understanding that I would hope for us to come to is, can we agree what we're going to break up our work into subgroups? I'm going to make a leap and ask the co-Chairs to check, do we have consensus that we're going to break down our work?

EMILY TAYLOR: I'm hearing consensus that we're going to break down our work. I think that's an absolute given. I may be overlaying my personal concern and assuming there's a consensus within the group to support it, but I think it's fair to say that there are concerns about how small la team we are and whether the subgroup label – but topics, leaders of topics, small items of deliverables, I think we're all in violent agreement. And in fact, I think we're kind of really keen to progress with the substantive topic, and what you've done is given us a framework to put all of those into. And thank you very much for leading this session.

So, we're just coming up to 10:00 local time. I've got some comments from Kerry-Ann on the list. She's saying she agrees with you, Zarko, that she needs one clarification regarding the homework that we need to shortlist similarly. So, now what we have is a great big kind of soup of everybody's priorities. And guess what? There's a lot.

And Kerry is saying that she recommends we shouldn't leave that for e-mail. The consensus on breakdown would be a good use of our time as a

group, and I think that that's a very good thing. Now, we've got – if I may, James, did you want to – so, Eric, please go ahead, and then I'll draw it to a close.

ERIC OSTERWEIL: In regard to what Kerry-Ann just said, I think that's exactly right. I think at some point pretty soon – and I think this might be consensus of what we're all sort of saying – is that we ought to basically take something, maybe it's the entire list in the Google Doc or not, throw it up on a Board and start grouping it together, start pitching things out, start deciding that two things are actually the same one thing, and then look what that looks like and try and circle back to this conversation, and then just iterate that cycle a couple of times.

But to Kerry-Ann's point, if we wait to do that over e-mail after today, it will protract that entire process maybe internally.

EMILY TAYLOR: I think you just hit the zeitgeist in the room, the feeling in the room. We've got a sort of spare half hour in the schedule. Unless anybody objects, could we get the Google Doc up on the screen and start with that work? Is that premature? Zarko, please.

ZARKO KECIC: Yes, I agree. That's the way how to do that. But let's get these topics that James and Boban brought up that I said we agree that's in the scope, and work our brainstorming with our interest within those groups. We have Internet security processes, huge. Take one topic and

work on that. Then next topic and work on that. And we'll come up with new ideas.

Because reading yours and Emily's and my items that we've put there, we're agreeing to [have done]. I have four, you have, I don't know, four or five. So, it is much better to work together and put all [inaudible] into these sub-items that we have here. So, we'll get structure within sub-items, and out of that structure we'll get tasks that we have to do.

And then we can build groups, will be that one-member group or five, it depends on work that we have to do. And also, those groups will not be entitled. Okay, group is James, Eric and Boban, and you'll do on that topic. Now, if you need expertise, you'll call [inaudible] you'll call Emily, so...

EMILY TAYLOR: Okay. Thank you very much. I have Denise, James and then Boban. And let's all think about moving forward, what next?

DENISE MICHEL: I support Eric's proposal and acknowledge Zarko's contributions as well. I think there's a fair amount of duplication, which is a good thing on this Google Doc. I think we can go through it and make it much more succinct. And I would prefer to go through that process, which is a more topic-oriented process, and then come back to how it makes sense to handle the work, who the topic leaders might be. Doesn't make sense to fit it into the subteams. I think that DNS security and security subteams are perhaps a bit too broad and may not be quite the right structure,

but I think the framework that James has proposed will be – seems like it would be quite effective when we reach that point.

EMILY TAYLOR: Thank you for that. James and then [Alain.]

JAMES GANNON: Thanks. So, I'm going to do another one. Can we agree that we need a framework to take topics and turn them into work items? And can we jump to make the assumption that tagging the items that we come up with as our [thoughts] against the Bylaws, against areas of interest, and then hopefully against a topic group which I've called [inaudible] or whatever it may be is the way we're going to do that? Because we need a reference back to the Bylaws so that we show we're in scope.

We need an area of expertise that we need people to be able to look at and say, "Okay, this is something that I'm not an expert in. This is something I am an expert in. This is something that I have an interest in." Be it ICANN, be it policy, be it security, be it risk management, we need some way of tagging these items for people who are not as familiar with the intricacies of ICANN-land as some of us may be, and then we need some way to caliberize them. I've got subgroups, I've put out a proposal. We seem to roughly agree on those groups, but that as a structure at least, can we agree on? Because then we can start the work that yourself was asking for and Denise is asking for to start putting these items up and start consolidating them, start getting them together into items that we can start pushing through that funnel.

EMILY TAYLOR: Okay. So I've got Alain, Boban, Zarko. Zarko, did you want to immediately respond to that, or do you want to join the queue?

ZARKO KECIC: If I don't forget, I can do that later.

UNIDENTIFIED MALE: [inaudible]

EMILY TAYLOR: [inaudible] You have an immediate response?

UNIDENTIFIED FEMALE: Personally, I don't think we need to spend a lot of time asking, "Can we trace every single contribution on this Google Doc back to the Bylaws and scope." I think that given the amount of time we spent on the Bylaws, on the terms of reference and on the objectives for this Review Team, I think the default should be if a team member has put it in a Google Doc, given that it's within scope and unless the team member raises the issue of, "I think this is an item we need to discuss about being in scope or out of scope," I don't think we need to spend a lot of time asking that question of every single entry. But assume it's in scope unless someone raises a question about it I think will help us move forward more quickly.

Okay. I have Zarko, you wanted to make a quick intervention. Sorry about the queue, everyone. And then I'm going to go back to James, Alain, Boban.

ZARKO KECIC: It is not intervention, it is just to add on to what James just said. Yes, that's something we have to do. But that's something that I said at the beginning of this conversation that we'll need subgroups right now because we can agree today on subtopics. We have main subtopics and we have to help find structure into our tasks within those subtopics.

And then somebody else should jump and divide that into activities that we have to do and connect that to ICANN documents, Bylaws and whatever, and then we should jump in to do real work.

EMILY TAYLOR: This is all real work, I'm afraid.

ZARKO KECIC: Okay, but why we are here?

EMILY TAYLOR: Yes, sorry, I was being slightly facetious. Thank you for that intervention. I think we have a lot to do and it's absolutely natural that there's a feeling of frustration that we all want to do kind of get it structured and get down to it. So, thank you for that. I've got James and then Alain and Boban.

JAMES GANNONG: Very briefly, I just want it on the record that I think direct mapping of topic area to Bylaw is a very important thing, and basically I would flip it around the other way, that if a team member is bringing a topic to be considered by the Review Team, they should be able to easily point to which Bylaw subsection that they think it fits under. I think that's a very important thing just from a governance point of view that we really should do.

EMILY TAYLOR: Could I just respond to that, James, and say I don't think anybody is questioning that? It's about how we use our time together, and perhaps that is an administrative task that could be followed up quite comfortably either by staff or by any one of us, yes. So, it's about how we use our time best together. I think nobody is in disagreement that we need to match the Bylaws.

I think that here's an assumption now that we're so familiar with those topics that the things that we suggested are probably in there. That is how I understood Denise's suggestion. Alain? Thank you for your patience.

ALAIN PATRICK AINA: Yes. I think I agree with James and [inaudible]. If we go back to the terms of reference document, we have a section on focus of the SSR2 scope of work. I think let's take it from there and make sure we all have the same understanding. And as James said, you could see clearly based

on the Bylaws section what we intend to do for each of them, make sure we all agree before we start looking at this group document. Otherwise, it would be difficult.

I put my idea, Boban put his idea, so, how are we going to put all this together if we don't have a referral to where we are putting them to? It would be difficult. So, I think as James said, first let's look at – and I think we can use the Terms of Reference document first. You had a section on scope of work and it explained clearly what we are supposed to do for each of these. I think this would be gusta. Otherwise, we will go through this document, I'm sure at the end it will be difficult to agree on some of the – because there are overlaps and etc., and we may end up going back to, "Oh, okay," of you saying do some follow-up after on the mailing list or staff or co-Chairs, and we'll be back again and again. So, my suggestion is let's look at the Terms of Reference document, the scope of work. We have agreed to that document and we take it from there, then we come to this document. So, this is my –

EMILY TAYLOR: Boban?

UNIDENTIFIED MALE: [inaudible]

EMILY TAYLOR: Okay. Matagoro is saying… First of all, there's been a bit of a thread on the chat which I'll just try to convey from Matagoro. First of all, he said, "We had identified some topics and areas through ICANN58 meeting in

Copenhagen. I'm proposing to consider them too in our selection list."
And I said, "Please add them to the Google Doc."

Kerry agreed with Eric, she thinks, and then Matagoro says, "Topics are included today in discussion from slide 20 to 25. I would propose that we jump to those slides, plus the one in the Google Doc. I strongly recommend that the topics proposed in the Google Drive be merged with one proposed in Copenhagen to have one single list, which duplication will have been eliminated."

So, we've got various – like three different options about how we move forward. Can I just insert a note of caution? If we're not careful, we're going to spend the rest of our day together deciding how we're going to move forward. Let's just move forward.

What we decided yesterday is that we would generate a Google Doc where we identify priorities. My first suggestion is we're probably all ready for a break, actually, but that we come back after a break and try to condense this Google Doc into priorities. Because what we're all saying in different ways is we need to identify priorities. This is the latest version. If we go back to the terms of reference, what are we doing with the work we've just been doing? The terms of reference is broad, this is attempting to narrow.

So, let's take a break – we need it – and all agree that we're all saying the same thing, which is we need to move forward. But let's not argue anymore about how we're going to do that. Can I just say, let's just try this Google Doc and try to get some priorities? If it all messes up, we'll go to other alternatives, but I think we can do this. Let's have some

coffee. Thank you. Let's come back at 25 past, let's have a 15-minute break. And could I also say thank you to James on behalf of the group for leading that session and for preparing.

[BREAK]

Okay. Welcome back, everybody. Thank you for returning promptly. What we're going to do is Eric has very kindly volunteered – or he may have been volunteered by me – to lead this next conversation because he's going to… There are two things going on at the same time, and that's why there's a bit of interaction between Eric and Karen.

Karen has started to synthesize our kind of sandpit document, if I can put it that way, into something sensible into a table. So, that's going to take a while, and also we can help to give her some guidance through working on it. And Eric is going to lead this discussion.

So, what we're going to do is try to narrow down all of our thoughts from last night. There's a lot of commonality and also a lot of other ideas as well. So, Eric, the floor is yours. Take it away. Thank you as well.

ERIC OSTERWEIL: Okay. Thanks, Emily. Karen tells me that she's still sort of doing her pass, and so I'm trying to figure out where the right starting point for our canonical list to iterate on together, but sort of ahead of that. This is what I'm proposing. I'd like to get early feedback from anyone who has opinions about whether this is the right or wrong or there's a better approach, but what I thought we would do is we'll take a look at the sort of aggregate list of topics that's been thrown together. We will try

to de-duplicate places where there are sort of common ideas put together, which I think is actually a really good thing. So, in the event that we find that multiple people said the same thing, even slightly differently, that's absolutely a good thing, means we're on the same page.

And I think what we'll probably find – and I want to sort of jump to it as soon as possible, but I want to make sure that nobody sees an objection early on that we can get in front of. I think we'll probably find that there will be some core things that we really think we ought to do. There are probably going to be too many things for us to ultimately do realistically, and so what we'll probably do is pick a set of core things that we think we need to start with and prune either permanently or at least temporarily a large set of things that while they might be interesting, they may just not be things we need to start with. Does anybody have anything they'd like to comment about that [inaudible] Denise?

DENISE MICHEL: I agree with everything you said. I just have an additional suggestion. Could one of the six staff in the room, while we're doing this in parallel, look at the brainstorming list from our very first meeting in Copenhagen and flag for us any issues that don't appear in the Google Doc so at some point we can circle back and look at those as well? Is that possible?

ERIC OSTERWEIL: Okay, so I'm standing by to [inaudible]. Okay, so I don't see any other flags going up, so nobody else has any sort of contrary thoughts? So, I guess what I need to do now is figure out what the right list to start with is. I don't want to rush Karen, so if the table is not ready, then I will revert to the Google Doc for the discussion.

UNIDENTIFIED FEMALE: [I think we're good with that.]

ERIC OSTERWEIL: Okay. Cool. So, let's see. Sorry, I'm thinking on my feet. So, if you'll all give me a second, because – alright, I'll tell you what. I'm going to go up to the board, I'm going to find a travelling mic, and I'm going to ask for somebody to help me out. I'll look at the screen and I'll start throwing things into groupings. But if somebody could do a sort of more mindful pass at the Google Doc, that'll help me.

EMILY TAYLOR: Eric, while you're moving, there seemed to be quite a lot of agreement around the issue of universal resolvability. "Can identifiers be uniquely resolved and consumed?" And there were a number of bullet points around that. Sorry?

UNIDENTIFIED MALE: I would hope so.

EMILY TAYLOR: You would hope so, wouldn't you? But sometimes it helps to state the obvious. And I think also improving the security of unique identifiers. I'm not seeing any, so, am I going too fast?

ERIC OSTERWEIL: No, but I was about to warn everyone, my handwriting is really bad. So, you all asked for this. I'm just throwing that out there.

EMILY TAYLOR: I can write. I have girly handwriting, yes.

ERIC OSTERWEIL: Okay, so I've got universal resolvability. And sorry, what was the second one that you said, Emily?

UNIDENTIFIED MALE: Green here, red, blue, yellow.

ERIC OSTERWEIL: The blue one's taken and I dislike red and green because I'm colorblind.

UNIDENTIFIED MALE: [inaudible]

EMILY TAYLOR: So, "Universal resolvability, number one. Improving the security of unique identifiers." These are ones where we all seem to agree.

UNIDENTIFIED FEMALE: [inaudible]

EMILY TAYLOR: Please?

DENISE MICHEL: Could we surface the people's understanding of the distinction between the bucket of universal responsibility and the bucket of universal acceptance? Just to make sure everyone's clear.

ERIC OSTERWEIL: I can tell you where my thoughts are, and then I'd love to have that attenuated by different opinions or perspectives in the room. In my opinion, universal resolvability is about the lack of ambiguity in the namespace itself. It's about the fact that when there's something.com or something.org or something.anything, there's one of those. It doesn't collide, it means something unambiguous, it's easy to get to, it's universally available to people who look up – etc.

Universal acceptance is about a client's ability to take a name that is universally resolvable and actually get to it. Like something.brandnewgTLD that my mobile platform doesn't know how to read. So, that's my opinion of the difference between the two.

DENISE MICHEL: So, if a particular version of Google Chrome isn't up to date on some of the IDN elements and needs to be updated, is that acceptance or resolvability?

ERIC OSTERWEIL: I would say that's acceptance because of the nomenclature I'm used to people using, resolvability I usually think is more about the namespace itself. Kaveh.

KAVEH RANJBAR: So, either acceptance or – I was focused on resolvability. So, what is ICANN organization role in that? So we want to review or comment on –

ERIC OSTERWEIL: Which? First, I want to make sure we have the same working definitions for the terms, or we choose different terms that are at least unambiguous so I could address the question that you're raising.

DENISE MICHEL: I think my question is –

EMILY TAYLOR: So, okay, let's do this this way. I'm nominally still responsible for this session, so I can volunteer to keep the list. Eric will –

ERIC OSTERWEIL: I'll [inaudible]

EMILY TAYLOR: As we did in the last one, because I'm just aware more than one person is asking for the mic. So, Denise, go ahead.

DENISE MICHEL: I think my question is, is universal acceptance a subset of universal resolvability? To be more specific.

ERIC OSTERWEIL: I don't know that I feel hard and fast – I feel like they're different, but I wouldn't have any problem being [overwritten] on that.

EMILY TAYLOR: Me neither, and I think I'm probably responsible for splitting them out into two, because I've put –

ERIC OSTERWEIL: No, I did that.

EMILY TAYLOR: Oh, did you? Okay.

ERIC OSTERWEIL: Yes. So, my perspective was resolvability says something about the namespace itself and acceptance says something about the client's ability to interface with it properly. But that's just my take based on my perspective, and I'm not hard and fast on it.

EMILY TAYLOR: James, did you want to make a comment?

ERIC OSTERWEIL: We're trying to figure out the buckets. So basically –

Okay, so Zarko wants to know if we can just move on. Okay, cool. So, Kaveh, did you want to ask something?

KAVEH RANJBAR: No, let's write them down and then...

EMILY TAYLOR: There was a piece around metrics that I'm not sure – yes, I didn't see. We got measurements and metrics, which has got increasing numbers of bullet points under it. There seems to be quite a lot of engagement around that.

DENISE MICHEL: So, I'm not – so, are we discussing these?

ERIC OSTERWEIL: Yes. I think –

DENISE MICHEL: Do you want some input?

ERIC OSTERWEIL: Yes. I'm just throwing things up here that [inaudible] reading it and I'll cross them off and I'll make them bullets or whatever.

DENISE MICHEL: So, my first inclination is that measures and metrics really important, but I don't see it as a free standing bucket but rather something that is integrated into a number of topics and buckets that we're going to address.

ERIC OSTERWEIL: Okay. Yes. I've put it on there initially because I wanted it to basically personally be enshrined in almost everything we do. The default should be, "Let's assume there needs to be a measure," and ideally if possible a metric associated with at least one aspect of what we're doing. And I thought that might be a bit controversial, so I brought it as a topic of like that, but yes, so I'll cross it off and then we'll just circle back. And maybe we can just agree sort of as gentlepersons' agreement when with start working on stuff, if there isn't a way to do a measure or ideally a metric about something, then we just say, "Okay, that's exceptional." Usually there is.

DENISE MICHEL: Yes, I'd like to underscore and agree with what you just said. I think measurements and metrics in every element is important.

EMILY TAYLOR: I have Cathy, then Boban.

CATHY HANDLEY: Anyone who's got some project management blood in them, they have a process called greenlight, and you just go through and write stuff down. I strongly suggest we do that now and do a greenlight session where you just go through what's been put down, and then go back and have these discussions about what's the difference between resolvability, or we will never get through this list. And that's a guarantee.

ERIC OSTERWEIL: Okay. So, I'm not a project manager, never anywhere in any of my former lives do I believe I was nevertheless. But nevertheless, that sounds really good. So, how about we do that? And the only thing – I'm asking if this fits with the sort of theme that you have in mind – the only thing I'll try and do is I'll try to de-duplicate as we go, and I'll ask people to object to having something greenlit.

In other words, "Hey, I see that up there but I think we shouldn't do it." Consensus then forms. Is that cool?

EMILY TAYLOR: Cathy.

CATHY HANDLEY: I would not do that. Having gone through this, it's a lot easier and everybody feels like they've had input. This is no judgment on anything, whether it's a duplicate of anything, just bam, put down what's there and then you start going back and going, "We've got this here and this here. Are they maybe the same thing?"

ERIC OSTERWEIL: Okay, so the first pass of greenlight is just to throw things out?

CATHY HANDLEY: Yes.

ERIC OSTERWEIL: Okay. Great. So, that is probably not best done on the board here since we have so many on the dock I don't think [inaudible] transcribe, so maybe we should edit the Google Doc in real time and we'll greenlight every line there. Is that cool?

EMILY TAYLOR: How would you do… So, I think everyone's –

ERIC OSTERWEIL: Does anybody object to that?

EMILY TAYLOR: It's cool idea.

ERIC OSTERWEIL: [inaudible]

DENISE MICHEL: I think it's a matter of – I'm sorry, Zarko and I were having a side conversation, so I may have missed this. I think it's both greenlighting, but also combining as well. [inaudible]

ERIC OSTERWEIL: Cathy didn't want to do both at the same time. She wanted to do that in a second pass. I think.

EMILY TAYLOR: I've got Boban who had asked for the mic, and then I'll go to James.

BOBAN KRSIC: Just a question for the staff. Do we have some moderation material like [inaudible] for anything else? Because I think it's easier to have a whiteboard, a chart or something else and to drop something and move something, stick something, Post-Its or any material to create the workshop. Because it's too hard to write everything down using Google Doc.

UNIDENTIFIED FEMALE: To move things around?

BOBAN KRSIC: Yes.

UNIDENTIFIED FEMALE: Do we have sticky notes?

UNIDENTIFIED FEMALE: [Staff?]

UNIDENTIFIED FEMALE: Did we bring any? No?

BOBAN KRSIC: No. Okay.

UNIDENTIFIED MALE: So, how about this –

BOBAN KRSIC: So, because we are talking about constraints like metrics and focus areas like – so, yes, I think it's easier to move something on a board.

EMILY TAYLOR:	Yes, I think that's a great suggestion. Unfortunately, we don't have the materials.
ERIC OSTERWEIL:	I think [inaudible]. Let's make something work there. So, let's do a first pass over this, let's greenlight it because it might reduce the size a lot, and if we reduce this thing's size, I'll do the legwork of trying to do something like that or I'll rip little pieces off into sticky pads and I'll put them in circles on the floor, something like that, and you'll figure it out.
EMILY TAYLOR:	Lovely. James, you'd asked for the mic. Cathy, do you still want to intervene?
CATHY HANDLEY:	Oh, no.
EMILY TAYLOR:	James?
JAMES GANNON:	Sorry. I'm searching for stationary stores nearby.
UNIDENTIFIED FEMALE:	[inaudible]

JAMES GANNON: Yes. So, yes, just [inaudible] Cathy thing for some context. If this was a real project, the way you do it is you get your user requirements, which are everything, anything. It doesn't matter if one of your user requirements are ICANN should be able to fly to the moon. You get them, you write them down, and then you do your consolidation, your ranking, your bucketing.

So, to stop me [bristling] inside, I'd prefer to go that way. But whichever way the group wants to do it.

EMILY TAYLOR: Thank you. So, we seem to have – should we just give a go to greenlighting this, going through the document one by one?

ERIC OSTERWEIL: First, can someone agree to hold the pen on the document so that if we need a line item, veto or change something, we can do it real time but one person is in charge of that? I can do that.

UNIDENTIFIED FEMALE: [I can do it.]

ERIC OSTERWEIL: Okay.

EMILY TAYLOR: Jennifer, can you do that for us? Thank you.

ERIC OSTERWEIL: That means I'm going to go sit down.

EMILY TAYLOR: You're going to sit down? Okay. So, are you going to take us through the document, Eric, or would you like me to do it?

ERIC OSTERWEIL: [inaudible]

EMILY TAYLOR: I'm happy… You can sit down and do it.

ERIC OSTERWEIL: [inaudible]

EMILY TAYLOR: Oh.

ERIC OSTERWEIL: Okay, I'm going to sit down. Okay, so yes, I'll be happy to [drive.] So, hey, number one is the first one that we talk about all the time. "Complete the assessment of implementation of SSR1, recommendation impact, implementation, lions, tigers and bears." Anybody want to non-greenlight that? Silence is consensus. Go.

Okay, so next one, "Scope of ICANN's SSR responsibilities action zone, influence zone, coordination zone." Anybody going to not greenlight that? Silence is consensus. Okay.

"ICANN SSR responsibility for the coordination of global unique identifiers." Okay, that one's kept.

"ICANN operational role."

UNIDENTIFIED MALE: [inaudible]

ERIC OSTERWEIL: Mic.

UNIDENTIFIED MALE: Yes. This first line, I just bullet point to elaborate a little bit on the [layer] one. So, they are not –

ERIC OSTERWEIL: Oh, I see, the sub-bullets. Okay.

EMILY TAYLOR: Sub-bullets.

ERIC OSTERWEIL: So, [inaudible] them as well. Okay, cool. Lost –

UNIDENTIFIED FEMALE: Sorry, I'm just trying to figure out why I can't – here we go, [inaudible] my edit capabilities [inaudible].

ERIC OSTERWEIL: Alright.

UNIDENTIFIED FEMALE: Sorry about that.

ERIC OSTERWEIL: No worries. Okay. So, I'm sorry, I sort of conflated some things. So, the item is scope of ICANN's SSR responsibilities. Action zone, influence zone, coordination zone, and the sub-illustrations are just filling in the information from above. So, we're greenlighting the first main pullet and the sub ones. Yes, exactly, the sub ones just are part of it. Correct?

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Cool. Alright, so the next main bullet. "Effectiveness of ICANN's SSR framework, SSR plan and its implementation. It includes security framework contingency planning, security framework robustness for rapid and evolving security environment." So, effectiveness – okay, that's greenlit.

Okay. So, there's some agreement there. Okay, so next one is "Physical security requirements in place and enforcement of minimum security specification for DNSSEC key storage facility."

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Okay. Greenlit. I'm going to assume that any objections will be shouted out, so if I don't hear an objection, it's not my fault.

EMILY TAYLOR: I'll watch the Adobe room.

ERIC OSTERWEIL: Oh, thank you. Okay, "Two, level of compliance requirement for registrars agreements.

EMILY TAYLOR: Yes.

ERIC OSTERWEIL: I've got a look of consternation from one person and yes from somebody else. We'll yes it for now and we'll let people elaborate later. I'm not calling anyone out, I didn't say anything. Not going to be the – okay, "SLAM and performance indicators."

UNIDENTIFIED FEMALE: Sure.

ERIC OSTERWEIL: Green. Okay.

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: That's three. I think SLAM is the actual –

UNIDENTIFIED FEMALE: Service level agreement [inaudible]

UNIDENTIFIED MALE: Service level agreement [inaudible]

ERIC OSTERWEIL: Okay. "Four, with regard to SSR1 implementation of [inaudible] 7, 10, 11, 27 to see what extent the current OCTO research feeds into the risk management especially in relation to the SSR of unique identifier space." I think this one's similar to one we're all in agreement, so –

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Yes. And then "Observation for SSR1 was to make sure ICANN outlines its processes for security, stability and resiliency, and keeping in mind comments made yesterday during OCTO's mandate," we should revisit how clear this outlines. If not clear, I can clarify on the e-mail list.

JAMES GANNON: [inaudible] clarification?

ERIC OSTERWEIL: Yes.

JAMES GANNON: So we put clarify [inaudible]?

ERIC OSTERWEIL: Yes. Clarify or… I'm sorry, the clarification is for the para below it.

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: Okay, let's see. These are Emily's. Universal resolvability. Thank you very much. "Universal resolvability. Can identifiers be uniquely resolvable and consumed? This would include things like alternate root name

collisions, universal resolvability in Internet of Things, IPv6 CGN complexity, query the role of ICANN on this. Nation state firewalls."

As a main bullet, does anyone object to that as a starting point for greenlit? Because I could go line item if we need to. But overall? Okay. Universal [inaudible] is kept, greenlit.

So, going down to the next main bullet, "Improving the security of unique identifiers. Includes threat mitigation. Identifiers. Authoritative domain name servers, recursives and stubs, domain name registration, data registrars, registries and registrars, IP addresses, [inaudible] system numbers, infrastructure components like routers and switches, protocol parameters, implementation, etc."

EMILY TAYLOR: James.

JAMES GANNON: Okay, so for this one, I'd like to know if we're going to break it down enough, because there are some that I would greenlight and some that I would have queries about.

ERIC OSTERWEIL: Yes, we definitely have to break it down form the main bullet for sure. Do you want to discuss elements under identifiers, or identifiers itself?

JAMES GANNON: Elements under identifiers.

ERIC OSTERWEIL: Okay. So, one thing we can do is we can do that now, or we can say, "Identifiers has pros and cons," and we should discuss them in detail in the next iteration. Which would you prefer?

JAMES GANNON: I'm happy to mark the higher level bullet as for clarification and come back to it later. I think that's more efficient.

ERIC OSTERWEIL: Alright, let's do that. Identifiers needs clarification. No, just the identifiers, a sub-bullet.

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: Identifiers. Yes, that one. Yes, I think that makes sense. This way we'll just do sort of like multiple passes, because that's how it works for [inaudible] Alright, "DNSSEC progress, key role, etc." Greenlit? Greenlit. Domain name abuse mitigation.

UNIDENTIFIED MALE: [inaudible]

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: I know some – okay, need clarification on abuse mitigation. DDoS.

UNIDENTIFIED MALE: [inaudible]

JAMES GANNON: Sorry, can I come in?

EMILY TAYLOR: Yes. Sorry, I was just about to ask you whether you're asking for the mic or whether that was an old thing.

JAMES GANNON: I can accept DDoS on the understanding that within ICANN's remit. ICANN is not going to solve DDoS on the Internet, but its role, yes, of course.

ERIC OSTERWEIL: Do you want to list it as clarify, or do you want to list it as [inaudible]?

JAMES GANNON: I think clarify so that we can put additional facts around it.

ERIC OSTERWEIL: Okay. DDoS is clarify.

EMILY TAYLOR: Okay. Also, all of this is within our terms of reference, which also – so, if we're object orientated, our terms of reference are referring to ICANN's mission and scope. They are automatically limited through ICANN's role. So, can we just take as [read] that we're not going to be taking ourselves out of scope or ICANN's mission? Denise.

DENISE MICHEL: Yes. To follow up on your comment, perhaps we could just take a couple more minutes with that caveat and everything in here. We're not suggesting we're… We can have the caveat on domain name abuse mitigation within ICANN's role, DDoS within ICANN's role. Is there still an objection or a need for clarification on that? Yes.

UNIDENTIFIED MALE: Yes, because I don't think that justifies it. We can put any word as defined by the ICANN [role], correct? I really want to see how DDoS is defined and treated in ICANN's remit.

JAMES GANNON: This is why we come back to it.

UNIDENTIFIED MALE: Yes, that's why I think we have to come back to this.

ERIC OSTERWEIL: Okay, cool. Yes, so – go ahead, Karen.

KAREN MULBERRY: I'm sorry. I just moved the table into the Google Drive for everybody and I'll send out the link, and then we could get it displayed for you so it might be a little bit easier. Or you can continue this and then I can clean up the table when you're done.

ERIC OSTERWEIL: Yes, let's just make that part of the next iteration. I think we're going to do multiple passes, and so let's let it be [non-printed]. But thank you very much, Karen. Okay, so yes, so just back to that one point. How about this? I'll make a ground rule and see if you guys would be okay with it. Right now you can say yes, no, or clarify. And clarify can mean we're going to discuss it, no means we're not talking about it again unless someone makes a big point to bring it back in.

So, yes doesn't mean we never get to go into any detail on this. Clearly, we're going into a lot of detail and we'll probably combine things. So, yes, no, clarify. Alright, cool. So, "Universal acceptance. Can identifiers be consumed by clients?" That would be talking about IDNs, new gTLDs, platforms approaches and status. As a major bullet, does that get a yes?

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Okay. Good, we got a yes by universal acceptance. Okay, cool. And measuring metrics. I think we already struck that one as kind of just a thematic element, but let's look at the sub-bullets and see if anything there wants to be preserved.

So, we're not going to greenlight the major bullet, but how can the community measure the stats of SSR? That one's mine. So, I'm going to say no, because I think we're going to incorporate that more concisely in other things. So, anyone want to preserve that as it is?

UNIDENTIFIED FEMALE: Yes.

EMILY TAYLOR: Do we end up losing it if we said we'll never discuss it again if we said no.

DENISE MICHEL: No, I think the point here was on our previous discussion when it was at the Board was that it didn't merit a separate topic, but we wanted to make sure that we strapped measurements and metrics in every topic and subgroup that's feasible. I think that was the point.

ERIC OSTERWEIL: And I definitely worry that we have the potential of boiling the ocean if we're not careful with this one. So, I blame myself.

EMILY TAYLOR: I just note that it's taken us 30 seconds to break the yes, no, clarify rule. I'm just saying, I'm not judging.

ERIC OSTERWEIL: No, we're going to call this one a no.

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: Okay, let's clarify it's a no. Alright, great. Okay, so "What are and how can the community measure the relevance of uses for ICANN identifiers?" Anybody say no or clarify? Default is yes. I hear consternation.

JAMES GANNON: Clarify please.

ERIC OSTERWEIL: Okay. Clarify. Okay, and then next one, the evidence-based DNS health index and abuse data – I lost where to go.

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: "Access to information, risk and benefits."

JAMES GANNON: Clarify.

ERIC OSTERWEIL: Okay, so DNS health index, clarify. Okay.

JAMES GANNON: Can I just clarify that statement? Are we talking about the identifier health matrix that [inaudible] was talking about? And if so, can we refer to it for the ITHI for specificity's sake? Thanks.

ERIC OSTERWEIL: Yes, clarify. Unfortunately, it's the only tool in our toolbox that fits. Okay, "ICANN's internal security, stability and resiliency operations. Allocation of resources, priority organization includes budget staffing, outreach and public information [inaudible] risk management compliance, relevant frameworks."

Is that a yes? Looks like a yes. Okay, we're keeping that one.

Okay, and then the next one is white hat operations. "What are the white hat operations that are taken in ICANN's space that may need exceptional handling? [Gratis] for registering sinkholes, and can this be included improving security of unique identifiers threat mitigation?"

UNIDENTIFIED FEMALE: I'd say no because I see this as an element in other topics and subteam potentially that we've identified.

ERIC OSTERWEIL: Okay. So we have a no. James.

JAMES GANNON: I'd say yes, which means it's a clarify.

ERIC OSTERWEIL: Okay, yes. Disagreement constitutes throwing down and stick fighting. So, you guys after lunch. Okay, cool. And so I believe the next set that says my second try is a subset of what Emily did, so we'll skip the Eric section, which I'm all for.

EMILY TAYLOR: Could I suggest that we just delete it from the document? Or no. We're moving on to a different document.

ERIC OSTERWEIL: Yes, we'll be moving on. We'll probably use Karen's in the next iteration.

EMILY TAYLOR: Okay. I broke the yes, no, clarify [inaudible]

ERIC OSTERWEIL: And Karen has a comment or question.

KAREN MULBERRY: I just wanted to note that there was a comment in the observer room.

EMILY TAYLOR: Yes, I was going to wait until we pass through the document and then add it at the end. Thank you, Karen.

KAREN MULBERRY: Alright, thank you.

ERIC OSTERWEIL: Okay, so next section. "If we analyze any cybersecurity breach exploit, it may be either server-side exploit or client-side exploit. The fundamental cause of server-side exploit is lack of secure coding practice or lack of secure implementation protocols. Client side exploitation can be prevented by user awareness, education. Observe that there are [inaudible] and registry management system, especially in those who are using web portal managing DNS entries and nameserver entries. Other important parts of possible vulnerability, database, [inaudible] DNS issues, proactive measures."

Okay, so I think these are very important. We need to probably put them in terms of something actual. Go ahead, James.

JAMES GANNON: Yes. Exactly that. They are important, so can we put a clarify so that we can come back to this and put it into similar language to the other ones?

ERIC OSTERWEIL: Yes, I think that's great, because we'll wind up with a bunch of stuff and either this is spoken for already or some aspect of it isn't, and we'll write it up and codify it. So, yes, clarify for this.

Alright. And then the next set, focus on subteam number two, "ICANN internal security processes. Subteam will responsible… Okay so that's described by the subteam will be responsible for viewing the completeness and effectiveness of ICANN's internal security process, effectiveness of ICANN's security framework.

Okay, that's a yes. "Due to ICANN's orientation, ISO, IEC 27001, blah, blah would recommend provide gap analysis, [inaudible] requirements for the management part of [NFA] and ISO standard base, [so in scope.]" Yes? I'm assuming that's a yes. Yes.

UNIDENTIFIED MALE: [inaudible]

ERIC OSTERWEIL: Okay. "Perform interviews and review descriptions and evidence of ISMS, BCMS, information security policy, information risk management and risk threat processing, information security objectives, information

security roles and responsibilities, ISMS, internal audit and results of conducted audits. Operation planning, control document, evidence of top management review of the ISMS." Yes? Okay.

So, those are sub to the big one, which is a yes. Okay, thank you.

UNIDENTIFIED MALE: [inaudible]

EMILY TAYLOR: Alain, did you want to take the mic?

ALAIN PATRICK AINA: Okay. So, up to now we are just doing yes, no and then clarify.

ERIC OSTERWEIL: You can call clarify.

ALAIN PATRICK AINA: Yes, I think we'll have to clarify.

ERIC OSTERWEIL: Okay, that one just became a clarify, please. The overall [perform] interviews then review descriptions and evidence of became clarify. Includes all those. Okay.

UNIDENTIFIED FEMALE: Clarify [inaudible]

ERIC OSTERWEIL: Okay, so "Various others from the Annex A, like rules, acceptance, use of assets, access control policy, operating procedures, confidentiality and non-disclosure agreements, security systems, engineering principles, information security policy for supplier relations, etc." I don't understand what that work item. Is that part of another thing?

UNIDENTIFIED MALE: [It's part of the same.]

ERIC OSTERWEIL: That's all one thing by itself? Okay, so is that a yes, no or a clarify? Because I didn't get it.

BOBAN KRSIC: Yes, just to clarify it, these are documents which are required and described in the Annex A from the norm.

ERIC OSTERWEIL: Okay.

BOBAN KRSIC: And the bullet points below that are points which are in the minutes are part of the normative standard. So, it's the same, it's a part of [inaudible] description and evidence of.

ERIC OSTERWEIL: So the sub-bullets that you have there describe the action item for that? Is that what you're saying? I'm sorry.

BOBAN KRSIC: No, the sub-bullets are requirements that are normative context in the management part of the standard, and the procedures in Annex A linked there and described there are only in the annex of the standard.

JAMES GANNON: Okay. Can I stop this here? This is a clarify. Move on. That's exactly what the process [inaudible]

ERIC OSTERWEIL: I was just asking if the bullets under are part of the big thing or if we have to go through those now. I was just doing a procedural question. So, like categorize and prioritize the outcome of the analysis looks like it belongs to the pair above, or –

EMILY TAYLOR: [inaudible] Yes, we'll do clarify, I think.

ERIC OSTERWEIL: Okay, so we'll just clarify. So we'll take each of these individually. Okay, so definitely clarify on –

EMILY TAYLOR: [inaudible] asking for the mic?

UNIDENTIFIED FEMALE: [inaudible]

EMILY TAYLOR: Yes.

ERIC OSTERWEIL: Okay, develop a short, medium and long term schedule to implement different controls in accordance with the requirements.

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify, okay. "Define a set of metrics to measure the effectiveness of the…" I kind of believe these are part of the bigger paragraph, but okay. We'll clarify. I think these inherit clarify from their parent.

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: Sweet, isn't it? Okay, "With the goal to achieve a high level of maturity and to pass successful certification process to [inaudible] ICANN." Part of big one. Clarify. Okay. Alright, cool, and we're getting somewhere.

Next section. "Analyze policies and procedures that are essential to ICANN identifier system activities."

UNIDENTIFIED MALE: Yes.

ERIC OSTERWEIL: Okay, that's a yes.

"Analyze the possibilities for faster exchange of information on methods of abuse and unique identifiers and recommendations for mitigation." Yes. Cool.

"Analyze universal accessibility and resolution of unique identifier systems."

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Yes. "Analyze ICANN internal procedures essential for SSR of the organization and global operations." Yes. It'd be hard not to do SSR review as an SSR Review Team, but we can probably manage it if we want to.

Alright, now this is getting faster. "Business continuity planning."

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify, okay. Bam. "Transition of IANA functions to operator plan."

UNIDENTIFIED MALE: Yes.

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Yes, good. "Security framework."

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Yes. "Incident response planning."

EMILY TAYLOR: Cathy is asking for the mic.

CATHY HANDLEY: I'd just like to go back to transition to IANA functions to clarify.

UNIDENTIFIED MALE: [inaudible]

UNIDENTIFIED MALE: I support that.

ERIC OSTERWEIL: Okay.

UNIDENTIFIED MALE: But I think business continuity planning is very important [for our work.]

UNIDENTIFIED FEMALE: Clarify, yes.

ERIC OSTERWEIL: Okay, well clarify doesn't in any way diminish it, it just means somebody wants to ask a question. We're just doing a first pass. So yes, don't worry. You'll get to fight for it.

UNIDENTIFIED FEMALE: Incident response planning.

ERIC OSTERWEIL: Incident response planning.

UNIDENTIFIED MALE: Yes.

ERIC OSTERWEIL: Yes, okay , cool. "[CBD] process."

UNIDENTIFIED MALE: Yes.

EMILY TAYLOR: What is CBD process?

ERIC OSTERWEIL: Clarify.

UNIDENTIFIED MALE: Okay. Well, I can [inaudible] coordinate them under vulnerability disclosure.

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: Vulnerability disclosures. [inaudible]

EMILY TAYLOR: [inaudible] in the list, and then [there's] a yes.

ERIC OSTERWEIL: I think we're going to need to clarify, because it's possible that one just needs a little bit of a discussion. But okay, coordinated vulnerability disclosure process.

UNIDENTIFIED FEMALE: Yes.

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Oh, it's a yes. Okay, cool. Awesome. "Ultimate root risk."

UNIDENTIFIED FEMALE: Yes.

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Yes. Cool.

UNIDENTIFIED MALE: [inaudible]

ERIC OSTERWEIL: What's that?

UNIDENTIFIED MALE: Clarify.

ERIC OSTERWEIL: Clarify? Okay. Clarify for alternate root. "Vetting process for EBERO operators."

UNIDENTIFIED MALE: Yes.

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Yes. Okay, cool. Okay, ICANN processes around vetting registry operators.

EMILY TAYLOR: Could I just note on this? This is a suggestion from the observer room. Nick Shorey is I think now at the National Crime Agency. He was

previously at the UK Department of Culture and attending GAC meetings in that role. So, thank you, Nick, for the contribution from the observer room. I think James put the suggestion straight into the document.

ERIC OSTERWEIL: I think – so I'll give this one a yes.

UNIDENTIFIED FEMALE: Yes. [inaudible]

ERIC OSTERWEIL: Alright, sweet. Okay, so this is ICANN58 brainstorming, and it is long. Okay, [inaudible]

DENISE MICHEL: Can I have just a quick clarification? So, did staff just drop the whole brainstorming list in, or just the ones that weren't duplicate of what was already there?

UNIDENTIFIED FEMALE: [inaudible]. We've just married what was in the brainstorming document as a consent… And there were nuances and [concerns] that were phrased differently, so we want to make sure that the team has their opportunity to review those. And be in agreement that this matches what you had in mind.

ERIC OSTERWEIL: Okay. I was looking at the first paragraph. Is this one of them? Shall review the extent to which –

UNIDENTIFIED FEMALE: [inaudible] what underline is the category?

EMILY TAYLOR: [OIC.]

ERIC OSTERWEIL: [OIC.] Alright, cool, so we'll skip that. "Measures and evaluations of security efforts." What is the question there?

UNIDENTIFIED MALE: [inaudible]

EMILY TAYLOR: James wants to come in.

JAMES GANNON: A point of order almost. So, if we [filled in] through this list, there are things here that are in no way relevant to what we're doing now. So, I think if we want to do our yes, no, consider on this list, we need to take a five-minute break, trim it and then trim it to actual things that are scope items for us and then come back and do our yes, no, clarify on

those. Because as it stands now, we have questions that are relevant to our process but not to the actual items like we've been doing above.

UNIDENTIFIED FEMALE: Yes, [inaudible]

ERIC OSTERWEIL: Okay, cool.

JAMES GANNON: If we want to break for five minutes, clean this up and come back, or what [inaudible].

ERIC OSTERWEIL: Yes, I propose that… Does anyone object to breaking for five minutes while we do the administrivia and come back and resume? One, two, three. No objections. Break for five minutes.

[BREAK]

EMILY TAYLOR: Sorry, just to calm any nerves around the table, anything that we do in this group will be subject to our terms of reference, within our terms of reference, which itself is heavily based in the Bylaws. So, a lot of these subjects that we're whipping through are wide, and a lot of them involve things that don't involve ICANN. Stay with it. We will return and

we will reduce our level of input according to our terms of reference and the Bylaws. So, I just wanted to keep reminding everyone that we're all on the same page on that. Okay?

ERIC OSTERWEIL: Thank you. Yes. Okay, so I'm going to start off with what is the scope of ICANN threat model. Sorry, I thought it was funny. We're doing full pass greenlighting again just to sort of clarify the rules. Yes, no, clarify. If there's a dissention about whether it's a yes or a no, it becomes a clarify so nobody can unilaterally yes or no something. There has to be an agreement to get [inaudible] and then...

So, "Measurement evaluation security efforts. What is the scope of ICANN threat modeling?"

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Yes, cool. "Is DNSSEC an ICANN security effort?"

UNIDENTIFIED MALE: No.

ERIC OSTERWEIL: Yes. Wait, did I hear a no?

UNIDENTIFIED MALE: No.

ERIC OSTERWEIL: No, okay, so it becomes clarify.

UNIDENTIFIED MALE: Yes.

ERIC OSTERWEIL: Okay. "How effective is ICANN risk management?"

UNIDENTIFIED MALE: Yes.

ERIC OSTERWEIL: Yes. "[inaudible] DNS abuse lifecycle."

UNIDENTIFIED MALE: Clarify.

ERIC OSTERWEIL: Clarify. "If and how ICANN's security efforts relate to the DNS."

UNIDENTIFIED MALE: Yes.

ERIC OSTERWEIL: Okay. I'm not giving you guys a lot of times, so I'm just listening very carefully. "How ICANN measures the effectiveness as security efforts?"

UNIDENTIFIED MALE: Yes.

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Okay. "What are ICANN's security efforts?"

UNIDENTIFIED FEMALE: Sure.

ERIC OSTERWEIL: "What are the benchmarks and good practices for successful security efforts?"

UNIDENTIFIED MALE: Clarify.

ERIC OSTERWEIL: Clarify. "Evaluate the DNS abuse threat mitigation measures, deficiencies, processing speed."

UNIDENTIFIED MALE: Clarify.

ERIC OSTERWEIL: Clarify. "Recommend upgrade and revision of security and stability procedures and action plans, review ICANN security procedures."

UNIDENTIFIED MALE: Yes.

UNIDENTIFIED FEMALE: Yes.

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: Yes, it looks like the two things got stuck together.

UNIDENTIFIED FEMALE: [inaudible]

UNIDENTIFIED MALE: [Clarify.]

ERIC OSTERWEIL: Okay, yes. [Dot] review is probably supposed to be a new one. Yes, exactly. Okay, "Organizational. What are the indicators for successful implementations and intended effects?"

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Okay. "RSSAC recommendations automatically considered as ICANN efforts toward SSR."

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Okay, good. "What are the changes to ICANN SSR with the IANA Transition?"

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify. Okay.

"How to interact with outside organizations." Clarify.

"What are the Key Performance Indicators?" Yes.

"How can we measure the extent of ICANN's success in implementing security efforts?" Yes.

"What is the significance of both internal and external and directly affect and/or affected by?"

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify. Yes, Steve?

STEVE CONTE: I recognize I'm staff and I'm not sure how much input you want from staff. The one with SSAC, I'd like to clarify on that if we could. Thank you.

ERIC OSTERWEIL: Cool. We're more than happy to hear from staff.

UNIDENTIFIED FEMALE: On which one?

STEVE CONTE: On SSAC.

UNIDENTIFIED FEMALE: Okay.

EMILY TAYLOR: And observers.

ERIC OSTERWEIL: Okay. And observers, yes.

Future Challenges: "Explore forecasting research on the Internet capacity performance."

UNIDENTIFIED FEMALE: [Inaudible].

ERIC OSTERWEIL: Okay, clarify.

"Should SSR consider the future?" Yes, okay.

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify. Okay. I will just listen.

"How do we assess future challenges to security and stability at DNS?"

UNIDENTIFIED FEMALE: Yes. [Inaudible].

ERIC OSTERWEIL: Yes. [Probably].

"What are the actual and potential challenges and threats?"

UNIDENTIFIED MALE: Yes.

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Yes. Okay. So this is just framing language: "Shall review the extent to which prior SSR recommendations implemented [and the] extent to which such implementation of such recommendations has resulted in the intended effect."

Okay so approaching to assessing – "How can we assess the efforts of prior recommendations, SSR1 implementation? What were the impacts?" Yada yada. This is SSR1 [redo].

EMILY TAYLOR: I think that might be two in one [squished] into one bullet point.

ERIC OSTERWEIL: Is it?

EMILY TAYLOR: I think so.

ERIC OSTERWEIL: Okay.

UNIDENTIFIED MALE: [Inaudible].

UNIDENTIFIED MALE: Clarify. Clarify the whole sucker.

ERIC OSTERWEIL: Okay. So we're going to break it up. "How can we assess efforts [to] prior recommendations?" If we redo that one, is that a yes/no/clarify?

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify. Okay, cool.

"SSR1 implementation. What were the impacts, results…" Clarify, okay.

"How do we get an understanding of what SSR1 recommendations have been implemented?"

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Yes. Okay.

"Which implementation measures form what were critical are deemed insufficient?"

UNIDENTIFIED MALE: Yes.

UNIDENTIFIED FEMALE: [Inaudible].

ERIC OSTERWEIL: Okay, clarify.

"Are there measures in place to assess SSR on work?" That's SSR1?

UNIDENTIFIED FEMALE: SSR1 work.

ERIC OSTERWEIL: Yeah.

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: So SSRI. That's different. Sorry. I thought that was pretty funny.

"Which extent of SSR1 recommendations is implemented?"

UNIDENTIFIED FEMALE: Implemented, yes.

ERIC OSTERWEIL: Yes. Okay.

"Review and grade importance and way it is implemented."

UNIDENTIFIED MALE: Clarify.

ERIC OSTERWEIL: Clarify. Okay.

"What are the indicators of SSR2 would want to use to measure success of security efforts?"

UNIDENTIFIED FEMALE: Yes.

UNIDENTIFIED MALE: Yes.

ERIC OSTERWEIL: Yes. Okay. That one was too much fun to say no to.

"How are we distinguishing operational stability and security from the measures that stem from compliance issues?"

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify. Definitely.

"How can we work on global policies?"

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Post Transition Factors: "Which recommendations are still critical for SSR since the Transition?"

UNIDENTIFIED MALE: Clarify.

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify. Okay.

Uncategorized – "Collect input from the community on how ICANN should improve on SSR."

Okay, that's a yes.

Alright. "May assess the security, operational stability, and resiliency, matters, both physical and network relating to the coordination of the Internet's system of unique identifiers."

Okay, so definitions. "What does security, stability, and resiliency, mean?" No.

EMILY TAYLOR: No, because I think we've done it.

ERIC OSTERWEIL: Yeah. James?

JAMES GANNON: This is the type of stuff that I think a lot of this we need to just put and clarify and then when we speak about it later, throw it out because we've already done it. So let's just put "clarify" on a lot of these.

ERIC OSTERWEIL: Okay. So you want to change that one to a "clarify." Okay, clarify.

"What do we mean by 'unique identifiers'?"

Clarify, okay.

"What is meant by both physical and network?"

JAMES GANNON: Clarify.

ERIC OSTERWEIL: Clarify.

"What does 'interoperable security processes' mean?"

JAMES GANNON: Yes.

ERIC OSTERWEIL: Yes. Okay.

"What has been or could be the impact of evolution and the number and type of devices in the DNS?" Clarify.

"What are the parameters to secure the DNS?" Clarify.

"Which portion of the Internet system of unique identifiers does ICANN not coordinate?"

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Okay.

"Where is the best source to determine most pertinent aspects – e.g. networking scope is wide and covers many actors in the community."

UNIDENTIFIED FEMALE: I don't fully understand the question so I'd say clarify.

ERIC OSTERWEIL: Okay, clarify.

"What is the main responsibility of the SSR2 Review Team?" I'd clarify. That one makes sense to me.

Okay. Procedures – UI procedures – clarify. I'll just [inaudible] that one myself.

Okay. Interoperable security processes – "How is this current address in domain name protocols addresses [in] DN protocol addresses?"

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify. Okay.

"What is the current state of ICANN in disaster and operational recovery planning?"

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Yes. Okay, cool.

"Identity and access management."

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify. Okay.

"Operational impact on security and stability." Clarify. That's very broad.

"What is ICANN's internal level of risk and how it [minute] and how is it managed?"

UNIDENTIFIED FEMALE:		Clarify.

ERIC OSTERWEIL:		Okay, clarify.

				"Conduct performance indicators and benchmarks of SSR."

UNIDENTIFIED MALE:		Clarify.

ERIC OSTERWEIL:		Clarify.

				Uncategorized – "Explore DNS analysis opportunities – malware."

UNIDENTIFIED MALE:		Clarify.

ERIC OSTERWEIL:		Clarify.

				"Is the assessment limited to those organizations ICANN has policy inputs to?"

UNIDENTIFIED FEMALE:		Clarify.

ERIC OSTERWEIL: Clarify.

Physical security – "Should we consider KSK signing physical security ICANN headquarters?" I think those are three different things.

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Let's clarify all those things.

"How can we ensure the security and reliability of unique identifiers and how do organization policies affect assessment?" Clarify.

"May assess conformance with appropriate security contingency planning framework for the Internet's system of unique identifiers" is just a broad category.

"How do we assess definition of scope of Internet system of unique identifiers?" Yes.

UNIDENTIFIED FEMALE: Yes.

UNIDENTIFIED MALE: Clarify.

ERIC OSTERWEIL: Did somebody say no? Oh, you said no. Okay. Let's clarify, sorry.

"When it says conformance, to what extent?"

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify.

Overall process – "The implication of security, stability, and resiliency, of DNS as per Bylaws." Clarify.

"What are the key point who address secure, reliable, and stable, DNS?" Clarify.

"How can we address the operational issue?"

UNIDENTIFIED MALE: Clarify.

ERIC OSTERWEIL: Are you sure you don't want to just say yes? That's a good question. I'm going to clarify that question later on.

IANA Transition – "What is the impact of moving the IANA services to PTI? How will this be monitored?" Clarify, okay.

"What contingency planning has taken place as a result of the CWG-CCWG?"

UNIDENTIFIED MALE: Yes.

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify.

Contingency planning – "What measures are taken to ensure relevance and applicability of contingency plan?"

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify.

Contingency planning framework – "What does that mean for DN protocols addresses?" That's like for the number four. Clarify.

"What is the appropriate security contingency planning framework?"

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Okay, yes.

"Who is responsible for the current contingency plan?"

UNIDENTIFIED MALE: Yes.

UNIDENTIFIED FEMALE: I say clarify.

ERIC OSTERWEIL: Okay, clarify.

UNIDENTIFIED FEMALE: [Inaudible] goes beyond security and stability.

ERIC OSTERWEIL: Okay.

"What is meant by 'the appropriate security contingency planning framework'?" Clarify.

Uncategorized – "What is ICANN doing in the area of interoperable security STDs to monitor ITHI?"

UNIDENTIFIED FEMALE: Yes.

UNIDENTIFIED MALE: Yes.

ERIC OSTERWEIL: Okay. Yes.

"How the end user feels secure, reliable, and stable?"

UNIDENTIFIED MALE: Clarify.

ERIC OSTERWEIL: Clarify.

"Does this review look only internally and ICANN processes?"

UNIDENTIFIED MALE: Clarify.

ERIC OSTERWEIL: Clarify.

"Who is responsible for the maintenance and upkeep of the unreadable?" Clarify.

"Area of assessment may assess maintaining clear and globally interoperable security processes for those portions of the Internet system of unique identifiers that ICANN coordinates."

Definitions – "What is meant by 'globally interoperable security processes'?"

UNIDENTIFIED MALE: No.

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify.

"What aspects of the unique identifier space is relevant to the definition of 'security processes'? "Okay, yes.

UNIDENTIFIED FEMALE: I don't understand that.

ERIC OSTERWEIL: Is this the [IETF] –

UNIDENTIFIED FEMALE: Clarify on the last one.

ERIC OSTERWEIL: This is IETF, no?

UNIDENTIFIED FEMALE: Clarify.

UNIDENTIFIED MALE: Yes.

ERIC OSTERWEIL: Okay, we have to clarify it but I couldn't even parse it.

                         Abuse – gTLD and ccTLD – "gTLD abuse mitigation."

UNIDENTIFIED MALE: Clarify.

ERIC OSTERWEIL: Clarify.

                         "Global abuse policies recommendations."

UNIDENTIFIED MALE: Clarify.

ERIC OSTERWEIL: Clarify.

"How does ICANN compliance impact SSR?"

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Yes.

gTLD compliance analysis – "What are the SSR issues with new gTLDs?"

UNIDENTIFIED MALE: Yes.

ERIC OSTERWEIL: Yes.

"ccTLD abuse" – I think it's probably TLD – "abuse mitigation."

UNIDENTIFIED MALE: No.

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify. Okay.

Assess effectiveness – "How effective is ICANN's coordination effort with the IETF and others?"

UNIDENTIFIED FEMALE: I say "clarify."

ERIC OSTERWEIL: I'd go with clarify on that one. It's a big, slippery, slope.

"How effective are ICANN's security efforts to known threats and preparation for future threats?"

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Okay, yes.

Emergent threats – "What emerging technologies are trends we should consider?"

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Yes, okay.

Uncategorized – "Root server stability security, how is root server stability and security?"

UNIDENTIFIED MALE: Clarify.

ERIC OSTERWEIL: Clarify, okay.

"How DNS works with secure, reliable, and stable." Look up text.

UNIDENTIFIED FEMALE: I don't know what that means.

UNIDENTIFIED MALE: Clarify.

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Okay, clarify.

And then there's some extra thoughts at the bottom – and this is not from brainstorming from [before] so we're back on the main track again.

"Understanding of malware and abuse vectors and mitigations."

UNIDENTIFIED MALE: Clarify.

ERIC OSTERWEIL: Clarify.

"Risk assessment and management."

UNIDENTIFIED MALE: Yes.

ERIC OSTERWEIL: Yes.

UNIDENTIFIED FEMALE: I'd clarify.

ERIC OSTERWEIL: Okay, clarify.

UNIDENTIFIED FEMALE: It's too broad.

ERIC OSTERWEIL: "Corporate data security and/or business systems."

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify.

"[Incident] response."

UNIDENTIFIED MALE: [Inaudible].

UNIDENTIFIED FEMALE: Clarify.

ERIC OSTERWEIL: Clarify, okay.

UNIDENTIFIED MALE: [Inaudible].

ERIC OSTERWEIL: Yeah, but we just got clarify so once we hear a clarify, that's the rule. The lowest common denominator.

UNIDENTIFIED FEMALE: I'm just going to move this last set up so it's not in the previous brainstorming session [inaudible].

ERIC OSTERWEIL: Okay, so now we are on to the fun part. We're at 11:30 and we're basically off schedule which is cool because I think we're doing something that's really important. We are before lunch, but we are potentially about to embark on something lengthy so we can either start it now or we can figure out something else to do with half an hour. But starting it now just means we stop in the middle and come again or we do a working lunch.

UNIDENTIFIED FEMALE: I think Cathy has a suggestion [inaudible].

JAMES GANNON: Before we embark on that lengthy exercise I would like us to do that in one chunk. I don't want us to start it, stop, and then start it again.

UNIDENTIFIED FEMALE: That's what I said.

ERIC OSTERWEIL: Here's the rub –

UNIDENTIFIED FEMALE: I'd like to move forward.

ERIC OSTERWEIL: We can't get food before it arrives and it's not here yet. So we are approaching an [inaudible]. One thing we can do is we can start massaging our list now into something more manageable and that doesn't involve the whole group, so it would give people a lot of free time to [ungiddyify] yourself.

DENISE MICHEL: Can we take a quick look at the Day 2 agenda just to see if there's anything on the agenda that we may want to pick up now, if people would like to pursue something else and I'm not sure when lunch was scheduled either. Was it 12:30…

So may I view this work as integral to moving the team forward? So my preference would be to use the next hour to continue working rather and understanding that we're going to have to take a break and eat and then come back to it.

EMILY TAYLOR: Can I make a suggestion as well, which is that if we need to take an extra half hour, we've had quite a few breaks this morning. We could have lunch – the lunch can just sit there for a bit so we can take an hour and a half for the next section which gets us more of a chance of getting through it.

ERIC OSTERWEIL: Okay. I think that all makes sense and I also would point out that I think we're able to do a working lunch if we have to, though it may be suboptimal in a lot of ways, we can take our food right in here.

Alright, so in that sense what I propose we do now is we go back to the list – I sort of feel like we're driving staff real hard so I don't know if we should use the table or the Google doc – but regardless, we go back to wherever the canonical list is now and we – there's the agenda up on the screen if people want to look at it.

Go ahead, James.

JAMES GANNON: I'm going to make a suggestion. I know Bernie has a good few in the list already. I don't know if this melds with what you're plan was but [of the ones] I would like us to move across to the table now and we can start discussing the ones that we need to discuss, the ones that are not yes or no. And while Bernie is moving the rest of them in because some of these will need a little bit of time to discuss, so that'll give more time for it to be fleshed out.

UNIDENTIFIED FEMALE: Where's the table?

BERNARD TURCOTTE: [Inaudible] the Google doc so you can just go through it while I [inaudible].

UNIDENTIFIED FEMALE: Have you shared the link with –

ERIC OSTERWEIL: Principally it just needs to be up on the screen that we can stand there but it should be shared out so people can –

While things load, this is the plan as I understand it – we're going to put this up on the screen, people are welcome to look at their own local versions and we'll go down the list as it forms looking at the "Clarifies" in order and the job with the "clarifies" is to basically either A) explain them, B) modify them, or C) nuke them, so that we wind up with a table full of "yeses" – where "yes" is implied by presence in the table [at the end].

As the list continues to [create] at the bottom [and we'll] work towards it, eventually we'll sort of reach parity.

DENISE MICHEL: Quick question – can the staff clarify what the status of this table is? Are you still adding things that we said yes that we asked for clarification on? What does this table currently represent?

BERNARD TURCOTTE: This table is [inaudible].

DENISE MICHEL: What about it? Is this just the clarification ones? Is it just the "yes" ones?

BERNARD TURCOTTE: [Everything].

EN

DENISE MICHEL: [Inaudible] capture the ones whether we said "yes" or "clarify."

ERIC OSTERWEIL: Are you putting those in there?

UNIDENTIFIED FEMALE: [Inaudible].

ERIC OSTERWEIL: They are? Okay. One thing we –

BERNARD TURCOTTE: I'm [porting] the line from the Google Doc into the box.

ERIC OSTERWEIL: Okay, cool.

BERNARD TURCOTTE: That's it. So you asked it: Yes/no/clarify.

ERIC OSTERWEIL: Okay, cool. Thank you very much.

EMILY TAYLOR: And it's a work in progress at the moment because you're following up from the conversation and there's quite a lot to go on at the moment.

ERIC OSTERWEIL: Thanks a lot, Bernie. We're going to go through this and we'll just keep going while you're modifying it and so when we come to something that winds up being a "no," we'll strike it. Is that cool? Alright. Just to make sure.

Alright, this is the plan unless anyone says so now, we're about to embark and it's going to be a lot of fun.

UNIDENTIFIED FEMALE: [So what question are we answering again]?

ERIC OSTERWEIL: We're going to go through each of these things. I think what we're going to try and do is we're going to try and come up with a list of things that we will then go and later – like the next step after this will be we will try to normalize, de-duplicate things. "Oh, we already said that. That's like issue number whatever the heck," and then we'll do an exercise in taxonomy after that – which of these things kind of group together, which of these things whatever? And then maybe we'll talk about sub-teams.

UNIDENTIFIED FEMALE: Okay.

CATHY HANDLEY: I think one of the things that you have to look at [because] I think there are things that are on the list as we went through the process that may not necessarily be under ICANN's purview. And we're going to have to take a look at the list that way also. I think that will help us.

ERIC OSTERWEIL: James.

JAMES GANNON: So those items should be marked as "clarify," and that's exactly [so] my concept in my head – and please tell me, Eric, if this is not matching with you – we're going to go down this list, right now we get to number nine and we get our first "clarify," we have a discussion about it, we either turn it into a "yes" or a "no," we might tweak the language to make it a yes, we might say, "No, we can't agree on it," or, "No," or whatever, and then we move on to the next "clarify" until we have a list of "yeses", and then we do our mapping and everything else after [that].

ERIC OSTERWEIL: Go ahead, Cathy.

CATHY HANDLEY: In response it's just in that "clarify" session, look at it, to some of it we have to clarify to figure out what they're saying and but we also have to clarify if it falls under not our remit, under ICANN's remit.

ERIC OSTERWEIL: Okay, so I've been doing a bad job of [queue management]. Zarko [inaudible].

ZARKO KECIC: I just wanted to add that this is not an exhaustive list. So if you get some idea, let's find a way to put new ideas in.

ERIC OSTERWEIL: Yeah, I think we want to do that. I think we want to make sure not to wind up iterating forever, but yeah, absolutely. At some point it's like we really have to stick something in, yeah, we'll break, there's no decorum we have to worry about with that.

Emily?

EMILY TAYLOR: Do we have an option of, "This is too hard for us to decide at the moment. Let's move on to things we know we can agree on" – with the "clarify" or does that break things –

ERIC OSTERWEIL: Yeah, I think that's a really good idea. We need to have a parking lot –

EMILY TAYLOR: We can keep them as "clarify," but a –

ERIC OSTERWEIL: We should probably move it to a parking lot somewhere.

                          James, go ahead.

UNIDENTIFIED FEMALE: [Inaudible].

JAMES GANNON: No, this is nothing to do with project management. This is to do with me as a Review Team member. Yes, we can do that but that needs to be time limited. We need to come to a point very, very, soon where we're working. And if we keep putting things off, no matter what they are, what the topic is, or what the reasons are, we have to come to a point where we have our scope of work done.

ERIC OSTERWEIL: Emily and then Zarko.

EMILY TAYLOR: I [Inaudible] yes. I totally support that. I'm proposing a sort of triage approach in that I think we're going to end up with much more than we can [read any] bunch of human beings can reasonably do, and ultimately it's a bit your parking lot analogy is that there are things that

are still causing us difficulties about whether or not we should be doing them, have a go but also in the interest of time and not getting stuck that we keep a sense of momentum because I'm personally finding the sense of momentum and progress really, really, helpful. I thought I'd just suggest that. I don't think it should be our default. It should be like, "We're stuck on this. Let's move on."

ERIC OSTERWEIL: Zarko?

ZARKO KECIC: I just wanted to add that [I've been] talking to people in the room, most of you think that we will finish today. We're not going to finish long time and we'll be adding tasks into the list. So it is important for now to have high level tasks and dig into it as we progress.

ERIC OSTERWEIL: Okay. Thank you.

                            James?

JAMES GANNON: Okay, so project manager again – can we then at least commit by the end of today we will set a closing date for our [user] requirements that this document that we will set a date either one week or two weeks or whenever from now, that our core requirements are done? Because if we leave this open forever then we will be essentially restarting forever.

And then my second point is that if we are putting things into a "still needs discussion" parking lot, we again need to set a closing date for that.

DENISE MICHEL: Both things that you mentioned would fall into our work plan, and part of our objective coming out of this meeting is a work plan with some timelines and some deadlines in it.

ERIC OSTERWEIL: That's totally fine with me. I would like to make a proposal in that vein that's maybe a little bit different so we can not agree to it, but I would propose that by the end of the day we aim to have a set of things that we broadly classified as things that we need to work on that have some consistency to them. That means that we've gone through this list, we've [de-normalized] a few or maybe not, but we've decided that these are things we're going to work on. We can decide it through the course of the day. Whether we can decide whether we want to have sub-teams on them or just that we know we need to work on them and the sub-team discussion comes later or decide that we don't want sub-teams, but by the end of the day we can walk out of here saying we really know that there's things that we know we need to do and we're getting ready to do them. And then that list can grow over time, it can iterate, we can change form, etc. but by the time we walk out if someone said you have to do something, are you prepared to do it? We could.

Alright, so we'll go to James.

JAMES GANNON: I know I'm talking a lot but I'd like to push it further than that. I really want our work structured by the end of today. I really want to know how we are going to start tackling these ideas. If building the list is the start of that process, by the end of today we've all flown in from around the world, I want to know how we're working, whether it's sub-teams or what way we're doing it, I would like our structure in place by the end of today.

ERIC OSTERWEIL: Okay, Cathy?

CATHY HANDLEY: Do not throw anything at me because does anybody have someplace they have to be at 5:05? Is anybody on an airplane tonight?

UNIDENTIFIED MALE: [5:30].

UNIDENTIFIED FEMALE: [5:30]?

CATHY HANDLEY: You are?

UNIDENTIFIED MALE: Eight.

CATHY HANDLEY: Eight, nine. So we can work until… you can stay here until 8:30. What James said, I think we really need to try and come out of here with something concrete.

ERIC OSTERWEIL: Zarko, are you in queue?

ZARKO KECIC: Yeah, I just personally agree because we cannot do that today. We will have some task structure, but we still don't know what has to be done under many tasks. So how you're going to structure team, we don't know what has to be done.

ERIC OSTERWEIL: What we can do is structure the team to assess what needs to be done, but now we're putting angels on the pin heads. So how about this – how about we state an objective and we don't tolerate… I'm sorry, we agree we may or may not make it but by the end of the day we might be able to… We could choose to strive to have a list of objectives that we will complete as the SSRT 2, and that that list may change and we may not be able to do our thing and we may have to [inaudible] but nevertheless by the end of today having just flown in from all over the world, our objective is these are things that we need to do, these are the pieces

that we think comprise those things, and we might even say these are the sub-teams that are attacking them.

Zarko.

ZARKO KECIC: Yeah, we'll need sub-teams to do tasks that we already agreed to, to connect different tasks to Bylaws and the other ICANN documents. And while doing that, team can dig deeper and decide what other tasks and areas should be covered by this. So in that case we will have a clear picture what task requires and who can do that.

ERIC OSTERWEIL: Okay.

Boban?

BOBAN KRSIC: Can we start to clarify the open issues and moving along –

ERIC OSTERWEIL: Let's do it right now. I sense a serious amount of violent agreement on that, so we are now moving forward. So just so I know who to look at, who's driving the screen?

UNIDENTIFIED FEMALE: That's me again.

ERIC OSTERWEIL: Okay, cool. So I think what we need to do first is go to the first "clarify," please.

        Okay, so #9 – "Improving the security of unique identifiers includes threat mitigation, identifiers [ET] requires clarification."

        James, go.

JAMES GANNON: I think I may be one of the clarifiers on this, so "unique identifiers" to me means numbers, names, and protocols, and ICANN has different roles in the security of those three things. So we need a little bit more clarity on what this line item is as a work item because, for example, there is a hell of a lot more responsibility on the name side than there is on protocols, for example.

ERIC OSTERWEIL: Okay, so before I take to the queue let me just propose a way to do this. When we get to a "clarify," when you have something to say and we're going to poll the room just say by default a "clarify" is going to be a "no" unless someone says something, and the clarification if you want to say like James just now said basically, "I have some concerns about this," I would propose that when you comment on a clarify you either structure your comment as, "This is how I would turn it into a yes," or, "This is why I want to turn it into a no." That way we can say only people say like, "I didn't know what it meant because that really belongs partially in the IETF's purview and I'd rather not touch it, I'm saying no." Or I could

say, "This is how I'd make it a yes." Is that the fair decorum sort of [inaudible] okay?

JAMES GANNON: [Inaudible] turn my comment into that then, into that suggestion?

ERIC OSTERWEIL: If you don't mind, yeah. That way then we'll take the queue Denise, Zarko, Emily.

DENISE MICHEL: May I clarify first? Going back to the reminder that Emily provided, that the caveat on all of this is that it's within ICANN's scope and mission and responsibility. So if your concern is that this could be construed as covering things that are outside of ICANN's responsibility so [inaudible] I need a little more information about it.

JAMES GANNON: Just exactly what [I'm going to] clarify. I would propose that we break this out into three work items, which is improving the security of the DNS, improving the security of the number space, and improving the security of the protocol space as they are three different things within ICANN's remit that need to be treated in three different ways.

DENISE MICHEL: So this is where it gets a little bit unwieldy. If you go back to the original Google Doc, this was a kind of a broad statement and then it had a whole big list of [very] all the specific elements underneath it.

EMILY TAYLOR: [Inaudible] heading.

DENISE MICHEL: It was a heading. You're talking about a heading that had even more details than you're actually indicating.

ERIC OSTERWEIL: Okay. Cathy?

CATHY HANDLEY: I don't argue with what Denise said about having several items, however, you cannot assess the three unique identifiers on the same plane. They are very, very, different and ICANN is not responsible for some of that security. When it comes to protocols and IP addressing, that's done through IETF, and ICANN has no influence over them. They may have influence over – and I can talk to this because it's the one I know – they may have influence over the discussion between someone at PTI allocating a block of addresses but that is not the same as the security of addressing or ASNs or protocol parameters. Thank you.

UNIDENTIFIED FEMALE: [Can staff] drop in all the things you've left out of that in the table? So the table should reflect everything that's in the Google Doc and you've left out a whole… and there's a number of bullets there that I don't think are reflected.

[EMILY TAYLOR]:   I think they are reflected [inaudible] separate [lines in the table].

UNIDENTIFIED FEMALE: The table jumps from "Improving the DNSSEC," so it leaves out a whole number of bullets.

BERNARD TURCOTTE: Yeah, in certain cases I've left out some of the [substance].

UNIDENTIFIED FEMALE: Yeah, and I think that's where James and others are [inaudible].

EMILY TAYLOR: I have a proposal to turn this into a yes, which would be to add "within the scope of ICANN's mission," to the bit after [inaudible].

ERIC OSTERWEIL: So taking the moderator Chair hat off, I have a lot of the same concerns with this one that Cathy brought up. I think this just paints just too wide a canvas for us to have to address, and I think to the point where if we wanted, for example, [to] just pick one of those identifier spaces –

domain names – and we wanted to address it in this team, we'd have to be extremely framing or we'd have to use extremely strong framing language to make sure that we were talking about the part of the DNS that mattered, or that if we were talking about different part of DNS, why it mattered within our purview. So I think I feel like this one's too broad. I feel like if there's something in there that people want to address in this Review Team, we should just rewrite it and say what it is you want to address.

Maybe a good sort of leveling thing to say here is, if someone says like, "Hey, that was mine," please nobody take offense at any of the nuking that we're doing going forward. This is just a structural work plan. So with all that sort of said, if somebody wants to jump in and say like, "This is something that that makes me think we should review," this is about I think about probably to get nuked unless somebody says there's something about it that they like.

Denise?

DENISE MICHEL: I'm sorry, so what's the suggestion?

UNIDENTIFIED MALE: [Inaudible].

EMILY TAYLOR: I think we'll come back to [inaudible]. Sorry to interrupt, Denise. As long as we don't lose the concept of improving security in some way, I'm

really [comfortable]… I totally understand and accept the sensitivities that you've all outlined so I'm sorry to… If there's something about seeing your initials next to something that makes you innately want to defend it, because it was mine initially.

I'm really comfortable losing it. I just don't want to lose the sense of making improvements, but I think that that will come through naturally.

DENISE MICHEL: I'm not comfortable just jettisoning the whole… and we still haven't reflected all of the bullets in there.

UNIDENTIFIED FEMALE: I'm trying [Inaudible].

DENISE MICHEL: Yeah, I think it's a formatting issue, isn't there? This is I think less than ideal. Yes, so I think we absolutely need – my opinion is that we absolutely need to capture what might be some pretty critical ICANN responsibilities and activities in the [area of] unique identifiers and threat mitigation, and we need to be specific. So I'm not comfortable just throwing everything out and I would prefer to work with those who have questions or need to winnow it down to make sure we get to an agreement.

ERIC OSTERWEIL:	Okay, so Kaveh you can put your [bar] up so I don't recognize [whose hand is that]. Kaveh, Elaine, and then Zarko, you –

UNIDENTIFIED MALE:	[Inaudible].

KAVEH RANJBAR:	I think Denise actually had the answer in her sentence by mentioning that ICANN activities. So I think we should look at what ICANN already does in these fields and not about security, what they do with unique identifiers and look at those processes and we can ask the staff what we're dealing with in regards of unique identifiers. And then we can choose from those processes or all of them or none of them to see how we can improve security of them or assess if they are helping security and stability of the Internet.
	So I think we should start from what ICANN is doing – ICANN activities – that's the key word.

ERIC OSTERWEIL:	Okay. We don't all have to agree with everything, so rather than me sort of like… I basically don't understand how we frame that in this question so maybe we need to –

KAVEH RANJBAR: I think I know why we can't, because if you look at the level of these things they range from very, very, high level topics to questions about very specific things. So I don't think you can [any ways] group or get –

ERIC OSTERWEIL: No, I was just talking about this one –

KAVEH RANJBAR: I know. So I think the most practical one is to basically ask ICANN for all of the procedures they have. You can even look at the organization chart and say, "Hey, this is the compliance. What processes do you have?" And then you can say, "Okay, these processes we don't care. This one we care," and/or, "Which processes do you have which are related to unique identifiers?" and then look at those. Because these are the ICANN activities. We are not going to invent activities for ICANN. We don't have… this is not within our remit, correct?

So the activities they already do, we should ask, understand them, and then decide if we want to go or not. And that would be our improvement to security of unique identifiers because I can come up with I don't know BGPSEC. ICANN does nothing in BGPSEC, correct? But that will definitely improve the security of unique identifiers.

ERIC OSTERWEIL: Well, we could debate that.

KAVEH RANJBAR:	I know we can debate but that's another point I have because most of these things are for that's why you have the constituencies. If they were like binary true or false, then you wouldn't need groups of people to make decisions in dispute, correct? So it's very important to focus on ICANN activities. That's my point.

DENISE MICHEL:	So if this said, "ICANN activities aimed at improving the security of unique identifiers," that would be acceptable?

KAVEH RANJBAR:	If you add "current" to that, I will agree – "current ICANN activities aimed at …"

ERIC OSTERWEIL:	[Inaudible]. Okay [inaudible], yes Zarko.

ZARKO KECIC:	I think I'm close to what you just said. I was about to suggest that we add "ICANN role in improving [inaudible]" – I think it's the same but [inaudible] can agree. It's let's look at the ICANN role in improving the security because [inaudible] many parties involved so what [is the ICANN for me] I was about to suggest ICANN role but we can also go with ICANN activity or whatever.

DENISE MICHEL: Again, that was the caveat on every single thing in this table – ICANN;s role – but if #9 is changed to "ICANN role in improving the security of unique [identifiers]."

ERIC OSTERWEIL: yes, okay. James?

JAMES GANNON: Okay, can we say yes to the chapeau and go through the bullet points [inaudible]?

ERIC OSTERWEIL: Yes. The bullets under #9 – okay so please scroll down a little bit. Thanks.

                        "ICANN role in improving ICANN activities in improving the security of unique identifiers includes threat mitigation" – identifiers requires clarification – "[Authoritative] domain name servers and recursive and stub resolvers." That to me feels way too broad for ICANN – way too broad.

KAVEH RANJBAR: And if it's the ICANN role I disagree. I think. The word "activity" is very key.

ERIC OSTERWEIL: Okay. James?

JAMES GANNON: Okay, I think we're on the same page – what role does ICANN have at that level of the DNS? Very little.

[ERIC OSTERWEIL]:   [Inaudible].

JAMES GANNON: Authoritative domain name servers, yes. My proposal is take out "and recursive and stub resolvers," as ICANN has no authority/remit/role.

ERIC OSTERWEIL: Steve?

STEVE CONTE: I totally agree about the recursive and stub resolvers. That's way, way, way, wide. ICANN through PTI IANA does operate some authoritative name servers at a TLD level and maybe [such way] the ones that they operate and [review] those.

ERIC OSTERWEIL: Right. So ICANN operates some name servers. ICANN is in charge of delegating to other name servers. And there's a lot of name servers in the world that ICANN has absolutely nothing to do with so we probably just need to be a little more specific. Are we going to investigate ICANN's operational acumen for this [inaudible] is run by ICANN? Are

we talking about any name server that ICANN is delegating to? Or are we going to leave that broadly in the question? The goal of this is to give us a work item. So we don't have to decide right now what ICANN does and doesn't do. We just have to decide what we're going to look at when we get there.

We can definitely leave "authoritative name servers" in there and we can figure out later.

UNIDENTIFIED MALE: Just to clarify my comment – I was referring to like .int and things like that in which ICANN is a top level domain provider.

ERIC OSTERWEIL: Yes, and numerous root server instances all around the world, for example, yeah absolutely.

Let's change that sub-bullet to just say, "Authoritative domain name servers," and we can figure out the details when we get there.

Emily?

EMILY TAYLOR: And we can now delete "identifiers requires clarification" because I think we've done that.

ERIC OSTERWEIL: Yeah, so the first bold sub-bullet can get yanked and then "domain name registration data registries, registrars, and registrants…"

James?

JAMES GANNON: Denise, do you want to go first?

DENISE MICHEL: [Inaudible]. Sorry.

JAMES GANNON: I have two minds about this one. Yes, it technically impacts the security of the DNS. However I'm seriously, seriously, concerned about overlap of work. We have a PDP, we have a WHOIS Review Team, we have a million different items out there in ICANN at the moment who are specifically looking at this bullet and I'm going to fight tooth and nail for us to not also be looking at it, to be honest. It's replication of work that is a million places elsewhere in ICANN.

ERIC OSTERWEIL: Before Denise goes and I just want to be real quick and just interject a perspective, no hat on at all. One thing that we can do is we can say that this is important to SSR and we can point at those that are doing it. I think we want to make sure that whatever we're doing as we go through this that we know that a holistic view of SSR doesn't mean we do all the work, it doesn't mean that we come up with all the

complexities, but we are at least holistic enough to say, "And this stuff is being done over there." So maybe we keep a bullet knowing that we can also result in a pointer. Is that fair?

Sorry, go ahead, Denise.

DENISE MICHEL: Yeah, I think a number of these elements are quite critical to our mandate and fall under our Terms of Reference and the reference in the Bylaws. I take your point that there is going to be naturally some overlap, but I think it's important for us to capture this and some of the work the OCTO and SSR staff are currently doing that impacts SSR.

ERIC OSTERWEIL: Okay, so do we have convergence? Okay. We're good. So we're going to leave that in there knowing what we can do with it when we get there.

"IP addresses and autonomous system numbers ASNs employed by the…" I know Cathy's totally on board with us taking care of that global Internet routing system. We should handle that for you all right. Cathy, I'm going to channel that you have a comment on this one.

CATHY HANDLEY: Thank you. I don't think it should be on there because there's a set of security measures that are taken by all the RIRs when it comes to doing any allocations and that, and I don't see that ICANN has a – I have to scroll up here – has an active role in doing anything with that other than individuals employed by ICANN that may participate in various for a that

affect it. But I just asked someone to explain to me or give me an example if they think it ought to be in there of what a security against, security of the unique IP addresses and what that would be and I don't think it should be in there.

ERIC OSTERWEIL: Okay, so I think I got Steve then Denise and then Emily and James, and then I'll throw my name in there if there's any…

STEVE CONTE: Thanks. I'm absolutely not going to come up with an example of that. I want to ask Cathy and the room, my understanding in my past long time ago experience of the role of ICANN or IANA within the sphere was to delegate sets of blocks of those addresses or ASNs to the relevant RIRs upon request and upon satisfaction of particular [automagical] formulas and things like that. So within that scope of ICANN functionality, is there a component of SSR, and if there is, should we be looking at it? So maybe I'm just reframing it or asking it a little bit more focused.

ERIC OSTERWEIL: Thank you. Denise?

DENISE MICHEL: Fully acknowledging the responsibilities of the RIRs, but to answer your question there is an IANA component to this. The Board of Directors is responsible for ratifying the global policies developed by the RIRs, so I think there's that. There's also the issue of [take] the Address

Supporting Organization and the RIRs are part of the ICANN community, I think it's premature to assume that the team would not ultimately recommend that the RIRs consider something. So even though ICANN staff isn't responsible for an operational activity, I don't think in my mind that doesn't mean that if in the course of our work something arises relative to SSR that we feel should be receiving more attention, more resources, there can be a broad recommendation that's not perhaps for ICANN staff but for other elements of the ICANN community to consider.

I would prefer to leave it on the table at this point for those and other reasons.

ERIC OSTERWEIL: Okay. Emily?

EMILY TAYLOR: While I do make it a rule of life never to disagree with Cathy, I'm mindful of what Eric just said about WHOIS. ICANN doesn't have to do it. We're mindful and aware and respect the limits of what ICANN's role is in relation to RIRs, ccTLDs, the IETF, and any number. But we need to take a holistic view, and that doesn't mean we have to do everything or that we have to say that ICANN has to do everything. But in my view it would be extremely odd for a Review Team that is tasked by looking at ICANN – the primary role of ICANN in coordinating the Internet system of unique identifiers and to leave IP addresses out of that – that would seem really odd.

ERIC OSTERWEIL: Okay. Thank you, Emily. James.

JAMES GANNON: Two points on this – I agree and disagree with Cathy. There is a very limited narrow scope of potential impact on the RIRs from the IANA side. I think that as an internal ICANN process should be in scope. But certainly the way that this is written at the moment I couldn't ever agree to it. I don't want any reference to global Internet [inaudible] systems in any of our documents ever because stuff like that is a [rattle] that we have no scope and no remit and no mandate or anything else to go near. And if we put in something like IP addresses and with regards to the internal IANA processes or something like that, I'm okay with, but the way it's written at the moment it can't [stay].

ERIC OSTERWEIL: Okay. Thanks. Kaveh and then Cathy.

KAVEH RANJBAR: I actually strongly disagree and I think we shouldn't have that at all because the arguments I heard can be used to basically justify any security incident in the world. I would even extend that to even sometimes further than Internet because many of these are linked to the unique identifiers. So because we don't have a justification that that would be I think that's already the reason not to look at that and include them because if we want to take that approach, then I have many this list has to be much, much, larger and I have many suggestions to add.

ERIC OSTERWEIL: Okay. Cathy and then me and then James are you back in the queue?

Cathy?

CATHY HANDLEY: Thank you, Eric. I'm a little confused by something Denise said. This is the review of the corporation of ICANN and how it's doing its security. I'm questioning whether or not – and if I'm wrong I'm wrong – we're going to be making recommendations to ICANN, to the ICANN community, for what they need to do, and everybody in there, which I think puts a lot of these things in a very different perspective because that also says we're going to make recommendations to IETF possibly on how they do things and that just seems to be getting larger and larger. And if I don't understand that, I look forward to an explanation but I have some real concerns about this group making recommendations on something that I think is really out of the purview of ICANN.

You don't have to take it out, but I'm just saying I think we need to keep in mind exactly what that little box is and reword some of these because I'm with Kaveh. If we start just putting everything like that in there and leaving it open, I don't want our recommendations to color folks' view of what we did and whether or not we as a team thought we could reach farther and we're the all-encompassing ICANN SSR2 Review Team that's going to tell everybody how to do everything. Thanks.

ERIC OSTERWEIL: Okay. So I think I'm going to jump in with a couple meta comments and then I have Denise and then I have Alain.

I think those are very good points, Cathy, and I think we should be very clear that what we're describing here is in no way a direct reflection on any proposed recommendations yet. And so one thing we could wind up doing is simply saying, "ICANN has a role doing these various things and this part's managed over there, this part is being addressed by a team over here, this part was totally something we looked at deeply, and so on and so forth," and I think to Emily's point about a holistic approach, there is – and I think James and Denise mentioned this, too – there is, for example, people that are trying to figure out who is the global root authority for allocation hierarchies. It doesn't mean they get involved in delegating out IP addresses. It' doesn't mean they're even involved in the last decade in something, but it is a place where they can say, "Oh, well the IANA function is blah-blah-blah-blah." So I think this is just framing that there'll be a discussion topic. It doesn't in any way portend a recommendation. Is that a fair assessment?

CATHY HANDLEY: Yes.

ERIC OSTERWEIL: Okay. So now I've got Denise, Alain, and then Kaveh.

[KAVEH RANJBAR]: [Inaudible].

ERIC OSTERWEIL: Go ahead, Kaveh.

KAVEH RANJBAR: I disagree with that because this is just [in order to make] the discussion a meta discussion because [you say] we put it there and then we will discuss, so when we will finally discuss because this is happening like [inaudible] we [inaudible] discussing this kind of stuff so if we keep it there and the next round we will again have to discuss. So I think at some point we have to get [back] to be able to do the work.

ERIC OSTERWEIL: So if I can bump the queue real quick as sort of a point of order – what we're proposing to do here is in one instance there will be a sub-team that will take a set of these things – potentially including this one – and they'll sit down and they will discuss the issues – that sub-team. And that may be you on that sub-team. It' sounds like it likely will be, at which point someone will say, "I think we should give direction to the RPKI to discuss how the global IANA root is going to be blah-blah-blah," and someone can say, "No. We are not going to do that," and then it'll be off the table. But right now I don't think we're trying to discuss, "What would we want to do so-and-so." I don't think only because of time because if we could do this all in line right now, we would.

KAVEH RANJBAR: I understand, but then that [puts] this whole what you're doing right now into question because, "Okay. Give this to sub-teams and let them

discuss if they want to keep them or throw them away." So what's the benefit of what we are doing right now?

ERIC OSTERWEIL: We've already eliminated a number from the homework from last night [inaudible] the next step is we'll coalesce them. Is that okay? This is just taxonomy.

I totally lost track of the queue now. I think Karen jumped in first and then I think the three of you did something in some order so [inaudible] fight for who goes first.

KAREN MULBERRY: There was a comment in the observer's room and I just wanted to let you know that Nick Shorey stated in the relationship between parties on this – so I've added it to the Review Team chat so you have a record of it.

UNIDENTIFIED FEMALE: I'm sorry I didn't understand that.

KAREN MULBERRY: It was a comment that was stated in the observer's room. There was relationship between parties on this, and I think it was back to the earlier discussion that you had on identifiers.

ERIC OSTERWEIL: Okay. Thank you. I'm not sure who had their card up first so Alain, why don't you go because –

ALAIN PATRICK: Just to echo what Eric said and maybe Kaveh and Cathy to ask them to just accept here that what we are putting in there is ICANN has a role in the coordination of the unique identifier including the numbers. So while we get there… and when we get there we will discuss the scope and if there is something, yes. If there is nothing, we don't. As Eric said. But we have to have this [on the list].

ERIC OSTERWEIL: Okay, thanks. Emily?

EMILY TAYLOR: My comment is, I don't want to repeat comments made by Eric and others. I agree with him. There's quite clearly because every time we discuss anything to do with IP addresses or ccTLDs it's going to raise sensitivities and concerns and anxiety amongst our colleagues who work in that space and are worried about ICANN's role encroaching into territory that it shouldn't.

Can we just take that as read at the moment that that is – I can see that Kaveh is already saying no and shaking his head. In the interest of moving forward, if we knew each other better and trusted each other more we would understand that when we come to making recommendations things that people who are working in that space are never going to agree to over their own dead body are not going to make

it into our final report, but I completely I must say quite strongly I totally disagree with the premise that if we allow us to even utter the word "IP address" we are somehow including the entire world of all of the world's problems including child exploitation, global hunger, warfare, whatever – it's obviously nonsense. ICANN has in its mission statement responsibility for unique identifiers. We would be failing in our duty if we don't at least say, "You know what? As well as the DNS, unique identifiers include IP addresses. It also includes ccTLDs within the DNS and ICANN has a kind of different role and a limited responsibility." That's all anyone's talking about at this stage. It's to include it in there that that doesn't mean that we go into the back of beyond, we try to by stealth extend ICANN's role into something it shouldn't be.

You guys are never going to allow that. So can we just take this as read and trust each other a little bit more for the minute to go through a table of things?

ERIC OSTERWEIL: Okay. Thanks, Emily. I have Denise and then James and I have Kaveh.

DENISE MICHEL: So again, with the caveat that's already in the table – ICANN's role in IP addresses and acknowledging that that's a very limited role, acknowledging that ultimately the team may not even get into any issues under this category, would you be… I think it needs to stay in, I think. And I'm open to any additional qualifiers that you think may be warranted.

ERIC OSTERWEIL: Thanks, Denise. James and then Kaveh, unless James wants to [inaudible]. Okay.

KAVEH RANJBAR: So Emily, with all due respect that's a wrong assessment because I'm representing ICANN Board here and also in my day job I really do not do anything with IP addresses. My job is very different and, to be honest, I don't care about politics of addresses. That's not why I'm very much jumpy about this [one and] a few others. The main reason is – and again, I'm repeating – I'm the ICANN Board delegate so I'm representing Board and I'm synchronizing with them. The main reason is to basically have an effective review with proper scoping where at the end we are happy with what we've done and effective for the organization. Not only IP addresses but some other issues [items] which we will get to including universal acceptance and things like that. I think when ICANN is not doing any action today about those stuff, that shouldn't be part of the review because we are an auditing team auditing security and stability of ICANN, and what you are doing. There is a lot of discussions and there are a lot of grounds to be covered, but I think we should focus it if we want to be effective on something we can manage. We are a team of 16 with limited time.

ERIC OSTERWEIL: Thanks, Kaveh. So James, then Alain, then I jumped in.

JAMES GANNON: Actually I was going to say exactly what Kaveh said so basically plus one.

ALAIN PATRICK: A little bit [inaudible] discussions but because Kaveh raised something about representing the Board, etc. I wanted to ask so did you get any feedback from the Board from the document we submitted to the Board? The Term of Reference we submitted to the Board?

KAVEH RANJBAR: Thanks for asking that question because I have to admit this is the first one with the under new Bylaws. This is the first of this type of review. So within the Board we also had some work to do so we actually did organize ourselves recently so how to do the communication properly and how to send stuff there and get stuff back. And so now we have that within the Board. We have the processes for that and the document is received by the Board. We are looking into that and I guess within a week or two we will be able to give you some responses. I cannot commit to any timeline but I can tell you now we have proper structure and we are reviewing the document properly within the Board. I have all the tools right now today to be two way communicating channels between the Board and this team.

ERIC OSTERWEIL: Okay. Thank you, Alain, for bringing that up. Thank you, Kaveh, for answering that. I was [inaudible] so I'm just going to [inaudible] then James is next.

I feel like we're having a lot of discussion about one micro issue early on but it's very important because we're also plumbing out our process hopefully the later disagreements are more focused on blood-letting and stuff like that.

I don't want to adjudicate this completely right now, but I do want to point out that Kaveh made one comment that I think might actually be a point of disconnect between a number of us. There's things that ICANN does and there are effects from things that ICANN does that are ICANN's responsibility because they've done something and it has an effect elsewhere and this will come up, I am certain, when we get to universal acceptance. You mentioned that just briefly. So in this case, ICANN does not dole out IP addresses to new companies because that's why we've got RIRs. That doesn't mean that ICANN hasn't done something that's affected the ecosystem of RIRs. And so that would be where we would be talking about things and it might even simply we say, "It hasn't done anything lately. Here's where all the documentation for the policies that govern each of the RIRs is." That could be it and that'll happen when we get to actually the review items here. Right now we're just trying to decide how we get to them and certainly if anyone proposes a recommendation that runs afoul of anyone's sensibilities, before it gets out of this team it's going to be heavily beaten upon.

So to Emily's point, there'll be plenty of opportunities for somebody with loose lips to be sunk on their ship before this team puts its name on the line. So I think there's plenty more rounds to go is all I'm saying. So no matter what happens here I wouldn't hopefully be worried that, "Oh, my gosh. Something slipped in under the covers and now the die is

cast." We're not casting any dies here today as far as I can tell. That's my two cents.

James.

JAMES GANNON: Thanks. Actually going back to Karen's comment on Nick from the observer room, I was a bit confused so I went and actually checked on it again. Nick was also making the point that IETF especially [inaudible] and [inaudible] and everything else could fit in under this as well, so just to make a note of that somewhere that again, it's another piece of the coordination different bodies [inaudible].

ERIC OSTERWEIL: That is a very good point, especially [use] TLDs and drafting IETF.

Okay, cool. So bringing this back – there is a bullet up there. It is likely not worded perfectly, maybe not even well based on our conversation, so we ought to put it into some shape where we either decide to yank it out completely or it's palatable enough as a work item starting point.

Cathy?

CATHY HANDLEY: Thank you. At the top of this flow chart it says "Mapping Bylaw Association and Additional Notes." What if under the "Additional Notes" section there was a note that said something about, "Will continue to flesh out or identify exact role of ICANN"?

ERIC OSTERWEIL: Yeah, definitely. Absolutely.

CATHY HANDLEY: Thanks.

ERIC OSTERWEIL: Thank you.

Okay. I think that was very useful. I want to do a clock check. We're coming up on the lunch hour and we've made massive progress almost getting through the first – it's actually the first one we talked about. It's actually #1 properly. But like I said, I think we're plumbing the process and I think this is all good.

James, go ahead.

Okay, next bullet which I can't see – "Associated network infrastructure components – routers, switches, address management systems, and Regional Internet Registries."

James, get in front of this one please.

JAMES GANNON: Remove it please. It has nothing to do with ICANN, in my opinion.

ERIC OSTERWEIL: Does anybody feel like they want to keep this one in? There's a proposal to yank it altogether.

UNIDENTIFIED FEMALE: [Inaudible] associated networks.

ERIC OSTERWEIL: Associated networks.

DENISE MICHEL: I think it's important to keep in mind that I think this was dropped in because it was part of the Identifier System Attack Mitigation paper, and it was dropped in just as a flag. Is this something that we need to look at or do we need to… so don't assume that I think everything that's in this table and on this list is something that someone is insisting that we address but rather having some of the things on here are on here to say, "Hey, is this something we need to look at or should we just delete it?"

ERIC OSTERWEIL: And just to sort of clarify that even further – Denise, thanks. That was very helpful – I think in addition the lack of mentioning something here doesn't mean it can't come up and be addressed and be worked into something as people start working on things. So it's like, "Oh, no. I didn't say associated routers," and later on it turns out that was important for some reason, it'll get pulled in. So this is really just high level framing. So there's proposal to yank it.

Cathy, sorry. Your card's up.

CATHY HANDLEY: Thank you. I don't understand it. I guess it's the RIR piece. I don't understand and if somebody could explain it to me –

ERIC OSTERWEIL: I think we're going to yank it. We'd like to take that bullet out back behind the shed.

Okay, next one – "Protocol parameters and the implementation of the associated protocols that [where to go] that make use of those parameters." I'm going to channel James and say kill it and okay, do I hear it seconded? Seconded by Cathy. Okay. Last bullet is terminated with extreme prejudice.

UNIDENTIFIED FEMALE: Hang on a second.

ERIC OSTERWEIL: Okay. We actually could take a lunch break.

I think we're really in good momentum here and I don't think that means that we can't take a lunch break, but could I propose that we take an abbreviated lunch break and then come back and hit it hard? What do people feel like? We can come back… So it's a 20-minute lunch break. Okay so quarter til.

[EMILY TAYLOR]:   [Inaudible].

ERIC OSTERWEIL: Yes.

[EMILY TAYLOR]:   [Inaudible].

ERIC OSTERWEIL: Okay.

JAMES GANNON: If I can make a suggestion. I feel that this work is much more important than outreach and stuff that we can do on a call whereas this is something that we need people face-to-face for. Not to say that the outreach piece isn't important but that is something we can easily do on a call.

UNIDENTIFIED FEMALE: Yes.

[STEVE CONTE]:   [Inaudible] can you just summarize for the room what the three [inaudible].

ERIC OSTERWEIL: Sorry, there was an off-mic conversation about… We're feeling like we're going to renegotiate the schedule because the work that we're doing now seems like it's much more a better use of our face-to-face time than things like the outreach which we can likely do over a call, etc. So we're going to have a lunch break that's going to go until 12:45/quarter to one, and then we're going to come back in here. Of course, people can bring lunch with you if you're still eating, but we're going to get back to it at that point and in the meantime the Chairs are going to go and reconsider the schedule for the rest of the day.

Thanks everyone. Quarter til.

[BREAK]

ERIC OSTERWEIL: We are 20 minutes past our 20-minute deadline so I doubled your lunch inadvertently. Thank you, or you're welcome.

Going back to our tasking and the Chairs all got together during lunch and we talked about things, and so what we're hoping to have by the end of the day is a clear path forward. We came up with a couple different, "Maybe we'll get here. Maybe we'll get there," and rather than give you guys all the strawmen that we came up with I think we'll just try and hit them. But we'll have a wrap-up at the end of the day wherever we do get to, and our expectation is we'll very clearly outline what our next steps are and where we expect to get.

Pretty quickly after we get done with this exercise, whenever we get done with it, we'll start talking about our overall timeframe, our overall delivery schedule, our overall work plan, etc.

Before I jump in, does anyone have any comments, questions, or any clarifications, or agenda bashing – although the agenda is pretty straightforward at this point?

Seeing no signs of comments I'm going to move forward.

The next "needs clarification" item I see is #11 so I'm going to jump right into that, and you guys know the drill.

"Domain name abuse mitigation." This said "needs clarification." Domain name abuse mitigation sounds very, very, broad to me. I am interested in sub-aspects of that. I could probably take a whack at redefining that if nobody else has anything to say before me. Since I'm chairing I'm happy to defer.

Denise?

DENISE MICHEL: I'm happy to give more clarification or connections to our Terms of Reference, our remit, the Bylaws. There's a number of intersection points in ICANN both operational and policy areas in SSR, staff responsibilities here. Again, this was [letting] more of a placeholder, more details are needed, perhaps we could note in the far column that more detail and fleshing out of ICANN's specific role in domain abuse mitigation is needed here.

ERIC OSTERWEIL: Yeah, and what our objective in reviewing it is. Is it the status? Is it to measure something? Domain name abuse covers a lot of ground and there are places where it actually applies to things that ICANN does but also what are we going to do with it? So I think what we need to do is we need to say, we're interested in domain name abuse obviously as it relates to ICANN's role, but in what regard? Why are we interested? Because we want to make it better? Because we want to say is the job good enough or propose ways to measure it? Etc.

Karen?

KAREN MULBERRY: I'd also wanted to let you know, too, that ICANN is conducting a DNS Abuse Study related to the CCT work but they've got a second part of that study that's going to be produced mid-June-ish kind of, and that might be of value for the Review Team to take a look at it. I know we had a real brief presentation from the folks that were conducting the study in Copenhagen so if you go down that path and you're interested in having more along those lines we can arrange to have the people who have developed the study and the results when it's done present to the Review Team.

ERIC OSTERWEIL: Go ahead, James.

JAMES GANNON: Thanks. [So if I] make a suggestion because I think this has been a recurring topic and I know I'm on one side [inaudible] others on other sides and can we have like a call dedicated to fleshing this out and what the goals are because I think we've got over the point of agreeing it has to be within ICANN's mission and role and remit, etc. I'm still confused as to what our outcome for it is and I think you put it very well there. Can we have some point to discuss with regard to DNS abuse what people want us as the SSR Review Team to do? Because I'm concerned about us getting consumers of information and making policy oriented decisions, operational stuff, and how ICANN treats its obligations I'm good with, but setting the direction and strategy for how ICANN does that is very different and I'm worried that if we don't have that clarifying exercise we're opening ourselves up to long, unended conversations about absolutely everything.

ERIC OSTERWEIL: James, I think that's a good point but I think what I propose we look at this item for – and maybe this is a good sort of if people like this we can apply this going forward in general is – domain name abuse is something that's topical and like Karen said, there's people doing studies on it so our objective with identifying it could be as simple as, "How does domain name abuse as quantified by other people's work or state of the art affect SSR for ICANN?" In other words, for example, you get a bad reputation for some aspects of the namespace maybe or whatever. We don't have to quantify it. We can just simply call it out – This is how it affects SSR. So it becomes an item for us and maybe it's a real slam dunk but that's just a proposal.

Next I have Steve.

STEVE CONTE: Just in line with what James was saying and also Eric, what you said, but maybe take a look at it from the Review Team's perspective of whether or not the actions that ICANN and not just the OCTO SSR team because the report that Karen brought up I think is outside of OCTO's team, looking at the appropriateness of what actions are being done within ICANN Org and community but maybe also look at a gap analysis. Maybe there's something that ICANN Org community should be doing that isn't touched on yet. So maybe there's room for that.

ERIC OSTERWEIL: Yeah. I think that's a really good clarification, Steve. We shouldn't necessarily assume we're going to have to be looking for a gap but if we find a gap or maybe we're in the right place to see a gap, we should be able to call it out. So I totally agree.

Next I have Cathy.

CATHY HANDLEY: Thank you, Eric. I just want to clarify – I think you said what my question was going to be. My question was going to be, can abuse take place that doesn't affect security, stability, and such, and yes, it can. And so your change is to narrow that down to not abuse but abuse this way with the security and stability. Thanks.

ERIC OSTERWEIL: Yeah.

Okay, Denise.

DENISE MICHEL: ICANN's specific role – so if the SSR1 specifically directs ICANN to take some action relating to abuse and compliance, we've got the registrar and registry very specific contractual obligations relating to abuse. We've got the OCTO and SSR staff activities relating to activities that are connected to domain name abuse and also metrics and measurements and tracking. And there's additional activities that relate specifically to ICANN's role. And from that, there are specific connections into security and stability. So just briefly, that's why I see it as an important part of our list.

Who knows ultimately what, if any, recommendations [it] may carry in this area but just to give you more information on ICANN's specific role.

ERIC OSTERWEIL: James?

JAMES GANNON: Thanks. Can I just make a suggestion that we go with if can we agree on Eric's language on it?

ERIC OSTERWEIL: I think generally it was domain name abuse mitigation as it affects SSR issues under as it affects SSR issues and that we always have the [inaudible] –

UNIDENTIFIED FEMALE: [Inaudible].

ERIC OSTERWEIL: Okay. Cool. Thank you everyone.

Next one is DDoS. I know people are dying to kick off so whoever wants to go.

James?

JAMES GANNON: Two things here that I think almost need to be split out – there is DDoS that affects L-Root specifically. That is something that is definitely within ICANN's mission. So is ICANN doing what it needs to do to mitigate potential DDoS threats, etc.? So that's one piece. And then there is the piece that I don't think we should go too deep into which is, does ICANN have a role in working out something to do with combatting the greater root server infrastructure pieces and where that fits in. That's a much more grey area for me.

If we're talking about DDoS as it affects L-Root, yes. Anything else I'd be much greyer on.

ERIC OSTERWEIL: Okay. Denise and then Emily.

DENISE MICHEL: I'd certainly agree about L-Root. I think it's premature to take everything else off the table. We heard at the DNS symposium and also from the OCTO SSR staff – and perhaps Steve can elaborate on this – the collaboration and facilitation role and information roles that ICANN OCTO SSR staff occasionally plays on this. There is also a connection in some DDoS attacks to contractual obligations for registries and registrars.

I think it's premature to take that off the table completely. I'm happy to elaborate on framing this perhaps a little more carefully.

ERIC OSTERWEIL: Okay. Thanks, Denise. I had Steve then Emily then Alain, and then Cathy.

STEVE CONTE: So plus 256 to James there to elaborate a little bit – not just L-Root but any other critical services that ICANN operates to include RPA zones that they also do. And I just want to reflect what John Crane spoke about yesterday about the things that we can touch and have direct impact on, the things that we as ICANN Org or community or whatever, the things we can influence, and then there's the things that we have no control over.

I think DDoS is the iceberg that falls into the we have no control over, but there are certainly some things that we have influence on and can

touch directly and that gets closer and closer to the items that ICANN or ICANN through PTI or whatever runs directly and manages directly [is] those resources.

ERIC OSTERWEIL: Thanks, Steve.

Emily, I think you were next.

EMILY TAYLOR: Just very briefly, I like James's categorization and actually we're directed to look at things that ICANN's directly and indirectly involved in and I think, as Steve says, there's obviously far less that ICANN can do about DDoS at large but indirectly through action, through outreach, and so on, there may be a role. And so perhaps the knowledge of how much ICANN can control the outcome should direct us into how much resources in terms of our time we put into those things, but I think it would be an omission to leave it out completely.

ERIC OSTERWEIL: Okay. Thanks, Emily.

I had Cathy and Zarko, and I think Alain, you dropped off.

CATHY HANDLEY: Thank you, Eric. I think to what James and Emily just said, I see there's typing that's gone on in the item but I think you need to split it out very specifically between the operational – one is DDoS as far as operational

issues and then DDoS as other. Because what you're going to do with operational issues is going to be hands-on, actual mitigation versus – that's pretty easy to do – but then put the other issues so there'd be two items under DDoS – one if it's operational, one if it's other.

ERIC OSTERWEIL: Okay. Makes sense.

Zarko?

ZARKO KECIC: I just wanted to clarify something because we have ICANN as operator, we have ICANN as policy maker, and we have ICANN as somebody who is giving recommendations. So when we are talking about DDoS we have a couple documents and one came out recently – how to mitigate DDoS generally.

Same thing with abuse – we are seeing that OCTO is putting a lot of effort in working on domain name abuse and they cannot do operationally much, but they can help community with recommendations and with fundings how to mitigate domain abuse.

So we have to agree are we going into that area where ICANN is working as somebody who is helping the community with recommendations and tools to fight abuse [that].

ERIC OSTERWEIL: Okay.

James, is your tag up from before? Okay, go ahead.

JAMES GANNON: I'm getting quite concerned now. So ICANN has no role in training anyone in how to prevent DDoS attacks. Can we just agree on that?

DENISE MICHEL: Can I pose a question to your statement? Some of the security training that they support wouldn't you say provides a foundation that helps in a broadly preventative manner potentially?

STEVE CONTE: Can I speak a little bit to that, Denise?

DENISE MICHEL: Yes.

STEVE CONTE: James, I agree with the way you said it, specifically is an absolute true statement. However, in the training that Denise brings up, especially when we're looking at registry training for ccTLDs and other organizations, we do talk and discuss about having tools in place to mitigate such attacks including discussing over provisioning and stuff like that. [Even though the] the landscape's changed we don't talk about how to fight DDoS specifically but we talk about business continuity both from procedural and process perspective but also from network and infrastructure perspectives.

EN

ERIC OSTERWEIL: Thanks, Steve.

I think what everyone is saying, despite the fact that it sounds like there's some conflict, is actually harmonious. So what I hear as far as the training goes is yes, people need to be trained for DDoS. Is it ICANN's role?

In the perspective that Steve talked about in trying to help people in the ICANN community that, for example, receive delegations from the root [and can] run their own TLDs, etc. telling them how not to expose themselves unnecessarily to DDoS – could that be, basically what I'm saying is if we see something here that needs to be framed as, "Why is SSRT looking at it?" And so if there's an SSR aspect of ICANN is helping people practice good hygiene that it delegates to, for example, what about that? Does that fit better or is that still you think too far afield?

I agree. DDoS is a big problem. It's not ICANN's problem. It's way bigger than just ICANN's problem. And even if it is ICANN's problem, it may not be the SSR Review Team's issue to address it unless we can show that some aspect of DDoS training or DDoS investigation or DDoS research is something that is best done from an SSR perspective by an organization like ICANN or PTI or something like that.

Go ahead, James.

JAMES GANNON: I think we need to make a very clear distinction between what ICANN does as a voluntary service and what ICANN is obligated to do, because

those are two very different things. OCTO SSR as part of their obligations may voluntarily also help some of the registries to make sure that they're doing things right, but that's not an obligation for them anywhere. And if we get into the grey area of where ICANN is doing some community service, if we want to call it that, and we start reviewing that, I'm not sure how we review that because we have nothing to review it against because it's not specifically part of the mandate.

ERIC OSTERWEIL: Okay. I get what you're saying and I'm happy to go with the group on this. I'm not hard and fast. But let me ask you this – if we looked at, for example in this case, DDoS as an influencer of the overall SSR of the Internet and then we trace back to there's an aspect of it that relates to things like the DNS root – like root servers or something like that – and clearly TLD registries are involved in DDoS as a reflector sometimes, or as targets, or whatever else, I'm not saying we should go way out of our way to include things that we don't have to so I would rather shed bags than add it. Is that something where it makes sense to put that in for an SSR perspective or do you think –

UNIDENTIFIED FEMALE: Alain's in the queue.

ERIC OSTERWEIL:　　　　　　Yeah, Alain's in the queue. Can we defer into Zarko because he has card [inaudible] because Alain is also raising to say something. So Alain, why don't you go and then James if you want to –

ALAIN PATRICK AINA:　　　　I think I agree with Eric. Definitely ICANN has a role dealing with DDoS. The point for us is narrow the scope, as we said, to operation to the root server system and also of our ICANN role in helping delegated a particular TLDs, etc. etc. So I think we also need to make sure that we narrow it down that it is clear enough for people to not misunderstand it.

ERIC OSTERWEIL:　　　　　　Thanks, Alain.

James?

JAMES GANNON:　　　　　　I have a constructive suggestion – can we definitively split this into two things? We have a mandate to review ICANN's operational response to DDoS on its root and its server systems. That is one thing we 100% have a mandate for. Then can we phrase the other side as a question for us to investigate – what is ICANN's role in combatting DDoS on the larger platform with regards to what should it do to be helping registries as – as a forward-looking statement rather than saying this is something we need to review their current implementation of? What should their role be in building a more resilient network of registries eventually?

ERIC OSTERWEIL: Yes. I think we can accommodate that, I think. And remember, this is a low-pass filter. We're going to be doing a lot of work on all these items down the road, including pitching them out later if we want to.

I had Cathy then I had Steve.

CATHY HANDLEY: Thank you. My question is more general when we start talking training and such, and I don't know exactly which one it is but there's an overarching responsibility that ICANN has. I think we've kind of agreed to get out and help do training and that kind of thing. And instead of getting into every single item we do and say "and training," maybe it would be better in the big overarching that we can put something in there that says they're responsible for a lot of different kinds of training so that people don't get confused and think we're going to train on DDoS and train on that.

ERIC OSTERWEIL: Okay. I think that's fair. It sort of falls in the same bucket we had before. We don't have to keep saying "with ICANN's purview," etc. and so forth.

Steve?

STEVE CONTE: Thanks. James, I'm comfortable with your statement except for the word combatting." I don't know if I want to use the word what ICANN

does to help other organizations combat ccTLD or combat DDoS so let's request a –

UNIDENTIFIED FEMALE: [Inaudible].

STEVE CONTE: Yes. Something like that – "help mediate" or "help mitigate" or something like that.

UNIDENTIFIED MALE: [Inaudible].

STEVE CONTE: Yeah. That's a very strong word and I want to make sure that we're very clear on what ICANN's role is on that. Thank you.

ERIC OSTERWEIL: Okay. I think that's all fine. So we'll plow forward. I want to make one comment and have it just sit and have people think about it and discuss it as needed, but one perspective of what the Review Team is doing is, while recommendations need to be put into actionable forms for ICANN and under ICANN's purview, it isn't necessarily the case that SSR considerations start with ICANN. We said that early on. We said we might be looking at thing that happen on web pages but not then recommending anything about web page serving. So SSR is a big issue

for the whole Internet and there's SSR issues way outside of ICANN's role and we obviously won't make recommendations on those.

Let's just be cognizant of that. I think that doesn't run afoul of anything we just clarified in the discussion. It was a really good discussion. But just keep in mind while ultimately we dovetail down into things that are within ICANN's purview we may start off elsewhere.

I'm scrolling…

UNIDENTIFIED FEMALE: Universal Acceptance?

ERIC OSTERWEIL: We had a "yes" by that, though. So can I skip it?

UNIDENTIFIED FEMALE: [Inaudible].

ERIC OSTERWEIL: Okay. Sorry.

The next one I have as a "clarify" is "measures and metrics – incorporate in all topics and sub-teams" – is #14 – "How can the community measure the status of SS&R." No. We booted that one. "Evidence based – what are and how can the community measure the relevant abuses for ICANN identifiers?" That one has a "clarify."

"What are and how can the community measure the relevant abuses for ICANN identifiers?" That one is a "clarify."

Does anybody want to lead that? I'll default to me if nobody wants to jump on it.

EMILY TAYLOR: I think I might have written that.

UNIDENTIFIED FEMALE: It says you.

EMILY TAYLOR: It does say me, but a lot of things say "me" that were other people, too. I think we were a bit like Cathy said about training, I think that measurement and metrics are an overarching piece and so we may not need this as a stand-alone item. However, we've been looking at a lot of metrics and measurements, and what I was trying to do was to capture that sort of, are we measuring the right things? Is this stuff available? Is it going to be useful? Is it going to actually help achieve the security objectives and improvements that one, I think, or everyone, would hope for?

Those were the thoughts I was trying to capture. I hope that helps clarify.

ERIC OSTERWEIL: That does. I threw myself in the queue and then I have Denise after me.

I think this one actually is really important so I think we should clarify it because we had, for example, a briefing on abuse yesterday and so I think abuse issues are really relevant because then people start talking about fragmentation of the namespace and wholesale blocking of components of the namespace and stuff. Clearly abuse has some role here. I think the clarification is we should just try and make some scoping statement before we break this into a work item that says, "What kind of abuse are we talking about as regards to the SSR issues that we're supposed to be talking about?"

Denise, do you want to go?

DENISE MICHEL: You've said pretty much everything I was going to say. I'm happy to continue talking about this if people still have questions but –

ERIC OSTERWEIL: James, go ahead.

JAMES GANNON: Okay. So was the intent [of this] DNS abuse? Because there are other types of abuses within the ICANN identifiers.

ERIC OSTERWEIL: I think we need to be very specific about what we're talking about. So first of all, the first bullet is a "no" so we'll yank that one out, but this one is, "What and how measures relevant abuses?" This one is basically

saying [if] one of the work items is to go find what the abuses are that we care about and talk about them. So we talked about a couple of abuses yesterday. This is essentially just saying there's an active component, it's called abuse, it happens in some way, shape, or form, for SSR, one of the items we have to do is line that out. I don't think we want to do it right now. We can't frontload all the work in this one meeting because we won't terminate, but we do want to be sure that we don't put gobbledygook in these bullets and then not be able to digest them later.

James, do you see anything in there that would help clarify for when we pick this back up in a sub-team or wherever else how to run with it?

JAMES GANNON: Again, it comes back to the question – are we really going to start trying to measure IP and protocol abuse? So can we put DNS specifically into this if that is the intent, because ICANN's identifiers is all three? We have to remember that.

ERIC OSTERWEIL: One of the things that came up was spamming, phishing, those sorts of things that are associated with a domain name, so the abuse is not domain name but we may be pivoting off of a domain name and so whatever and so it's like I'm not sure how we phrase that but we need to phrase it and sort of roll past this. I sense that we are all actually in agreement and I think we need to get the semantics right, but let's get them as right as we can get with a light touch and move.

You want to call it DNS – would "DNS abuse" work?

[JAMES GANNON]: [Relevant].

ERIC OSTERWEIL: Sure. Okay. "DNS relevant abuses and identifiers" and then we'll move it to a "yes."

EMILY TAYLOR: I think there's also a bit of garble at the end for "ICANN identifiers." I think that might confuse people. I think that we could just say, "Measure relevant DNS abuses," and then stop.

ERIC OSTERWEIL: Yeah. Agreed. Actually I don't think your mic was on. Emily pointed out that there's a tailing a bit of text that says, "ICANN identifiers" that's a little confusing so why don't we just yank that off and just call it, "DNS abuse."

The next one right below it is – and it's a yes/no – the next sub-bullet under it is, "Evidence-based DNS health index and abuse data – what evidence tells us access to information, etc." I think we've also said in line, isn't this just the ITHI stuff? So I propose we just call that bullet "ITHI."

James, go ahead.

JAMES GANNON: The way that this is phrased – specifically the line, "What the evidence tells us," that's not our remit, I don't believe. We're not there to interpret the data there. We're not making a qualitative call on the level of DNS abuse within the industry or anything like that. I don't see that as our role. If anybody disagrees with me, we should have a conversation about that.

Sorry – Denise is asking what do I mean by qualitative – I don't believe that we're there, that our role is to sit here and take in the data on the current level of abuse within the DNS marketplace and make a ruling or a calling on what that tells us. We're here to say whether ICANN is dealing with the level of abuse in an appropriate manner, but we're not here to state that it is a low/high/medium, that it is too much, that it is too little. I don't see that as our role at all.

ERIC OSTERWEIL: Go ahead, Emily.

EMILY TAYLOR: Again, I think I'm the author of that bullet, so I was just trying to convey what was in my mind when I wrote it, which is I think I'm a bit less directive and directed in the phrasing than perhaps is coming across. I'm actually saying let's look at the evidence. Evidence usually tells you something. Obviously we're not going to be commenting or expending energy on things that are outside our role or remit. So you can look at evidence [bases] in two ways. You can say, "I have a theory and then I

will look to the evidence to prove or disprove it." You can also say, "What's the evidence telling me?" Because normally the evidence is telling you things you didn't think of in advance.

So I'm suggesting a first pass of the evidence with an inquiring mind bearing in mind the limits of all of the stuff. Can we just have a great big bubble at the head of, "Within ICANN's remit, within our terms of reference, within what is possible on the planet?" Let's look at the data.

If this is telling us something that will have an impact on our terms of reference we should not ignore it or close off that line of inquiry in advance.

ERIC OSTERWEIL: Okay. Thanks, Emily.

I have Denise.

DENISE MICHEL: Are you comfortable with that, James? Yeah. Again, I think this is early days and we don't want to close off where we might go with it, right?

JAMES GANNON: I like Emily's phrasing. Maybe after, we can tweak it a little bit to fit that phrasing because that made sense to me. Just the way it's phrased at the moment just strikes me a slightly different way.

ERIC OSTERWEIL: Okay. Great. So whoever the staff person is helping out with the item, just do what you can and it sounds like we'll circle back and polish whatever needs polishing but we're accepting that one and moving on.

The next one I have that is a "clarify" is #16, I think, unless someone saw something at #15. I didn't see anything there.

"White Hat Operations" – and then below it I guess is part of that one – "What are the White Hat operations that are taken in ICANN's space that may need exception handling gratis for registering sink holes, etc.? Can this be included in improving security in unique identifiers' threat mitigation?" There's a little bit of a discussion there.

James, go ahead.

JAMES GANNON: Thanks. I will take the banner of this one. I think this is an excellent topic. I think it's particularly relevant. I think it's contemporaneous. I think it's really important. And I really think that, even as it's written now, I think it's a good topic to take forward.

ERIC OSTERWEIL: Denise?

DENISE MICHEL: I'm just not really clear what's encapsulated in #16.

ERIC OSTERWEIL: I think #16 is saying basically should there be special considerations or accommodations for things that are happening that may not be – and I think this is topical from yesterday. I think it specifically came up – whereby somebody is taking sort of a White Hat, proactive, action inside of ICANN's space to protect the SSR issues and normally that person would get zapped because they've done something wrong but do they deserve special accommodations, for example – registering a sink hole domain improperly but it's a sink hole domain that's very critical to a clear and present threat.

Whether that's in or out of scope I'm not sure, but I think that's the general idea. I'm the author of it but I don't really care. Whatever we decide is fine with me. Is it too specific? Are you okay with it?

DENISE MICHEL: Yeah. Now that I understand what you're referring to I think it's fine and would roll up into another category.

ERIC OSTERWEIL: Okay. Cool. Great. Thank you very much. So that one's now a "yes." And all these things are going to get passed over and reworded at some level at some point, so we'll definitely make sure that this is a low pass filter.

The next "clarify" I have is I think #19 – "Proactive measures – advisories, technical alerts."

UNIDENTIFIED MALE: [Inaudible].

ERIC OSTERWEIL: Are those part of the "clarify," too? Because I'm just having a formatting… Okay so I'll just read the whole thing.

"Secure coding practices, patch management, security awareness, etc. for addressing service side exploits and client side exploits possibly of a vulnerability database specifically addressing DNS issues proactive measures, advisors, technical alerts."

This is a "clarify" so people had different opinions. I'll try and lead us through deciding on this one.

I see this one as basically outlining that there are a number of problems that come from things that stem from things like secure coding practices, and clearly there are a lot of utilities in the community like vulnerability databases and then yes part of are those actually are very specific to DNS issues. There's the service side and client side exploits, so how will we describe this in terms of SSR?

James, go ahead.

JAMES GANNON: I'm just going to challenge these one at a time. My concern with what has been listed as #17 is client side exploits. ICANN does not develop client side stuff, so I would see that as out of scope. We're not going to be making recommendations on DNS clients or even most DNS servers.

And I would really need to understand #18 better. Are we posing that ICANN creates its own database? If that is something, then I would have

serious issues with that. And "Proactive measures," yeah, that is something I would like to keep for #19.

ERIC OSTERWEIL: Okay. So the secure coding practices – client and server side sound like they're active development perspectives of security and James, it sounds like your perspective is that may not be under the umbrella of SSR stuff, especially as viewed from ICANN's perspective. A vulnerability database reminds me a lot of John Crane yesterday talking about when they tried to do a [cert] – I think it was John who was talking about that – and the difficulty there. So I think that's probably part and parcel.

And then advisories and technical alerts – interesting. James, it sounds like your personal perspective would be to nix #17 and #18, and #19 you might be on board with. How does anybody else feel about any of that because [inaudible] feedback it's going to be that way?

UNIDENTIFIED FEMALE: Did you say keep #18 and #19?

ERIC OSTERWEIL: No. Keep #19, nix #17 and #18, is what I thought I got from James.

Steve, Cathy, and then Denise. Go Steve.

STEVE CONTE: I supported how you have clarified it, so I think those items you hit and how you hit them were exactly right and especially with the [cert] issue.

I think you would get nothing but heartache and pain as a Review Team if you tried to recommend that ICANN be a [cert]. However, that's not the time to have that conversation.

Proactive measures – I think that's absolutely fine and who's not to say that's already happening just in the trusted communities where we don't have visibility.

ERIC OSTERWEIL: Okay, thanks.

                         I think Cathy's next.

CATHY HANDLEY: Same thing

ERIC OSTERWEIL: Denise, you're [yanked].

[DENISE MICHEL]:   [Inaudible].

ERIC OSTERWEIL: #17 and #18 got nixed, and #19 now becomes a "yes."

                         Next one I see as a "clarify" is #22 – "Perform interviews and review descriptions and evidence of…" and then there's a whole bunch of Isms.

James, you're up.

JAMES GANNON: I would like to hear the concerns around not having this as a "yes." This is standard ISO 27001 management of security systems and management of IT [inaudible]. This is industry standard stuff.

EMILY TAYLOR: Sorry, I'm obviously not raising concerns that it shouldn't be in there. It's only a formatting thing in that it's possibly delving into a level of detail that's below the high level that we're currently at. I think it's sort of describing high detailed working methods, all of which are absolutely sensible and we should do. So it's just a question about whether it's taking us down into the next level. That was all but I'm really not going to die in a ditch about it. There's clear support around the table on that.

ERIC OSTERWEIL: Thanks, Emily.

Steve?

STEVE CONTE: I have no issues with the concept of talking to ICANN's IT Department to determine what level of certification they have. My question to the Review Team is, does the Review Team feel the way that it's worded now it almost sounds like a audit of ISO 27001 right now and does the Review Team have the skill set and wherewithal to do that audit itself?

ERIC OSTERWEIL: Okay. I've got Denise and then I've got James and I think [inaudible].

                         Denise put her card up first and then you guys can share the mic.

DENISE MICHEL: Compliance with appropriate international standards is one of the recommendations in SSR1. I think that obligates us to at least look at this area and how they implemented [that] recommendation. This may be a level of specificity that may or may not ultimately be appropriate or something this team chooses to do, but I have no problem with the general approach of reviewing common Best Practices and standards in the SSR area as they apply to ICANN operations.

ERIC OSTERWEIL: Okay. James, Boban? Either of you guys?

BOBAN KRSIC: Due to the fact that I'm an ISO 27001 lead auditor and we're a little bit of assistance, I think we have the experience here in the team to review [areas of] security management.

ERIC OSTERWEIL: Okay. It sounds like this one gets a "yes," and it sounds like this one got questioned because it just had a lot of specificity, and that's fine. Ultimately it might roll up into some broader category like [infosec] management stuff and blah-blah-blah. So we'll put it as a "yes." We'll

move on. All these things get reviewed multiple times before they get turned into any working item.

James?

JAMES GANNON: I just want to make a really quick comment. We're talking high level gap assessment, not audit.

STEVE CONTE: Okay. I'm not trying to block it all. For the record just to be clear I just wanted to make sure that this was worded in the right way and that we were understanding the same things as we move forward.

ERIC OSTERWEIL: Zarko?

ZARKO KECIC: Can I make clear that there will be only gap assessment, not certification?

ERIC OSTERWEIL: Okay. Yeah. Maybe put that in the additional notes. I think these things are all about to be transformed anyway, but yeah. Let's make sure that we catch everything that we need to.

Rolling on - #23 – "Various others from the Annex A like rules for acceptable use of assets, access control policy, operating procedures,

confidentiality, or non-disclosure agreements, secure system engineering principles, information [security policy for] supply relationships, etc."

ZARKO KECIC: [Inaudible].

ERIC OSTERWEIL: [Inaudible] same as the first? Okay. Cool.

EMILY TAYLOR: Very quick – let's not lose this because we'll come back to it [because] I think that's absolutely [inaudible].

ERIC OSTERWEIL: Okay. Great. Thank you.

Yes, Cathy?

CATHY HANDLEY: This is just administrative – can we make sure that #23 maybe is #22B or something like that so that because the way they're written they could read as two different things but they're all associated with the same [stuff] we need –

ERIC OSTERWEIL: We are definitely going to do a duplication pass so we will get [to that] –

CATHY HANDLEY: Just an administrative note – put them together so we don't lose what they are.

ERIC OSTERWEIL: Can you put that in the notes that this one is an awful lot like… Okay, awesome. Thank you very much. Thanks, Cathy.

Okay #24 – "Categorize and prioritize the outcome of the analysis."

UNIDENTIFIED FEMALE: [Inaudible].

ERIC OSTERWEIL: Okay, so that came from the one above. Okay. Alright. So #24 is a pinky toe. Okay. [Inaudible].

So I'll go to #24 – "Develop a short, medium, and long-term, schedule to implement different controls in accordance to their requirements."

DENISE MICHEL: I think [inaudible] clarification because I didn't understand exactly what that exactly meant.

ERIC OSTERWEIL: We're talking about controls so we're talking about compliance so we're talking about a lot of the auditing we were just talking about and we

just classified those as gap analyses, so I think basically it's just the same thing that the [other ones] –

[DENISE MICHEL]:   [Split out so] [inaudible].

[ZARKO KECIC]:   Put it together and [it's a gap analysis] –

ERIC OSTERWEIL: To be clear, yes. There's a good opportunity to say what I had imagined – and I want this to be what we all agree to so this is just my misunderstanding or if I didn't say it clearly or whatever – what I proposed going forward is that after we get through with this list and we have a bunch of "yeses" then we take them necessarily and we start de-duplicating them and putting them in buckets together. So the fact that this set all kind of run together and they may have been more [homogenistic] before, etc. is going to get worked out when we start putting them into gap analysis or [infosec] or internal security [acumen] or something like that. So this will, I think, all work itself out. So we should absolutely take notes of the things you all are saying but I wouldn't worry too much about whether there's redundancy yet. Is that fair?

[DENISE MICHEL]:   Yes.

ERIC OSTERWEIL: Okay. Cool.

Next one – "Define a set of metrics to measure the effectiveness of implementation." That's the same thing, I think.

So now we get a little bit of a run of "yeses" which is awesome down to #32 – "Transition to IANA functions operator plan."

Denise?

DENISE MICHEL: I think I may have asked for clarification there and I think we need to add "as it relates to the SSR remit." Because it's broader. You're talking about a broader topic, right?

JAMES GANNON: Yes. I do think we're in a moment going to have a bigger discussion about this where business continuity fits into SSR.

DENISE MICHEL: Yes.

JAMES GANNON: So in my mind business continuity isn't an SSR item and thus I see this as in scope, but if we need to have a discussion about where business continuity fits in within ICANN SSR then –

DENISE MICHEL: Yeah, this is [to these] yeah. And again, the point there was that business continuity is much broader than SSR but SSR is an important component of business continuity and we can just accept that clarification throughout, and I think we're good.

ERIC OSTERWEIL: Okay. I have Alain then I have Cathy.

                       Alain?

ALAIN PATRICK AINA: It's not quite clear for me transition to IANA function operator plan. So I see [not clear] for me.

ERIC OSTERWEIL: James, do you want to answer that? Cathy [put your card] can James jump on that real quick? He wants to respond.

                       James and then Cathy.

JAMES GANNON: This is just like a 30-second background. When NTIA was contracting with ICANN to be the IANA functions operator, one of the big clauses within the original contract was C7.3 which required ICANN to have a plan in place that allowed for a seamless and uninterrupted transition to a new IANA functions operator if such a transition needed to happen.

When we got hold of that plan, it was extremely sparse. It was not an operational plan. So this is transition of IP systems, key data exchanges, making sure that everything is seamless. It's essentially a mini business continuity plan.

So one of the recommendations that we had coming out of the whole Accountability and CWG work was that when PTI was formed and ICANN was working with PTI to set up its systems and plans and processes was that C7.3 which created that operational plan needed to be reflected in a new plan between ICANN PTI and a potential unknown future IANA functions operator, and that that plan will be reviewed by the community which will be [us].

ERIC OSTERWEIL: I'm sorry. Cathy was next in the queue.

Sorry, yeah. He was responding to you so sorry, Cathy. Alain wants to come back. Go ahead. Sorry, Alain.

ALAIN PATRICK AINA: In this case, I think the wording should be "transition of IANA function operator," not "transition to IANA function operator." So if I got you correctly it is the plan we have to transition to a new operators.

UNIDENTIFIED MALE: [Inaudible].

ALAIN PATRICK AINA: But transitional –

ERIC OSTERWEIL: Okay. Alright, Cathy.

CATHY HANDLEY: I would change it to put "business plan continuity regarding transition of IANA functions," because that C7 I know that very well because I put it into the contract so I know exactly what it is. And that's what we're looking at – not the overall transition plan to a new IANA functions operator. It's specifically the continuity plan in place now for… it's more like a business continuity plan for IANA functions. I can't read that, so…

JAMES GANNON: If we just put [it] in a note on the side [about] this is referring to the C7.3 replacement to give it context.

CATHY HANDLEY: But it's not transition plan to new IANA functions operator. It's a very specific business continuity plan and change that from "transition plan" to "business continuity plan under the new IANA functions" –

JAMES GANNON: You're the expert. Can you throw in some language to make it clear because I think we're both on the same page but we just want to get the right language so I'm happy for you to reword it?

CATHY HANDLEY:	I would just change "transition plan" to "business continuity plan."
[ALAIN PATRICK AINA]:	To that what we have in #31 or because #31 is –
CATHY HANDLY:	"Plan for new IANA functions operator" – something like that.

ERIC OSTERWEIL: Okay. Alright. Cool. Great. Thank you, everyone.

Next one I see is #36 – "Alternate root risk" is a "clarify." So I'm not sure what the concern about the alternate root as a work item is but I'll say that I think the potential for the DNS to be fractured by alternate roots whereby resolvability depends on which root somebody's going to where the namespaces are not managed by the same authority, therefore will innately diverge from each other is an SSR concern. But I'm happy to have conversation about that.

Kaveh?

KAVEH RANJBAR: This is just also curiosity, what ICANN in any form can do about this? It's a risk, okay. But what can we do? We really don't have any, any, power by any means.

ERIC OSTERWEIL: I don't see anything in there that's a recommendation. I do think that if there is sort of codified concern over an alternate root then when things are discussed that clearly portend an alternate root, there can be a normative reference for some people who are concerned about it but it doesn't necessarily have to be a recommendation, for example.

Bernie?

BERNARD TURCOTTE: Thank you. In line with Kaveh's thing, this one bugged me when I saw it. Does it really pass the initial [Sid] test within ICANN's limited mission? I could start an alternate root. What is it? First you would have to define it because I can start one on my computer right now and call it an alternate root. It's going to work. We could be chasing our tails on this one.

ERIC OSTERWEIL: Okay, James?

JAMES GANNON: So in my mind when I put this down I had a recommendation at the end in my head is that ICANN needs to go and do some risk analysis on what would the impact on the Internet be – which it coordinates and it is responsible for ensuring the stability and resiliency of – of a proliferation of alternate roots, for example? There is a piece of research there that ICANN needs to be empowered to do to analyze the impact on their root of a proliferation of alternate roots.

KAVEH RANJBAR: Again, it goes back to the same kind of argumentation that yes, I understand that. But if we follow that logic, there is so many issues that everything falls under that. Everything related to IT security – not even Internet – IT security can fall under this. I can't agree with that line of argumentation.

ERIC OSTERWEIL: So taking off all my hats, that you just described is why it's an SSR issue. It simply is because like you said, an alternate root fractures the namespace that pretty much everything needs in order to be on an Internet because there is nothing without a [inaudible].

KAVEH RANJBAR: With that argument I can also argue that power plants are very important because if you don't have power in some parts of Internet, Internet will go dark and [inaudible].

ERIC OSTERWEIL: [Inaudible] ICANN's role in power plant management [inaudible].

KAVEH RANJBAR: What is ICANN's role in alternate roots?

ERIC OSTERWEIL: Its role in the alternate roots is defined by its role in the root.

KAVEH RANJBAR: No.

ERIC OSTERWEIL: Because they're alternate to something which is the ICANN root.

KAVEH RANJBAR: No.

ERIC OSTERWEIL: I think that's true, otherwise there need be no alternate. [It'd] be part of the multi-root system. [It'd] be a multi-tree [inaudible].

KAVEH RANJBAR: I think we should take that offline because I have a lot of argumentation about that but again, [inaudible] based on [inaudible] argumentation of these type of issues that we are adding I don't think there is… If you take that kind of justification, many of these things will fall out because that justification which is just a blanket one that it impacts on something somehow – indirectly or directly it affects something that ICANN does – I can add so many other things to this list and I can argue much more stronger for those ones.

ERIC OSTERWEIL: So Kaveh, is it the concern that the presence of this item in this list is tantamount to ICANN being responsible to make sure there are never any alternate roots? Is that what you're worried about its implying?

KAVEH RANJBAR: No. I'm worried about consistency of SSR2 – this review – because if you start covering this stuff I'm telling you today give me half an hour, I will come up with a list of a hundred other things which if you go [inaudible] that I think you should cover those. Forget about if I argue for or against, I'm saying to have a consistent ground for selecting the items we want to work on. And we haven't found that. We just came up with a mind map so some stuff we people think are important. If we go out of the room, there are other people who would have many other things, and all of that will fit that logic.

ERIC OSTERWEIL: Okay.

KAVEH RANJBAR: So, the outcome of this team, anyone who looks at it and says, "Oh, but why did they look at this? Why didn't they look at that?" I think we need a consistent ground for selecting these items, and we don't have that. This is just what came to our minds and then we are [defending] all of them based on the general blanket argument.

ERIC OSTERWEIL: Sorry, I got distracted. I guess I don't understand why – I'm sorry, I'm doing a lot of talking so I'm also – sorry, I was about to say I was watching the queue and I wasn't. Sorry, go ahead, Emily.

EMILY TAYLOR: Kaveh, you are right to remind us that we need to be working on things that are within ICANN's remit, within ICANN's scope and that have a very strong security, stability, resiliency issue. ICANN does have [inaudible] mission is management of the root, right? Is that a contentious statement?

KAVEH RANJBAR: Management of root zone files, which is very different.

UNIDENTIFIED FEMALE: Coordination of the root zone.

EMILY TAYLOR: Sorry. I forgot. I have to choose every single word carefully. I've been – okay, what they said, blah, blah, blah, root. That's my [inaudible] So, ICANN has some role that I think we all understand – apart from me, obviously – to do with the root. Eric has made a point that part of what makes the Internet the Internet is a system of unique identifiers which are universally accessible and resolvable.

Alternative roots are with us. Obviously, Bernie could set up his root. I think he already did. But I think that there is a risk analysis piece in my

view. I think that this is well placed on the list by James to look at, well, what if an alternative naming system gains traction? What will the impact on the security, stability, resiliency of what ICANN [inaudible] within its purview? I think that that is well placed on the list in my view.

KAVEH RANJBAR: So, then may I suggest that we add DOI? Because that's an alternate naming system. Then we have to go to alternate numbering system as well, which in IoT [inaudible] are like 20 – no, seriously, because they are unique identifiers. So if we – that's my problem with this argumentation.

EMILY TAYLOR: I don't see any problem with it, Kaveh. I think that you're right at this part, there are a number of proposals. But there are also a number of ad hoc solutions that are out there that are outside a unique identifier remit. A lot of the IoT doesn't fit within the classic naming and numbering.

So, yes. It'll go nowhere. I can see that there's a lot of resistance because we can't immediately see a recommendation falling out of this. In my view though, we would be wrong to sort of – say, there's this phrase in English. Sorry about – English idiom which is, "Ships? I see no ships." This is Nelsonian blindness. This is happening. This has an impact on the security, stability and resiliency and the single Internet. One Internet.

I remember from someone's [strapline], do we just pretend we don't see it because it happens to make our role a bit easier? Or do we actually own up to the fact that it is out there? We might be powerless to prevent it happening, and that could be what we end up doing. But I think closing off the inquiry – we've had some versions of these conversations throughout our work. Do we close off the inquiry because we can't immediately find a solution? Or do we leave it on the table for now until we can really solidly find a way to get rid of it? So, I would just support the voices that say keep it on for now.

ERIC OSTERWEIL: Okay. James and then Bernie.

JAMES GANNON: In my mind, so we have a shall assess on future threats and challenges to the SSR of the DNS. So, the ICANN DNS. That's in the Bylaws. And to my mind, alternate roots, DOA, I'm not saying that this Review Team is going to sit down and work out these challenges and work out these challenges and work out ICANN's response to them, but we do in my mind have a role in instructing ICANN the organization to ensure that they have assessed the risk.

I'm not saying that's we go off and solve all of these problems. That's certainly not what I'm trying to do when I'm putting this in. But I'm saying that I feel that the ICANN organization needs to be empowered by the community – which is us – to do that risk management piece, to assess the future challenge and threat of DOA, of alternate numbering systems, whatever they may be. I'm not saying that we need to do it for

them. I'm saying that the community needs to empower ICANN to assess the threat to our Internet in the ICANN space within the role that we have, which we are told to shall assess those, ICANN's ability to respond to these things. And that's why I really want to put in something about this so that we can go and tell ICANN organization to do that risk management piece. Not to go off and become the defender of the one Internet or anything else, but to do the risk management, to be empowered, to go off and say the community has told us we need to work as what we need to do. Not to defend ourselves but to be prepared for the future of the Internet and how that is going to work in the future. And then that's my goal with it.

ERIC OSTERWEIL: Thanks. I've got Bernie, then I've got Kaveh, then I've got Alain. Bernie?

BERNARD TURCOTTE: No, because I have two comments for James. One is I think that will make us just another – my personal assessment – another one of those commentary groups which IETF has many of them. So, the people in IETF make standards, and there are many people around them – and one or two of them are ICANN constituencies – just make commentary about them. Nothing happens because the standard is there, people are using them. So, that's one part. But I think you're talking about a very important point, and I think that's something which is worth clearing up. We are on the ship and the ship is going in a straight direction.

And my understanding of the review is we actually have to look into the direct what's happening straight forward, so when you're navigating, if

there are any risks – going straight forward. There is another type of analysis, strategic risk analysis and all of that where it gives you a full map. "Oh, if you turn right or left, then you have this." And I fully agree that this kind of stuff should be there. But that's a [very different] type of review that's high level, strategic and normally doesn't come with recommendation, it's just understanding the risks. So, my personal view on SSR – and I'm going to clarify that at least from the Board side what they understand – but my personal understanding is we actually have to look at the risks forward. Obviously, if we see things on that path, if you see yourself, I think we should clarify. So, if we encounter something close by, we say, "Hey, keep an eye on that. Flag that." But that's all. We shouldn't go fish for them, because if we start going fish hem – and this is fishing for them. Going for DOA is fishing for them. But when you're doing a review and we see, "Oh, this is actually…" if you're looking at the root server accountable system for example and then we see, "Oh, this might be a possibility." Sure. Yes, I have no issue with flagging them, but that's all. Trying to [map landscape] that's impossible.

ERIC OSTERWEIL: Okay, Kaveh. I've got Alain, then I've got James, and then Bernie, I'm not sure. [inaudible] hanging in there. So...

UNIDENTIFIED MALE: What he said.

ERIC OSTERWEIL: Okay. Thanks. Jumped the queue [inaudible] so then I'm in after that. So, Alain, go ahead.

ALAIN PATRICK AINA: I agree with Kaveh, and I just want to tell James that when I hear you, then I wanted to play back what you said a few moments ago. We should focus what ICANN must do, what ICANN may or might do. It's the same thing [inaudible].

ERIC OSTERWEIL: James.

JAMES GANNON: Can I propose a compromise?

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: Sure.

JAMES GANNON: I think me and Kaveh are actually on the same path. I might not do it right now, but I want to empower the organization to – when we're going along that straight path and the radar sees on the path an iceberg, that the organization has the – not the permission but the empowerment from the community to do something about that with

regards to do we turn left, do we turn right or do we steam less but straight ahead?

So, if we reword, we don't call out a specific thing [but] that we want to assess ICANN's capability to respond to if something like that – I need to think of the word in my head, but that we assess the capability as it stands at the moment. I don't know what it is, and if we then after that assessment say, "Okay, yes, you guys have it in hand," or "No, you need more resources, more funding, more whatever," then that could be a recommendation at the end of the day. Does that play better into – because that's my goal at the end of the day anyway. I'm not so concerned with the specific technologies that we're going to look at. We all have our own personal opinions on that depending on where we're coming at it from. But it's that guidance piece that I would like to have [us in.]

KAVEH RANJBAR: It works for me. I have to check with the Board as well, but in general, I think this is –

ERIC OSTERWEIL: Okay, so I'm in, and then Steve and Kaveh are kind of both – I'm not sure. Okay, so Steve's [inaudible] that. So, the question of whether there's an iceberg dead along our path or askew to our path or far field from our path is a matter of opinion, and it's based on what different people see based on where they sit in their various walks in the community. So, the fact that you don't see one dead ahead doesn't preclude the fact that there is one maybe potentially straight ahead. So,

to use your own analogy, yes, if there is an iceberg ahead – and to James's point, if for some reason or another the organization is not empowered to look at that as a strategic risk that needs to be addressed, you risk losing the only collision-free namespace that exists in the Internet today. So, to me, whether you think it's likely or unlikely, it's fundamental. So there's that too. You can consider things that are likely to happen. You can also consider things that would be catastrophic if they did happen. Just another way to look at an SSR's [team]. Yes, a set of meteors striking every single root server on the planet – including where the HSM's at – would be really bad, and so we put that in a report, people might think that they should get like a bottle of wine and a pizza and watch it in a movie instead, right? I get that, but nevertheless, there are these sort of catastrophic events that people might worry about.

Alright, so I have the hat back on [inaudible]. Steve and then Bernie. I'm sorry. Cathy. I missed you. Sorry. Are you in now? Okay, Cathy's in now, because she's mad.

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: Okay.

CATHY HANLEY: This is neither side of the argument, but I think what we've kind of heard here, and it's kind of a joint project, risk management analysis on

emerging and alternative identifier systems, something along those lines, not – because even if it's an alternate root, you'd have an identifier system. And [inaudible] was DOA.

UNIDENTIFIED MALE: [inaudible]

ERIC OSTERWEIL: Yes, that sure opens it up a lot.

UNIDENTIFIED FEMALE: Okay.

ERIC OSTERWEIL: Maybe we'll circle back. Steve?

STEVE CONTE: Yes. I've been really afraid to put my card up on this. I think clearly, there's a lot of room for dialog here. There are a lot of interesting opinions, and I think that that's worth exploring. So, on that aspect, I say yes, let's keep it on there because as I think you guys mentioned multiple times, it doesn't guarantee that there's going to be a recommendation coming out of it. But I think the fact that we're exploring it at this level this early in the game means that there should be some exploration.

As far as naming – ironically speaking – as far as naming this item, evolutions in namespace, something like that just to – alternate root to me from a DNS guy has a very specific meaning to it, and that falls within the DNS. James clearly brought up some technologies that fall outside of the DNS that are still worth having conversations about. So, something that allows us to have those conversations in a more free space.

And then finally, last comment is that I would caution against your wording, James, about empowering ICANN to make decisions. And this is probably – I'm in the weeds on this one, but more of empowering them to have the ability to explore and ascertain what – is it an iceberg or is it just a bunch of foam? I don't know if the SSR Review Team is the right body to say, "You couldn't turn left or right." But the SSR team should be able to say, "You can turn on your radar and actually see if it is an iceberg or not."

ERIC OSTERWEIL: Thanks a lot. Bernie?

BERNARD TURCOTTE: Thank you. More along the lines where Cathy was going, I don't agree. I would flip it on its head a bit from where you were going. You're looking at alternative naming technologies, and almost what I hear is we're almost recommending that ICANN be aware of developing technologies which could impact the Internet supremacy – I'll use that word for lack of a better word – or displace it as the unique identifier system on the

ERIC OSTERWEIL: Go ahead, Cathy.

CATHY HANLEY: I inadvertently left off the part because it's in Emily's writing and I couldn't read it. And their impact on the Internet today. So, that would bring it back to exactly what you were talking about.

EMILY TAYLOR: Sorry. Just deciphering my – yes, I put the impact on and I couldn't work out what I meant, so I put in square brackets, "One Internet," because... You know.

ERIC OSTERWEIL: Alright. Kaveh and then James. Is your card back up? Okay. Kaveh and James.

KAVEH RANJBAR: So, I actually have a suggestion now thinking more after discussions. Because I would really support if SSR team looks into what the procedures ICANN organization might take to encounter these things. So in general, like how ICANN is going to deal not with a specific alternate root, but in general, like with competing namespace. So, if they have a process, do they have something to flag it, and then will

they go to [act] or will they do research, report back to the Board or to comment, whatever. So if they have a process for that or not, and then if that process is good enough or not. I would support SSR looking into those or recommending those. But looking into specific issues, well, I still have my main concerns.

ERIC OSTERWEIL: Okay. I've got James, then I've got… Okay. James, go, and then I'll figure out which of you went first.

JAMES GANNON: Thanks. So, I've just put some proposed text into the Google Doc. So, change it to "Assess ICANN's ability to respond to strategic threats to the unique identifier and coordinate." Do we have any objection to that phraseology? Can we agree to that as a consensus? Yes?

ERIC OSTERWEIL: Sure. Yes. Okay, looks like we have consensus.

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: It's 5:00 somewhere. Alright, cool.

UNIDENTIFIED MALE: Is this the ability to identify [inaudible]?

UNIDENTIFIED FEMALE: [inaudible]

UNIDENTIFIED MALE: I'm sorry.

ERIC OSTERWEIL: If we can just wordsmith one item – what do you mean by "the"? Okay, alright, so "39: Understanding of malware and abuse vectors and mitigations." Man, kind of feels like small fish compared to what we were just [inaudible].

DENISE MICHEL: [inaudible] but similar rationale that you're using for the conversation we just closed is relevant here, and even more so because of the very specific responsibilities that ICANN has that relate to abuse mitigation in the DNS, and its responsibilities there. But if there's some wordsmithing that someone thinks is warranted – does anyone have details on the clarification that was needed or the concerns that people have?

JAMES GANNON: Sorry. I'm still getting over the last one. I know we have our caveat [chapeau] of within ICANN's remit and whatever else, but malware is content. It travels over the DNS sometimes, and if we're looking at potentially DNS accentuation or something like that, maybe, but I'm not

sure – again, if I can get a goal. I'm not sure what the goal is for this Review Team in looking at something like that.

DENISE MICHEL: So, you have quite a flexible application of standard. So, you can say assess ICANN's ability to respond to or understand malware and abuse vectors as it relates to ICANN's responsibility in the DNS. That's far beyond [inaudible]

JAMES GANNON: I don't understand what ICANN's responsibilities there are. Some content providers do, but I'm still stumbling constantly over this level of responsibility that there seems to be a disconnect on.

DENISE MICHEL: Yes. And so the failure of ICANN to enforce contractual obligations on the part of registrars and registries directly relates to the ability and facilitation of malware. And abuse vectors –

JAMES GANNON: I agree with us looking at the failure of ICANN to enforce its contractual obligations. I don't agree with us looking on the other side of it, the impact of that. That's outside of our scope. We are here to see what ICANN has done, not the impact of that.

DENISE MICHEL: Again, impact isn't contained in 39.

JAMES GANNON: No, but it's part of our entire conversation about this, and it's recurring.

EMILY TAYLOR: Hang on a second. Oh, sorry. Are you –

JAMES GANNON: [inaudible] I wasn't sure –

EMILY TAYLOR: I was just going to say the same thing.

ERIC OSTERWEIL: We may or may not be. I was just going to say –

EMILY TAYLOR: [inaudible] on the issue.

ERIC OSTERWEIL: Yes.

EMILY TAYLOR: Okay. Just a housekeeping item. I'm giving Eric a break as Chair for a second. He's got lots of input on the issues and it's exhausting. So, I'm going to run the list for a little while. I think let's just have a quick time check. It's 20 past 2:00, and just take a breath for a second. We're doing

really well on this, but let's just try to keep moving it along. If we think that we're down into lower level of detail, then we can manage that. So, please carry on with the conversation. Do we have Eric next and then James who's in the queue?

ERIC OSTERWEIL: Yes. So, I'm just – oh, yes. I was just trying to recapture my train of thought. Abuse mitigation, I think this just goes to sort of like the motivations. One of the things I thought I'd read in some of the subtext – but may be wrong – was that there are sort of things that happen that wish, "Man, I wish we had practiced better hygiene, because now we've got this problem over here." So, this is just I think – if I can try to read between the lines, just saying we should consider the things that cause us to wish we had done a better job of hygiene management, because this hygiene has got an SSR implication. Again, it's not a recommendation, it's just what motivates us to look in new directions, I think. That's how I read it.

EMILY TAYLOR: Yes, because of the sort of changeover I'm a bit confused about where we are with this one and what the propose – so we're on 39. Is there a proposal to rephrase it?

UNIDENTIFIED MALE: Not yet.

EMILY TAYLOR: To drop it?

DENISE MICHEL: So, do you need understanding of malware and abuse vectors and mitigations as they relate to ICANN's operational and contractual obligations?

JAMES GANNON: I'm very aware of malware abuse vectors and the mitigations for male abuse, and I don't see where it fits into ICANN's remit. I see where it fits into the registries and registrars potentially for some of them that are also hosting companies and stuff like that, but as somebody who works in this space as well, I'm not seeing the relationship to an organizational review of ICANN.

DENISE MICHEL: Yes.

JAMES GANNON: As I said, if we're talking on the other side of the coin about reviewing ICANN's potential failures and contractual compliance, that's something I'm fully behind you on. I think that's something really important for us to look at. But I think the contextual training that we are putting that into by looking at malware and abuse puts us on the wrong foot. This wording is malware vectors and malware mitigations. That is literally nothing to do with ICANN.

DENISE MICHEL: And perhaps the wording is what is confusing. So, the work that's occurring in DART and the domain abuse data gathering fits in quite well here and is directly relevant to registrars and registries fulfilling their contractual obligations, for example relating to WHOIS, relating to validation of registrations. Sort of a whole series of things. And ICANN has responsibilities in those areas, so we can–

EMILY TAYLOR: We're getting a two hander here, and I'm aware that the energy levels in the room are quite – people are starting to get distracted. We can either have a break and you two have a conversation and try and actually – I think that we're going to have similar sort of – we might have similar, about these or four of these coming up which may – so, that could be one way through. We could have a break. We could just push through. Or how do you want to resolve this? Eric?

ERIC OSTERWEIL: I propose that we take a break and just reset, and maybe there's a conversation you guys want to have – or maybe not – and then we come back and then we hit it fresh because I think we've been blazing really hard.

EMILY TAYLOR: I think so. I think it's mentally exhausting. We might well have to sort of punctuate our work with breaks a bit more regularly than normal: Steve, did you have a comment?

STEVE CONTE: Just a question. Maybe this can be answered after break as a completely – not as a defensive question, but more as an open question on this to James and to Denise for sure, but maybe for us the Review Team too. After looking at the presentation of the domain abuse reporting tool, I'd like to hear if you feel as a Review Team or as an individual if that had relevance to the ICANN mission, because I think the answer to that question might help move this dialog forward a little bit, and then we can work on how to phrase it after that.

EMILY TAYLOR: Thank you, for that. Denise? Eric? Anyone else?

DENISE MICHEL: Sure. Both ITHI and DART, the domain abuse report gathering relates to directly a number of responsibilities that ICANN has. Again, enforcing contractual obligations on the part of gTLD registries and registrars is particularly key, and the increase of a variety of abuses, particularly in the gTLD space is a security and stability threat in different ways. And we have SSR1 directions that also come into play here, I think.

So, my answer is yes or no. There are some other reasons and the reasons why. In fact, that's why the SSR staff is spending a lot of time in DART.

STEVE CONTE: Yes, that's why I want to make it clear it was a non-defensive question. I'm not trying to defend the DART. I'm trying to ascertain whether or not it had value to it. Because there's interest. It's got juicy bits to it, but is there a value to it?

ERIC OSTERWEIL: Point of order, Steve, you don't have to be so defensive, man. It's okay.

STEVE CONTE: I'm sorry, man.

ERIC OSTERWEIL: Yes, okay. So, I think it is very relevant, and I think it's actually very illustrative of a number of the conversations we've had today to explain why I personally think it's very relevant. So, domain abuse. It's got the fact that I might become a registrant and I might take a domain that I've gotten a hold of and do something with it that constitutes abuse in some [lone] person's perspective might wind up in a threat feed or something else. Why is that ICANN's problem? It's not really ICANN's problem, but domain abuse has led to in some cases wholesale blocking of TLDs. And that is a namespace accessibility problem. And you can say that the problem started somewhere else, and that's a fair comment. Nevertheless, the rampant levels of abuse in certain parts of the namespace has led to universal reachability problems. And that becomes an ICANN concern. Whether or not you can decide how ICANN should or shouldn't remediate it is a separate issue that comes up if we ever decide to structure a recommendation around it. Nevertheless, we

were led to this problem that I think falls within the SSR, of our remit, because if something happened very far afield from what may normally seem like it's an ICANN, and that has motivated a lot of the dot connecting that I think some of us have pointed out today. So, I think it's a really good question, so I just used that sort of as a pivot point to illustrate. I think sometimes when we're talking about something that seems like way out of bounds, maybe we need to draw a map to see if it actually is as far out of bounds as it seems. And in this case, I think this is very imbalanced because of topical issues.

EMILY TAYLOR: Can I put myself in the queue? And then you?

DENISE MICHEL: Madam Chair, you may.

EMILY TAYLOR: Steve, to your question, yes. One, it was really fascinating and interesting, but two, I think it does have a direct impact on ICANN's mission. So, I agree with all the things that Eric said, plus I would like to just revive – to remind us of ICANN's compliance role in relation to the contracted parties, and it's important that that compliance role is based on evidence. And if there is a major issue, with all of the caveats about the data, if there's an indication that a particular registry or registrar has got some real problems, I think speaking to registrar colleagues after the events yesterday and the day before, they were like, "If that was me, I would really like to know." It's not just because it's going to

[hound] the compliance action, but also I might have a problem on my network I don't know about. And ICANN has got a role in that.

So, apologies for jumping into the queue. Denise.

DENISE MICHEL: Sure. And so, James, I think if you simply look at some of the reasons why the objectives of the DART program, you'll see some obvious relevances and reasons why it's an SSR issue and why it's an ICANN issue like an objective of assisting the operational security community by sharing open data and data analyzed by the reporting tools, studying malicious registration behaviors, helping operators understand, consider how to manage their anti-abuse and security programs, terms of service, historical tracking of security threats. And those are just the sort of the interfaces with the registrar and registry community, and they aren't addressing the contractual obligations and ICANN's compliance activities in that area, or some of the related issues.

So, I think it would be good to work on phrasing that captures that part and avoids – I'm not sure what we're avoiding in the conversation, but there's a whole range of responsibilities that ICANN has in the DNS abuse area that relate to SSR that would be good for us to capture in a way that makes everyone comfortable.

EMILY TAYLOR: James, and then I think we'll have a break.

JAMES GANNON: Very briefly, yes, stuff like DART is incredibly important. I'm in no contention over that. And its potential use to increase the SSR of the system we're in is invaluable, and it will – I hope – really help Contractual Compliance to step up their game. And when we look at it on that side and when we're looking at it within the world of ICANN and its contracted parties, I agree. But for example, DART does not go off and do malware analysis. It's not looking at the attack vectors that that malware is using. It is a metrics project. It is a data analysis project. It is not studying malware and abuse vectors. It's not doing that, and that's my concern, is that if we accept language like this, it opens a whole area that ICANN really doesn't have a responsibility in.

I'm fully on board with making sure that ICANN has the right tools to study DNS abuse and to inform contractual compliance to do what they need to do and to increase that side of it, but when we get outside of those bounds – which I think this language does – I think it goes too far. Then we're outside of bounds in my opinion.

EMILY TAYLOR: Okay. Understood. My suggestion is that we seem to have agreement about substance, and the wording is difficult. Let's have a 15-minute break. I would really suggest – I can't compel anybody, but we've been inside all day. Try to get some fresh air, have a proper break for 15 minutes and come back. And perhaps we can either note that we need to – we know now what we mean by this. If anybody can propose some rewording after the break, then okay.

ERIC OSTERWEIL: Yes, and I think that's a great idea. I think let's do that, so that would get us back by my own clock 2:48, and I think that's good. And let's say if we come back and we can't put a nail in this, that we move into a parking [lot]. And I think James is making a lot of sense and Denis is making a lot of sense, and I hope I'm making a little bit.

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: Thank you. I appreciate it. But nevertheless, that doesn't mean that we're going to necessarily resolve it. And I think we do have a bit of ground to cover. So, let's see some parking [lot] if we can.

[BREAK]

EMILY TAYLOR: Should we get started? Because we did a little bit of a fib about the 15-minute break and it was more like half an hour. So, should we start getting moving again? And before we start, I'd just like to say thank you to all of you for staying with this. This is exhausting. It requires a lot of brain capacity. In fact, although we're only halfway through the document, we're actually getting quite close to the results of our brainstorming. My hope is that we will either find a lot of duplication or we will feel like the moment has passed for lots of those things and we may be able to move quicker.

I don't want to preempt that process, but I just want to sort of give a sense that the end is in sight. We're nearly there, and this is incredibly useful. Even if we seem to be getting into sort of nuanced wording or difficulties of interpretation, we need to go through this because we've all been involved in some capacity in complex projects, and the terminology that we use now will stay with us for quite a long time.

So, unfortunately, this is a worthwhile thing to try to nail it. That said, I think we don't always have to go into the back and beyond. If others have said what you said, just sort of – and I'm guilty of this, we don't have to repeat what others have said in the interest of moving faster. So, I think I can see that the wording of ICANN 39 seems to have changed during the break.

DENISE MICHEL: Yes.

EMILY TAYLOR: So, thank you to Denise and James for that. Do either of you want to just talk us through that?

DENISE MICHEL: I think we're good.

EMILY TAYLOR: We're good? And that's a yes? Well done, thank you. The next one is risk assessment and management.

DENISE MICHEL: I have a –

EMILY TAYLOR: Yes.

DENISE MICHEL: From my personal viewpoint, I think just clarifying that it is the risk assessment and management directly related to SSR responsibilities since ICANN has a much broader risk management effort.

EMILY TAYLOR: James?

JAMES GANNON: In our new spirit of cooperation, I will support Denise on that, because ICANN has an enterprise risk management framework that is not necessarily within our scope, whereas there is an SSR piece of that enterprise risk management that is. So, yes.

EMILY TAYLOR: So, do we need to note – okay, so yes, so we can change that to a yes. Fantastic. "41: Corporate data security and/or business systems." Does anybody want to – so, just revisiting our defaults, if nobody is speaking to this to justify keeping it in, if nobody is strongly objecting –

DENISE MICHEL: I think we should keep it in. I'm not sure what the clarification was on this, but I think it's relevant to the SSR1 recommendation and relevant to the internal operations SSR of the operations, of ICANN's own operations.

EMILY TAYLOR: Anybody object? Steve, you –

STEVE CONTE: No objection, I'd only like to note that this probably has relation to items 21, 22, 23 which was the ISO stuff that we spent [inaudible] earlier today.

EMILY TAYLOR: Okay. Thank you very much for that. So, we can change that to a yes, and note that there's a degree of duplication. Incident response. Can anyone remember why we were clarifying? James?

UNIDENTIFIED FEMALE: [inaudible]

EMILY TAYLOR: Ameen?

NOORUL AMEEN: Yes. There's a confusion. Please check with item number 34 [inaudible].

EMILY TAYLOR: So, I think we can change that to a yes. Okay?

UNIDENTIFIED FEMALE: Or delete it.

EMILY TAYLOR: Or delete it. Okay, right. Okay, now we're starting to get into the brainstorming. So, we've got sort of slightly more stream of consciousness stuff. So, do we still need on this list, "Is DNSSEC an ICANN security effort?" Would somebody check that we've mentioned DNSSEC in this? I seem to remember that we have. Eric.

ERIC OSTERWEIL: I recall that we have. I'll double check if you want, but I'm certain that I've seen it.

EMILY TAYLOR: Yes, I think we have. So in that case, I would propose to delete this.

ERIC OSTERWEIL: Number 10.

EMILY TAYLOR: "How effective is ICANN's risk management?" Sorry, that's a yes.

"Study the DNS abuse lifecycle." We had quite long conversations about DNS abuse and the limitations. James.

UNIDENTIFIED FEMALE: I think duplicative and delete it.

EMILY TAYLOR: Okay, delete. What are benchmarks and good practices for successful security efforts?

DENISE MICHEL: I think that's also similar to one to just phrase in a different way to 23, 24, 25 and standards and some of the others. Do people like this wording in particular, or do you want to just note that it relates to other best practices and standards?

EMILY TAYLOR: How about we just "yes" it for now, and then on our pause when we look for duplicates – because we probably won't be able to spot everything right now. We just "yes" it for now and then it will get munged with something.

Okay. We're on "Evaluate the DNS abuse threat mitigation deficiencies processing speed."

Clarify. So –

DENISE MICHEL: I think again that –

EMILY TAYLOR: A duplicate?

DENISE MICHEL: Unless someone has [inaudible]

EMILY TAYLOR: Does anybody love this and want to keep it? Good.

                           "Recommend upgrade and revision of security and stability procedures and action plans."

DENISE MICHEL: I'm not sure what that means.

EMILY TAYLOR: Cathy.

CATHY HANDLEY: I think I would probably take that out of there. It's more of a result that's kind of what we're doing through the whole thing. So, I would take it out.

EMILY TAYLOR: So we can delete? "Are SSAC recommendations automatically considered as ICANN efforts towards SSR?"

UNIDENTIFIED MALE: [inaudible]

EMILY TAYLOR: Steve.

STEVE CONTE: [So it's] like that one. There's a process inside of ICANN called the Advice and Request Registry that parses the advice and requests from all SOs, ACs and things like that. And I'm part of the group that looks at the SSAC, RSSAC recommendations and advice. There are specific ones within SSAC that have been submitted to ICANN that are either not recommendations for ICANN or that ICANN feels that it's not within their scope or remit, or other reasons to not take that advice.

So, I think as far as being constructive to this, I think that we can have something in there about ensuring that we evaluate recommendations that come from SOs, ACs, specially SSAC and RSSAC, but I don't think there should be a blanket, "We should just accept what they recommend and implement."

EMILY TAYLOR: Many thanks for that clarification. It's very helpful. I've got Alain and then James. Anybody else want to be on the list? That was a no. Alain, did you want to speak to this point? No? James.

JAMES GANNON: I talk too much. Yes, there is a bit of politics here as well. So, SSAC does not issue binding advice. Only GAC can kind of do that. So, they can't be automatically – I think most things that SSAC write are taken extremely seriously, and usually done, but we can't ever say that they're automatically considered ICANN efforts, because they're not automatically binding to be implemented. So, I'm going to put out a proposal to delete this line.

EMILY TAYLOR: I noticed doing a quick search that the only time SSAC is mentioned in this list is here. Does anybody want to try and capture that as a thing kind of floating around about SO and ACs and sort of interaction with that? Or are we too tired?

ERIC OSTERWEIL: Maybe the fact that it's only come up once means that the group doesn't feel strongly enough about it.

DENISE MICHEL: We may circle back to something that relates to SSAC or RSSAC or another entity as we pursue one of the many topic areas that we have,

so I'm fine either way, leaving it or deleting it, noting [inaudible] we'll have another [connection].

EMILY TAYLOR: So, Cathy, did you want to come in on this?

CATHY HANDLEY: It's more of a question. And it's not really a do, and I don't think it would be in the place of down the road a year from now for us to make something mandatory so everything that comes up needs to be automatically done. So, I would probably get rid of it.

EMILY TAYLOR: James, is your flag up to speak, or are you good?

JAMES GANNON: I've just put a note in. We can delete the line item, and I've put a note in the notes that we might potentially add something around SO/AC recommendations about security somewhere else.

DENISE MICHEL: Yes, I just want to remind people that the rest of the items we're going through – hopefully quickly now – are the brainstorming snippets from that sticky note exercise in Copenhagen. So, a lot of these are just top-of-the-head questions or half sentences. Don't take any of them too literally. I would suggest you use them as a stepping off point to

consider whether they touch on something that we've forgotten or isn't reflected somewhere else, not take them too literally.

EMILY TAYLOR: Well said and well reminded. So, the next one is, "What are the changes to ICANN SSR within the IANA transition?"

My thinking is that we've done this, haven't we? No? Oh, God. Okay, James. Go for it.

JAMES GANNON: Sorry. So, we've done one specific tiny little piece of it, which was a very specific directive. But there's a bigger piece potentially there to be looked at, so I'd like to keep it.

EMILY TAYLOR: Anybody object to keeping it?

DENISE MICHEL: I'd just like to note that we should combine the IANA PTI ones. We've got three of them now.

EMILY TAYLOR: Okay. So, that's a "yes".

DENISE MICHEL: Okay.

EMILY TAYLOR: How to interact with outside organizations. I'm not quite sure what that means. I'm taking it as meaning something to do with outreach. Can we take it as something to do with outreach?

DENISE MICHEL: Yes.

EMILY TAYLOR: No?

JAMES GANNON: There are a million different things that can mean. It needs clarification or removal. If we want something about outreach, that's a different thing.

EMILY TAYLOR: We're doing outreach, so why don't we just remove it?

JAMES GANNON: Yes.

EMILY TAYLOR: Okay. Very good. "What is the significance of those internal, external, blah, blah."

I would propose to delete that, and I can add – I think I remember writing that. And that goes to our terms of reference which we sort of moved beyond this now. "Explore forecasting research on the Internet capacity performance (DDoS)." James?

JAMES GANNON: I propose removing this. ICANN doesn't do Internet capacity.

EMILY TAYLOR: Does anybody disagree?

DENISE MICHEL: I don't know.

EMILY TAYLOR: You don't know?

DENISE MICHEL: So there's DDoS in parentheses there. Does anyone recall contributing this to the brainstorming? Okay.

EMILY TAYLOR: We also have DDoS and extensively discussed it at ICANN 12, so I would propose to remove. I'm not [inaudible] because I went back. Okay. So, should our team consider the future? I think that this is a terms of reference item which has now been superseded. Does anybody disagree? Okay. Please delete.

Can we assess the efforts of prior recommendations? Delete? I think that this is included in –

UNIDENTIFIED FEMALE: I'm sorry, lost my place.

EMILY TAYLOR: Yes, I've just ended up on item 12 again. So, I think this might mean the SSR1 analysis which has been –

UNIDENTIFIED FEMALE: It has been addressed elsewhere.

EMILY TAYLOR: Addressed elsewhere, so I would recommend deleting.

"SSR1 implementation, what were the impacts or results of each successfully implemented recommendation?" I think this is a duplicate item and it can go.

UNIDENTIFIED FEMALE: Yes.

EMILY TAYLOR: I'm now on 68. "Which implementation measures from what were critical or deemed insufficient?" I'm reading this as part of the SSR1 piece. I think –

UNIDENTIFIED FEMALE: [inaudible]

EMILY TAYLOR: Yes? And I would suggest that we delete it, because I think we've got it well covered. 69 doesn't have anything decided, but again, I would suggest it goes. Yes.

So, "71: Review and grade importance and way it is implemented." I think we're in the same territory, all in violent agreement. Let's go. Goodbye.

"73: How are we distinguishing operational stability and security from measures that stem from compliance issues?" I'm not sure how much we've got compliance in our net, as it were. James?

JAMES GANNON: So, this is something I'm very passionate about, as I think everybody knows at this stage. But I like the question, so I'd like to propose that we keep the question because it's something that I think we need to work on.

EMILY TAYLOR: Does anybody object? Agree.

"How can we work on global policies?"

UNIDENTIFIED FEMALE: [inaudible]

EMILY TAYLOR: James?

JAMES GANNON: We have no policy remit. Remove it.

EMILY TAYLOR: Okay. I'm going to get rid of it. We're going to get rid of it.

"Which recommendations are still critical for SSR since the transition?" I think that we have a whole transition piece already. But just noting as we're going through some of these, as James said on the last piece, some of the questions are really good, and if they're helpful in framing it as a question, we'll keep them in.

So, "What does security, stability, resiliency mean?" I would propose to delete this, because I think the moment has passed. We've defined them in our terms of reference which we've agreed. Oh, sorry, Karen, I didn't see your flag.

KAREN MULBERRY: There are a couple of comments in the room from Matagoro and from [Graham].

Matagoro: "My worry is that we are deleting a lot of brainstorming points and this could be a sign that a member have [tried]."

[Graham] agrees with that comment.

UNIDENTIFIED MALE: [inaudible]

KAREN MULBERRY: I'm sorry?

UNIDENTIFIED MALE: Mr. Matagoro is saying that it might be a sign that the members are tired.

KAREN MULBERRY: Tired. Okay. Sorry, I'm having…

And then the next comment – he just had another one: "And for the forecast item which has been deleted, could be replaced with unique identifier rather than Internet."

Another comment: "Emily is too fast and I would request to pay attention to remote member."

UNIDENTIFIED FEMALE: Could you back up?

EMILY TAYLOR:	Matagoro, please accept my apologies, and I will continue to try and pay full attention. So, can we just reverse the last deletion, I think?
UNIDENTIFIED MALE:	[inaudible]
EMILY TAYLOR:	So, which? Is it way, way ago? What was it? The forecast item?
UNIDENTIFIED MALE:	[inaudible]
EMILY TAYLOR:	Can anyone provide –
JAMES GANNON:	It was the one that, "How does the Internet scale to additional devices and how do we do the forecasting of that?" Which is outside of ICANN's remit.
DENISE MICHEL:	You can hop over to the Topics of Discussion document and find it. It was, "Explore forecasting research on the Internet capacity/performance."

JAMES GANNON: Yes.

EMILY TAYLOR: Restore it, put a "yes" on it and sort of mentally note that it will probably be part of that bigger piece.

UNIDENTIFIED FEMALE: Okay.

EMILY TAYLOR: I hope that that –

DENISE MICHEL: And if Matagoro in particular could take a look. Its 77 is where I dropped it in at the table on the document. "Explore forecasting research on the Internet unique identifiers." Is that acceptable to Matagoro and other people?

EMILY TAYLOR: I can see that he's typing, so I'll just wait for that to come through. I think that we are safe to delete 78 on the meaning of unique identifiers. It is something that is covered in the adopted terms of reference. So, I would still propose to delete that.

                       And Matagoro, [inaudible] just to reiterate where we are in the process, we're now – as you know, because I can see from your comments – we're revisiting brainstorming from our very first meeting in

Copenhagen. What we're really doing here is looking for things that we've missed in our issue identification. A lot of the conversation has moved on until then, and that's why we're trying to get through it with quite a light touch at this stage. But please do what you've done and stop us if we're going too fast. Okay?

JAMES GANNON: Can I just make a point of order?

EMILY TAYLOR: Yes.

JAMES GANNON: Can we give Karen the ability to break into a discussion, so that if she sees a comment she can get in there as opposed to waiting for a few, that we give her that empowerment? My favorite word.

EMILY TAYLOR: That would be hugely helpful. Yes, please.

JAMES GANNON: Yes.

EMILY TAYLOR: Just shout. If we're just moving too quickly, because we're so in the document, it'd be just really helpful.

KAREN MULBERRY: I'm happy to. And I go back and forth between your room and the observers' room to kind of keep an eye on if anyone is interjecting anything.

EMILY TAYLOR: Many thanks. So, Eric?

ERIC OSTERWEIL: Yes, just one other point of order. It's 20 after 3:00 on our last day, and it would be really good if we could just bang through this, so I respect that we need to sort of cull a lot of input, but I think maybe at this point going past is necessary. So, just we need to be cognizant of the fact that what we have to do after this is try and de-normalize these a little bit, put them into buckets. So, I'm writing up the ones we've accepted on the little index cards, which is a lot of fun while we're doing this, so that we can try and get a jump on the next session.

EMILY TAYLOR: That's brilliant. And actually, if anybody feels like they would prefer to help Eric with that task rather than all of us doing everything, please do so.

So, the next one is "79: What is meant by both physical and network?" I think I propose to delete because it's covered in our terms of reference. Yes, I believe that the –

So, "81: Impact of evolution in number and types of devices on the DNS." I think that's part of a bigger piece that we're discussing about the evolution of the namespace.

UNIDENTIFIED FEMALE: [inaudible]

EMILY TAYLOR: Yes, so can we keep it in? Anyone?

UNIDENTIFIED FEMALE: I think it would be useful.

EMILY TAYLOR: Okay, anyone want to take it out? Guys, do you want to step into the other room? And then we just –

So, "Parameters to secure the DNS." This is number 82. My proposal would be to delete it because it's very, very broad, and I think we've already gone into a bit more detail now.

Are you driving? Can you scroll down? I've reached the end of –

UNIDENTIFIED FEMALE: I am not on this. Up there, it's Jennifer.

EMILY TAYLOR: Oh. I'm sorry.

UNIDENTIFIED FEMALE: 84?

EMILY TAYLOR: "84: What is the best source to determine most pertinent aspects? E.g. networking scope is wide and covers many actors in the community." I think this is a question that goes to terms of reference, and –

UNIDENTIFIED FEMALE: We've covered it.

EMILY TAYLOR: And we've covered it. I would propose to delete, unless anyone objects.

"What is the main responsibility of the SSR team?" Again, I think we're doing it. So, UI, which I think means unique identifiers, not any medical thing. I think delete it. It's hard to understand.

"Interoperable security processes. How is this currently addressed in domain names protocols and addresses?" Anyone? Steve?

STEVE CONTE: My recommendation is to delete. I read that mostly as an IETF function because we're talking about the protocol and the interoperability and that's an IETF functionality during development.

EMILY TAYLOR: Thank you. Anyone? It's gone.

"Identity and access management." Okay, that's quite a big subject. It has not come up, so it's gone.

"Operational impact on security and stability." I think those are precise words from the Bylaws and it's asking what those mean, and we've been through this.

"What is ICANN's internal level of risk and how is it managed?" I think we've got this elsewhere. Yeah, we have a lot on that, haven't we?

"Conduct performance indicators and benchmarks." Again, I think we've dealt with that under the auditing piece.

"DNS analysis opportunities, malware." Again, we talked extensively around data.

"Is this assessment limited to those organizations ICANN has policy inputs into?" I think this is a terms of reference question and has been superseded.

"Physical security." Now, I think we discussed that earlier and we got it in definitely. So if somebody could, before deleting it, just double check that it's already in there. Because I think we all agreed to that, otherwise it goes. It's deleted. Or can we just "yes" it?

UNIDENTIFIED FEMALE: That's our only reference to KSK in particular if you want to keep it.

EMILY TAYLOR: Okay.

UNIDENTIFIED MALE: Same thing as we had before. "Physical security of facilities."

EMILY TAYLOR: So it's covered already. We can either "yes" it or just delete it because it's already a duplicate, I think.

"How can we ensure security, reliable, unique identifiers? How do our policies affect assessment?" Again, I think that this is captured better elsewhere, and I would propose to delete.

"How do we assess definition of scope of Internet systems, unique identifiers?" That moment has passed. We did it.

"How do we assess when it says conformance? To what extent?" I think these are words from the Bylaws which have been incorporated in our scope and we've gone beyond it.

"How do we assess overall process [at] the implications of security [inaudible] by the Bylaws?" Again, I think that's part of our terms of reference, and that was a job we did as part of that. So that's 100 I propose to delete. I think I'm still seeing it there. Is it still there?

"How do we assess the overall process of security, stability?" Propose to delete.

"How do we assess what are the key points [who] address secure, reliable, and stable DNS?" I don't quite understand what that means anymore. I think we've probably been – yep, get rid of it.

"How do we assess who can address the operational issues?"

UNIDENTIFIED FEMALE: I think we've covered that also.

EMILY TAYLOR: Okay.

"What is the impact of moving the IANA services to PTI? How will this be monitored?" I think we've discussed this and it's captured elsewhere.

"What contingency planning is taking place?" I think that goes to – we did a lot on that earlier.

"What measures are taken to ensure relevance and applicability [of] the contingency plan?" I think we've covered that in a lot of good detail.

"Contingency planning framework. What does this mean for blah, blah, blah?" I think, [Boban], [you're happy] that that's covered in our earlier piece.

"The appropriate contingency planning framework." Again, I think this is the same.

"Whose responsibility for the contingency plan and what is…?" The next three items are all the same. So 107, probably said "yes."

Right, 111: "How does the end user feel secure, reliable, instable?" What do we think about this. I don't think we have anything about end user. Ameen?

NOORUL AMEEN: [inaudible] it's not coming under the SSR purview as per James' [inaudible].

EMILY TAYLOR: So is your proposal that we just get rid of it or that we keep it?

[CATHY HANDLEY]: He was referring to not getting into the client side malware assessment and details, which I think is different than how the end users feel about SSR and the confidence level of SSR. I'm just noting. That's how I interpreted this. I don't know who suggested this, but I think it raises an issue that we haven't addressed yet and that is more of an end user confidence in the SSR and the Internet security, stability, and reliability. It seems like a big bite, but I think it's….

EMILY TAYLOR: Okay, I think it does. That was my pause on this. I don't actually anticipate that we would need to generate a lot of new materials [inaudible] just masses and masses of very solid academic research on things like levels of trust, individual users' sense of security. My suggestion is that we probably just keep this in for now because it has something about end user trust things. Bernie?

BERNIE TURCOTTE: I think we're just wrapping up the consumer trust review. As James was mentioning, why do we go look for work that someone else is actually directly doing?

EMILY TAYLOR: Very fair point.

[CATHY HANDLEY]:   Can I just reply quickly. That's trust in new gTLDs which is different than trust in the SSR of the Internet.

EMILY TAYLOR: Why don't we keep this in for now? James?

JAMES GANNON: ICANN is not [inaudible]. Again, this is a [inaudible]. Do we really want to open it?

[CATHY HANDLEY]:   That's not true.

EMILY TAYLOR: Okay, this is a big item. Margie?

MARGIE MILAM: Yeah, I just wanted to follow up on the CCT work that's underway. They had a consumer study survey and tried to solicit. It wasn't just new gTLDs. It was all gTLDs. Honestly, after a lot of work and money in it, the results were very difficult to actually do anything with. I know that group is struggling quite a bit with the issue. Maybe in Johannesburg you might talk to them about some of the frustration they've had with addressing those issues.

EMILY TAYLOR: I'd like to just run through the list, if I may. Kaveh is waiting to speak, and Ameen. Sorry? You're fine? Ameen?

NOORUL AMEEN: I just want to point out, [inaudible], I'm agreeing with your point. It's not directly [comes under the client side or consumer security]. But if you remember the [incident] of 2015 when ICANN got attacked, it was because of spear phishing campaign. The mistake done by a client, a user, that will impact the organization or any [inaudible]. Indirectly it comes into the picture.

EMILY TAYLOR: Thank you for that. Denise and then James and Karen. Karen, do you want to just leave your prerogative?

KAREN MULBERRY: There are two comments that have been submitted in the chatroom. One from Ram: "Item 111 was discussed during the Copenhagen

meeting." And then from Matogoro: "I propose we rephrase it, but I think end user feeling on SSR need to be captured."

EMILY TAYLOR: Could I ask Matogoro if he could propose some rewording on the chat room? Because I think that, limited though it might be and existing materials [through] there are, we have missed so far. This exercise is really to find stuff that we have missed. I know that there are different feelings about how much resource we should put into this, but ultimately consumer trust has been done. It is within ICANN's purview, and the relationship with security is something that is perhaps missing. James?

JAMES GANNON: That was exactly [inaudible] my proposal. If we want to say that we want to look at this excluding what has been done by the CCT, I'd be okay with that. I just don't want it to get into a second CCT review in this group because we easily could. We could easily consider it within scope. We really could.

EMILY TAYLOR: Okay, Denise, have you got a proposal?

DENISE MICHEL: Yes. I can add a note on that in the final column avoiding duplication of other. And end users are not only customers. Of course, they can be business users, they can be others as well. There are a number of

intersections for ICANN on the policy front, on the compliance front, on the registrant front, and other places. So I think it's worth leaving in, and we can decide later whether or not we're going to actually do work in that area.

EMILY TAYLOR: Are we happy with that?

UNIDENTIFIED FEMALE: Yes.

EMILY TAYLOR: Okay, and nobody wants to for us to also take on tasks of other Review Teams, and that point is well taken.

So 112: "Does this review look only internally in ICANN process?" I think we've gone beyond that. I propose to delete.

"Who is responsible for maintenance and upkeep of the unreadable [inaudible]?"

UNIDENTIFIED FEMALE: All right, get rid of that.

EMILY TAYLOR: That's going.

"What is meant by globally interoperable security processes?" I think that has been – is this something that we've dealt with on the terms of reference? Do we need to keep it in here.

UNIDENTIFIED FEMALE: I think it's quite vague and not worth retaining.

EMILY TAYLOR: Okay. Anyone object? It's gone.

"What aspects of the unique identifier space is relevant to the [definition] of 'security processes'?" Again, I think this has been caught up in the terms of reference.

This is IETF, no? I think let's take that out because it's not IETF. Maybe it meant something else?

"Abuse mitigation" we've covered extensively.

"Global abuse policies and recommendations" I think is better captured elsewhere.

Karen, are you asking for the microphone? You have your thing up.

All right, 121: "ccTLD abuse mitigation" is covered.

UNIDENTIFIED FEMALE: We don't specify [inaudible].

EMILY TAYLOR: "How effective is ICANN's coordination effort with IETF and others?" Have we captured that elsewhere?

UNIDENTIFIED FEMALE: No, I don't believe we have.

EMILY TAYLOR: Okay, I propose that we keep this in. Obviously, where relevant to our scope and ICANN's mission and all of the other stuff.

"Root server stability, security." Again, I think we haven't actually captured that anywhere else and I propose to keep it in as a placeholder, so change it to "yes."

"How the DNS works with secure, reliable, and stable." I don't think we need this. Do you think we need this? Anyone? No. Okay, it's gone.

That takes us to the end of the list. Brilliant. Why don't we just see how Eric and the others are getting on making some sense of that, and then we can move on to that. Well done, everyone. Tiring, but we got there.

Yeah, catch up on your e-mail and they'll be a few more minutes. Those who are joining through remote can just have a little breather.

Okay, for those who are joining on remote, I'm just about to hand over to Denise to chair this last session of the day. A few members of the group have been working through our agreed issues and eliminating duplicates I think or doing some sort of arrangement I think. We're now

going to get on our feet as a team and stick a bunch of sticky labels onto paper on the wall I think.

DENISE MICHEL: If one of the staff people could grab the stickies from the other room for us. We think the quickest way to get these into manageable buckets of work is to just use the sticky method and to have all the team members grab a handful of the stickies that reflect the items in the table and put them in one of three groupings. Then we'll take stock of whether those three buckets seem to be the best ones and move them around, create a fourth bucket or a different bucket if we feel we need it.

We're open to suggestions. We were thinking perhaps the three buckets to start with to see if it makes sense is SSR1, DNS Security, and then ICANN Security. Again, we're just making these up I think, but DNS Security would be the broader Internet/SSR-related efforts and activities, and ICANN Security would be the ICANN operations and activities relating to more specific ICANN responsibilities.

Open to suggestions of different buckets to start out with. Again, if it seems like things aren't fitting very well into all of these, we can easily create an additional one. For those on remote, we're going to step away from the microphones for about ten minutes or so, populate buckets, and then come back and discuss and see where we are.

If team members could get up now and grab….

EN

UNIDENTIFIED FEMALE: [Just] put these on a chair? Because they're individual, so basically you [can only have] one team member per paper to go place.

DENISE MICHEL: Yeah, if you could just set the stickies down on the chairs back here. If people could just grab several and decide which bucket they go in.

CATHY HANDLEY: I know. I'm just curious how we….

DENISE MICHEL: Yeah, Cathy, I think you just missed this little intro discussion. The suggestion was just as a starting point – and if people have suggestions of different titles for these buckets, we can use those. We can create additional buckets. But just to start out, we have SSR1, DNS Security, and ICANN Security. Did you have suggestions of different names or additional buckets?

CATHY HANDLEY: I just thought we identified buckets this morning.

DENISE MICHEL: We had initial strawman buckets.

CATHY HANDLEY: We don't want those now?

DENISE MICHEL: They're the ones that I just said. Those are the three buckets we had this morning.

UNIDENTIFIED FEMALE: No, they're not.

DENISE MICHEL: What are the buckets we had this morning?

JAMES GANNON: There is SSR1….

EMILY TAYLOR: Boban, you might want to pause your work just for a second.

UNIDENTIFIED MALE: Hold on.

BOBAN KRSIC: Okay.

JAMES GANNON: We have ICANN Internal Security Processes, ICANN DNS Security Coordination Processes (a different thing), Future Threats and Challenges, and the IANA Transition.

UNIDENTIFIED FEMALE: We're open. I think part of this exercise is moving things around to see which fits together best. [inaudible], did you have a comment?

UNIDENTIFIED FEMALE: Just a suggestion of setting up an "Other" bucket to see what falls outside of this, and then that might inform the dialogue as to what other buckets you might need.

EMILY TAYLOR: Cathy?

CATHY HANDLEY: Again, when you say "outside of this," which this? What James just read off or the three buckets?

UNIDENTIFIED FEMALE: Either, any, whatever. Whatever buckets are defined and agreed upon by the team, I would suggest an "Other" to see what falls outside.

[CATHY HANDLEY]:   I think we have to agree. What's it going to be?

DENISE MICHEL: Is there one slide with the five proposed buckets on it?

UNIDENTIFIED FEMALE: No [inaudible].

DENISE MICHEL: Okay, SSR1 Review we've got. What's the next one? ICANN Security we've got. What's the next one? DNS Security we've got. What's the next one? Future Threats. And then the next one is IANA. I'm happy to put up Future Threats and IANA and see if we have enough stickies to put in those categories and we can go.

All right, so we have five buckets that we're dividing these stickies into: SSR1, ICANN Security, DNS Security, Future Threats, and IANA PTI. So I would appreciate if all the team members and others would grab stickies and divide them up, and then we'll review them. Thanks.

Are there any other stickers people need help with? Do we have them all on the wall at this point? Let's reconvene then around the mic. Could people take their seats please?

ERIC OSTERWEIL: Hey, everyone. So we're going to push forward. I'm going to do this a little bit freeform at the beginning, make sure everyone feels like this is the right approach. So definitely shout if this runs afoul, something you see. I'm going to just quickly double check that everyone feels okay with the buckets that we have here. I think everything up here is a starting point. So don't feel like things are crystallizing, necessarily becoming ossified.

The buckets that I think you all put together are Future Threats, IANA, DNS Security, Other, SSR1, and ICANN Security. We've all gone around and put the items from our list into the buckets that seem like they're the best respective fits.

Now what I propose we do is we go and we look at the ones that are co-located with each other and see if we deduplicate them, see if we want to re-digest them into something else. At this point, we've talked them all through, so they're hopefully loaded a little bit like in [soft state] in our heads and maybe we can try and wrap them up.

Does anyone have a pad of stickies? Because I'll just write new ones with the group's collaborative input. Like the leftovers from before. Perfect. Oh, pink. I'm totally using pink. Sweet.

Okay, cool. Future Threats. There are four here: "How do we address future challenges?" "What emerging…." Actually, wait a minute. Let me ask a question for a point of order. We can digest these all in real time and try and see if there's a better way to list them and normalize them, or we could just start to say if these are the right buckets, do we want to start seeing who would be amenable to turning them into subgroupings? Whether they become sub-teams or they become milestones that we march toward as a collective team or not?

Because if there's a team of people interested in one item and I'm not interested in it, then I may not be as helpful [and] denormalizing it. Maybe if we identify the constituency for each of these buckets, then that constituency will be the best place to normalize what the work

items are. These are just suggested inputs anyway. What do you guys think of that? James?

JAMES GANNON: I support that because then the group that is interested in that area are the best to know how to bring together the multiple items into that [inaudible] exercise. If you're interested in ICANN internal security and security [auditing], you will know that this one goes with this one goes with this one and will become one item. As opposed to there's no point in somebody who is brand new to ICANN coming and looking at the IANA transition one and trying to consolidate that. It makes sense to me.

ERIC OSTERWEIL: Okay, so Denise just had I think a good idea. She suggested why don't everyone take a sticky or a set of stickies and put your name in the bucket that you'd like to work in, or buckets. That way, for example, if everyone's name is in every bucket, then we'll take the buckets one at a time as a group. Yeah?

[ZARKO KECIC]: You're so stubborn because there is no way to do this like you are proposing. Okay, I will put my name somewhere and what? My name will stay there. And when somebody else needs me or anyone else, what are we going to do? So let's do consolidation together and then work on teams and stuff like that.

ERIC OSTERWEIL: What I was going to propose was that we all work on de-normalizing, and then what I realized is that not everyone may care about something we're de-normalizing. So people might feel like, "Why the heck am I drawn into this discussion?" and they might tune out. Do you think that that's false logic?

[ZARKO KECIC]:   We are already a team, so all of us should take care of everything. Yes because….

ERIC OSTERWEIL: I think I know which buckets your name is going in. All of them, right?

[ZARKO KECIC]:   No, I'm not going to put my name anywhere because I will work on where I am needed, not where I want to do.

ERIC OSTERWEIL: Okay. We can proceed down whatever path anyone likes. I am very stubborn, but I'm not trying to be stubborn about this. I'm happy to take input or even to stand down and another direction subbing. If there's a suggestion, I'm totally interested. I see Steve and James and Zarko.

[ZARKO KECIC]:   Yes, I have a suggestion because at the beginning of projects, first you have tasks to do. Then you add resources to that. So we are working on

tasks or we are adding resources to some foggy stuff and we'll then redo tasks.

ERIC OSTERWEIL: Honestly, to be a little bit tongue-in-cheek, this is Agile methodology. This is one way to do resource management. It may not be everyone's favorite, but it's almost like a Kanban board up there – almost – but okay. James?

JAMES GANNON: I was about to say exactly the same thing. We have identified our work breakdown structures, we're adding project tasks into those work breakdown structures, and we're assigning team members to it. This is a standard working method for ICANN groups. It may not translate to external methods. It's pretty close to an Agile working method. That was one of the models that was used when this working method was brought up, and it has been proven to work really well in this context.

[ZARKO KECIC]: Okay, that's fine with me.

ERIC OSTERWEIL: Steve?

STEVE CONTE: Just to add maybe an alternate way to look at this because we're not an organization on our own here, we're individuals and we don't know

each other's skillsets. Instead of looking on it as the ones you want to be in on, maybe look on it – because you know your skillset better than anyone else here – so maybe look at it from where you think you'll be needed and add your name in that way.

[ZARKO KECIC]: Yeah, that's true. When I have final tasks, I can assign myself to the task, not to a group of tasks.

ERIC OSTERWEIL: Okay. Alain?

ALAIN PATRICK AINA: [inaudible] agree with him so that we need to finalize these [things] before we can decide where we want to be. Otherwise, honestly I'm not comfortable right now because I'm not sure we are at the final version of all of these things, [so starting putting in names].

ERIC OSTERWEIL: Okay, that's cool. So it sounds like, if I can read the [inaudible] consensus, it's let's go through all the buckets together and denormalize them together and then we'll get a sense of what each bucket has in it. Then people can decide where they're needed.

EMILY TAYLOR: Eric, what does "denormalize" mean in this [context]?

ERIC OSTERWEIL: I'm sorry. I meant normalize. I mean deduplicate. I put deduplicate and normalize together and I got the opposite of what I meant. What I mean is let's go through and let's look at all the things that are there. Let's remove duplicates or let's synthesize things that are getting at a common theme but not well and put one sticky for five or something like that.

What I would propose is, if you would like, I'll take the roving mic and I'll go bucket-by-bucket and I'll refresh our memories of the stickies that are there and we'll see if we can come up with a better set of things. Does that sound nauseating or realistic? Yeah?

[ZARKO KECIC]:   Yeah, that's one thing that we have to do. And another thing, we have a number of high-level tasks over there. They can be put into [inaudible] groups, not only one. So maybe on one paper we'll have two or three.

ERIC OSTERWEIL: You mean like I see a sticky and we put a copy over there and put a copy?

[ZARKO KECIC]:   Yes, exactly.

EN

ERIC OSTERWEIL: Okay. Yeah, that's fine. Absolutely. Okay. So I'm going to give that a shot. Can I hand the mic off to somebody else please?

DENISE MICHEL: What am I doing? Reading off the [inaudible]?

ERIC OSTERWEIL: Yeah, and then [inaudible].

DENISE MICHEL: All right, you won't be able to see me, but I'll start over here with the bucket called Future Threats just to quickly read for you the stickies that are here.

"How do we address future challenges?" (That's specific.)

"What emerging technology should we consider?"

"What is the impact of the evolution in the number and types of devices?"

"How effective are ICANN efforts to prepare for future threats?"

So these are quite broad topics under future threats. Does this resonate in particular with anyone that they would like to lend their expertise? I think it probably needs to be defined a little bit more. If there's someone who would like to take a rapporteur position for Future Threats, perhaps the rapporteur could help flesh out what a Future Threats group might be addressing.

IANA is the next group. Under IANA, we have:

"Changes to SSR vis-à-vis IANA transition."

"Business continuity plan for new IANA functions operator."

"Scope of ICANN SSR responsibilities under IANA PTI."

We already have two members who will lend their expertise on this topic/group. That's Cathy and James. James?

JAMES GANNON: Are you asking for rapporteurs now?

DENISE MICHEL: Sure.

JAMES GANNON: Either myself or Cathy, I'm happy.

UNIDENTIFIED FEMALE: [You can do it.]

DENISE MICHEL: All right.

JAMES GANNON: Co-rapporteurs.

DENISE MICHEL: Anyone else on IANA at this point? Again, we'll be going through these groups and have them open for additional members.

ALAIN PATRICK AINA: Okay, for point of order. I don't know. Would it be possible for [inaudible] we put the work item on the screen? It's possible?

DENISE MICHEL: Sure. Jennifer, do you want to put the table up on the screen? Pardon? Yeah, I think it's going to be difficult for staff at this point on the fly. But I think within the next few hours, they'll be able to organize the table according to the buckets that we have. James?

JAMES GANNON: Thanks, Denise. We've done a paper-based exercise, so people need to go over to the wall to look at the paper-based exercise. We're good, but we're not that good at being hybrid digital-paper. If we've done it on paper and our organization is on paper and everything else, then we need to continue to do it [over there].

DENISE MICHEL: How many people do we have remotely? I'm happy for people to get up and go look at the items themselves. I think part of the exercise that Eric was keen to walk through is to identify any duplications that we have in there. Karen?

KAREN MULBERRY: The two review team members we have remotely have left the room, and I don't expect Matogoro to be back. Ram said that he may be back, so it just depends.

DENISE MICHEL: We'll continue then, flag any duplications in DNS Security and identify – okay, here we go.

"Assess DNS threat landscape, domain abuse, and mitigation relevant to ICANN's role."

"Analyze policies and procedures that are essential to ICANN's identifier system activities."

"What is the scope of ICANN's threat modeling?"

"Assess ICANN's ability to respond to strategic threats to the unique identifiers it coordinates." Should we put that together with threat modeling as a way of...?

JAMES GANNON: Denise, [inaudible] on the record. We have no observers and we have no remote members, so can we make a [inaudible] that we don't need this on the record and can be just a team exercise here?

DENISE MICHEL: Yeah, if people are more comfortable coming up to the window, we're happy to do that. Maybe that's a better way given the lack of [engagement today]. We'll stop the mics. We'll reflect the groupings on the wiki and on the e-mail lists. If people could go up to the window, put your name on topics you're interested in being engaged on if it so moves you, and group stickies together if you see duplications that should be addressed. Let's take ten minutes to do that and then regroup for our next steps.

We'll give people just a couple more minutes to wrap up – the windows with the stickies and then we'll do our real wrap-up for the day. Okay, let's wrap this up. Okay, we're in the homestretch. It's 4:30 and we're scheduled to end at 5:00. I think people's energy levels are waning, so 5:00 might be a good wrap-up time. Although I know Cathy really wanted to work later than 5:00.

CATHY HANDLEY: [inaudible] tomorrow.

DENISE MICHEL: So you say. I think the next steps for us are to get staff to help record the groupings, the major buckets that we've organized these topics into. Note the duplicate groupings or the items that have a strong connection or commonality, reflect that as well. And put all this online.

Give team members a little bit more time to reflect on whether they see anything missing, reflect on whether they see any additional duplicates

or additional items they'd like to discuss further, and most importantly identify groups or topics they're particularly interested in working on.

Then finally, we'd like to in particular identify a rapporteur volunteer for each group. I think James and Cathy have already volunteered for the IANA group, so right now we have four other groups for which we need a rapporteur, a person to help take the lead in getting additional team volunteers. They'll be the person who will take the lead in reporting back to the full team on the team's activities and helping to organize the work to move forward.

We have the follow up effort to flesh out our buckets of work, which seems like may lend itself to a subgroup approach. I'm happy to discuss that further if people think it's a bit premature to move into the subgroups at this point. But in any event, we'll group our many issues together under the subgroup or topic areas and complete this exercise, put it online to give members who are not here a chance to contribute to it, and then in the next couple days, consider that final for this exercise.

We'll also over the next few days as our follow up look at our overall timeline for the Review Team's work, our target date for completing our activities and submitting our final report, as well as the interim key milestones. In particular, review the placeholder date that we have for our first draft report that we want to issue to the community to get feedback and work with the rapporteurs of these groups to come up with a more robust workplan. See if we can get agreement over the next week on a more specific workplan for the team's efforts.

I'll stop there and invite questions, comments, disagreements, additional suggestions on moving forward with this work. Anyone? Margie?

MARGIE MILAM: Just one of the things to consider. So you're essentially suggesting five sub-teams? Is that essentially what you're thinking? Because that's a lot of sub-team work to manage.

DENISE MICHEL: I have Eric and Boban.

ERIC OSTERWEIL: One thing we could consider is that the sub-teams don't literally break off and go away. It could wind up literally just prioritizing work and marching straight through it.

DENISE MICHEL: Boban?

BOBAN KRSIC: [inaudible] the fact that we have only three tasks on the IANA subgroup, maybe we can, I don't know, group two topics.

[DENISE MICHEL]: The Future [Threats] is a small group as well.

BOBAN KRSIC: [inaudible] also a small group. And we have DNS Security or ICANN Security, and ICANN Security I think we have 30 or 35 [things there].

DENISE MICHEL: James?

JAMES GANNON: I'll give a counterpoint that not all of these have to start at exactly the same time. The IANA one can start in three months, six months and we would be able to work relatively quickly on that. Same potentially with the Future Threats one. There might be a little bit of a kickoff and then there could be a period of quiet. These do not have to be five concurrent subgroups. We have to remember that. That's the workplan piece, which is why I thought it was important to get this done first so then we can work into our workplan resourcing, scheduling, availability, etc.

UNIDENTIFIED MALE: Okay, that means let's start with topics SSR1, DNS Security, and ICANN Security.

DENISE MICHEL: It sounds like a good suggestion to me. Other people's reactions? SSR1, ICANN Security, DNS Security as three groups to work in? James?

UNIDENTIFIED FEMALE: James agrees.

DENISE MICHEL: Emily?

EMILY TAYLOR: That sounds like a great suggestion. There's something I hadn't really thought of, but I think it could be included in the Future Threat work, which is some sort of write-up of the threat landscape that we spent some time exploring. Help me out here, how to [inaudible] in a project manage-y way, but I imagine that in the final report that we generate there will be a piece of background which is like, "Here we are in (whatever year it is). This is how cybersecurity is generally. There are lots of areas where ICANN doesn't have a role and (blah, blah, blah)." A sort of scene-setter. I just wanted to not lose track of that, and I would imagine that we just pop it in as another work item with the Future Threats because it's very similar sort of big picture landscape-y type of thing. Sorry.

DENISE MICHEL: Thank you, Emily. That sounds like a good suggestion. Other comments? James?

JAMES GANNON: I want to make a suggestion that we do not write that. That we get somebody to write it for us. That's a chunk of work that is easily done by somebody else.

DENISE MICHEL: Are referring to the threat assessment, Future Threats? Yes.

JAMES GANNON: Yes.

DENISE MICHEL: Yes, I would agree with that. It lends itself to a first draft by someone that's really familiar with this set of issues, and then we can edit and expand on it as needed. I think that's a good suggestion.

Other comments? Suggestions?

All right, so we have a finalization of these groups. We have a request for topic experts, rapporteurs. We'll do work in the next few days on a more detailed workplan. All of these will be on the list for additional input, thoughts. Push back if you think we should handle this differently.

Staff, could you remind us if there are other outstanding issues that we need to address here today before we conclude.

KAREN MULBERRY: We had circulated some time ago a draft workplan, and it is in essence a timeline. So you have some idea in terms of managing your project, the steps and the amount of time. At some point, we just need to look at it and adjust it so we can get it posted on the wiki page.

DENISE MICHEL: Yes. As I indicated, the follow on work after today is to in finalizing these buckets of work also formalize a more detailed workplan that will apply to the subgroup work as well as the team's work overall. Thanks for the reminder that the workplan is a deliverable that we have for the Board and the public. So that will be our key piece of follow up work coming out of this afternoon.

Any other items that we need to address?

JENNIFER BRYCE: Hi. We had Outreach Plan and Next Steps on the agenda as well.

DENISE MICHEL: Right. I think in the interest of focusing on our buckets of work and topics to cover we decided to punt on the outreach discussion to move it either online or to our next conference call.

Anything else that we've left hanging for this afternoon? No? Then could staff remind us? We're not having a call tomorrow since many of us will be in the air. So it will be next week. Could staff remind us when that call is? Then I'll open the floor for any closing comments, remarks people may have. James?

JAMES GANNON: The call is at 7:00 UTC.

DENISE MICHEL: Thank you, James. Next Tuesday.

UNIDENTIFIED MALE: [inaudible]

DENISE MICHEL: 6:00 UTC?

UNIDENTIFIED MALE: [inaudible]

DENISE MICHEL: Ah, okay. Anything else before we wrap up? Well, thank you, everyone for volunteering your time and taking time from your busy schedules to be here and join us in this work. We will look forward to working with you online. It's important to keep up this momentum. We're encouraging everyone to follow up and keep up the engagement online. We'll look forward to information from staff hopefully in the next couple of days on the Johannesburg meeting plans. That will be our next face-to-face opportunity, but we're hoping to get some important work done before we come together face-to-face in Johannesburg in late June.

I think with that, Emily?

EMILY TAYLOR: Thank you all so much. The level of engagement, both from the people in the room and the online room, has been fantastic. I really feel personally that we've developed from a group of individuals to

approaching a team, and that's so important as we get to the next steps. So thank you very much from me.

We do have a lot of work ahead, and just to repeat, use the list. Please engage in the calls as you have been doing. I think that, Denise, apologies if you said this, but as we develop the workplan into a formal document, I think those of you who have formal project management experience can really help the team there in getting that into a really good format. You know who you are, and that would really be greatly appreciated as we move forward. So thanks a lot, everyone.

DENISE MICHEL: We're done. Thank you all.

[END OF TRANSCRIPTION]