ICANN Dakar Meeting
Joint DNS Security and Stability analysis WG (DSSA) - TRANSCRIPTION
Thursday 27th October 2011 at 11:00 local

Note: The following is the output of transcribing from an audio. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.

Mikey O'Connor: ...how we conduct this analysis. And again this is pretty preliminary and probably pretty inside baseball for observers. But again you're all welcome to stay.

So while the Adobe room gets sorted out, Olivier, I'm going to just throw a dart and see if you're in the room and see if you wanted to kick off our discussion about what you've heard this week about the work we've done and so on and so forth.

Julie Hedlund: Mikey, this is Julie. Olivier is unfortunately not in the room so your dart did not hit its target.

Mikey O'Connor: Oh rats. How about some other co chairs? Any other co chairs...

Julie Hedlund: And we did send you some information about the Adobe Connect room. We do actually have several people in the room so we've sent you a link to that and hopefully that will sort that.

I do have Jörg here and also - and Jim Galvin was here but did have to leave. But I don't know if Jörg wants - ok Jörg is saying he's only (unintelligible).

Jörg Schweiger: So hi, Mikey, hi everybody. Jörg Schweiger, Co Chair for the ccNSO. So I try to give Mikey a couple of minutes to sort himself out. And doing so by giving a very brief report on how our information or our - the work of the DSSA has been received by the ccNSO.

Although I do have to admit that - the feedback was quite brief and that might just be according to the fact that the presentation of the working group's work has been moved around the agenda of the ccNSO meeting for a couple of times at least behind the scenes so probably nobody was aware of the fact that there would be a presentation.

But if I look in the back there at least a couple of ccNSO members so they might just - solicit their input to what we've been doing in this very meeting. So to put it briefly just one kind of feedback and that was (Ronoh) sitting behind me asking whether or not we are considerate with any kind of governmental interference as well and if that is in scope or not.

And we agreed on that as we clearly do see that any difference with governments would be in scope of the (unintelligible) that are being taken of by the DSSA. And that's all I got concerning the ccNSO.

Mikey O'Connor: Thanks Jörg. I'm in the room, yah. I think I got in too early. I had to restart a whole bunch of stuff. And so any other co chairs in the room? Or if not I'll feedback what I heard from the GNSO. Anybody else there?

Julie Hedlund: Mikey, there are no other co chairs in the room.

Mikey O'Connor: Okay well in the GNSO session we talked about several things. One is a suggestion that as we get deeper into the analysis here we engage the DNS providers especially some of the independent DNS providers as resources in our group.

And one of the things in our charter and part of the project that we're in right now is to reach out beyond our initial membership when we see the need for additional expertise.

And I thought this was a pretty neat idea so I think we'll take this one under advisement in the co chair group and see if we can find some folks that could join us.

Another point that was made was that in this update deck we make a pretty important point which is that the scope of the DSSA work is pretty narrow; we are looking only at the - essentially the root and TLD levels of the DNS. We are not looking at levels in the second level or beyond. And we're not - we're certainly not going out to the edge of the network.

And we make that point pretty vehemently. Let's just see how my skills are here? There's the charter. I'm hoping that the screen is synced for everybody in the room so that when I roll around you can see it. This is the point that we made about scope. And you can see how narrow our focus is. And that's not a decision of the DSSA per se that's a decision of the five ACs and SOs that chartered us.

And the point was raised that we should make this really clear in our report. And I agree with that. And that we may experience some disappointment from some who would hope that our scope was broader. And that may be true but this is our scope. So that was one of the points that was made in the GNSO.

And then one quite lively technical discussion that launched in the GNSO session and then carried on onto our list was a point that Bill Manning raised about an interesting puzzle with regard to DNSSEC and the conflict that it may or may not experience when people stand up reputation management systems.

And that one carried over to our list and we've had a pretty lively discussion mostly between Bill and Jim Galvin but others as well. And I think that we've agreed that that's one that's going to go into our analysis pile probably in the area of operational vulnerabilities so on and so forth. I won't go too deep into that discussion. But anyway it was a good conversation. And we got some good feedback.

Julie, I'm going to ask you to be my eyes and ears here and ask for a show of hands in the room would it be useful for people in the room if I very quickly took you all through this update slide deck? Have all of you been in another session where we updated you on our progress or would it be useful for me to just very quickly go through this again? And if Julie could just let me know what the sense of the room is.

Julie Hedlund: Hi, Mikey, this is Julie. So we do have a few people who say it would be useful based on a show of hands. So I think that's probably a yes.

Mikey O'Connor: Okay well let me just very - and I'm assuming that I'm controlling the screen, right? So...

Julie Hedlund: You are controlling the screen in Adobe but I'll just need to follow on from your queues here in the room since the Adobe and the room slides aren't synced.

Mikey O'Connor: Oh okay. All right well let me...

Julie Hedlund: Oh actually it's not a problem for you. Kristina is now right next to me so I can watch her screen which you're controlling in Adobe Connect and then I'll know where we are.

Mikey O'Connor: Okay perfect. Well let me get back to our charter. This is just a reminder - and I've already sort of touched on this - but we are a group that was chartered by a very broad collection of ACs and SOs. The list is there on the screen for

you. And our mission is really to gain a better understanding of the security and stability of the global DNS.

That's not to say that we are chartered to make sweeping recommendations or anything like that. We are really a group that's trying to gather data, conduct analysis, reach new understandings.

So the goals - we'll skip that. Here's where we are in terms of the work that we're doing. We spent basically the inter-sessional - leading up to Singapore getting ourselves launched. And then between Singapore and now the first part of our work plan is to really identify threats and vulnerabilities and a kind of informal assessment of that is that we're about 70% of the way there.

We've got some issues that you'll see in a minute are still under discussion and we've got some work to do to really flesh that out. But we're making pretty good progress against a very big base of information. And so I would - if you were to ask me as a project manager how you're doing I'd say we're on track and doing a darn fine job thank you very much.

A quick slide just talking about what we've been doing. And again we've been working on vulnerabilities and threats and so on. One of the things that we have worked pretty hard on is the issue of confidential information is a big deal for this group because when we get into the analysis there may be the need for the sharing of that kind of information.

And we needed to make sure that everybody who is going to be providing the information, primarily registries and registrars and the like and maybe DNS providers, are comfortable that their information is safe. And so we've got a pretty good protocol that's nearly done. We're not quite done but nearly done on that.

And as you can see we're in the solicit additional ideas phase right now. And for those of you in the room this means you. So as you listen to the rest of

this feel free to chime right in and give us some more ideas. And we need to put these threats and vulnerabilities in some sort of priority sequence. We will not be doing that today. We will pick on. But over the next few weeks after Dakar is done that's one of the big focus points is to rank order this list that we've developed.

So the next slide is trying to show just how big the pile of information that we've been looking at is. And it doesn't really do a very good job because the stuff on the left is a tiny fraction of the huge piece of work that the working group has done. And what we've done is ruthlessly consolidated it down to the three pages that you see on the right. And we'll get to those in a second.

We did have a pretty lively debate as to who the owner of the quote at the bottom is. And we've decided that we are part owners of that now. This is the scope thing and I talked about a minute ago and then onto the threats.

So the first pile of threats we've started thinking of as sort of threats to the underlying infrastructure itself. And in this category we have four very broad topics that we consider in scope for our analysis listed at the top of that page.

In the middle we have a topic that we haven't finished discussing yet. Whether the business failure of a registry is a threat to the underlying infrastructure or not and there are good cases to be made on either side of that. And if you have thoughts about that we'd love to hear them.

And then at least on a preliminary basis we've taken the depletion of the IPv4 address pool out of scope primarily because the routing table growth is going to happen no matter what and the DNS itself is not a heavy consumer of that.

And again if you are very deep into the IPv4 address pool depletion thing and you think that it will impact the DNS in the narrow way that we're thinking about it we'd love to hear from you about that.

The next page is direct attacks. And we have a series of attacks that we have in scope. Clearly DDoS attacks - not all DDoS attacks however - we want to make it clear that these are just DDoS attacks against the root and TLD servers not all DDoS attacks against everybody on the Internet.

All of these in scope threats are with that caveat. You know, we're not going to deal with everything to do with packet interception. We're going to look at packet interception attacks as it applies to the root and TLDs.

In the middle are a couple that we're still working on. IDN attacks, again against root and TLD. We've decided that we're going to hang on for a bit and wait for the variance projects to get done and circle back to this one. And then we're still debating the malicious or unintentional alteration of DNS configuration information at the root and TLDs again.

And then we have several that we've taken out of scope. Footprinting is a term that's used when you scan the zone files of an infrastructure provider and build a footprint of their infrastructure by doing that. There are a number of these kinds of things that we think are threat factors but they're fairly limited and they're not likely to cause widespread instability. Same point on this slide which is if we are making a mistake we'd love to hear about that.

And then indirect attacks we have one that's in scope and a number of them that are out of scope. The out of scope ones are primarily out of scope because we don't feel that these are attacks against the DNS at the root and TLD level. This is not to say that they're outside of ICANN's scope, that they're not important they're just outside the scope of our project.

But in scope is a pretty esoteric email problem which is that as IPv6 roles in there's the possibility that bad actors will hop their servers very rapidly across a large number of IPv6 addresses in the address space which may cause collateral damage at the root or the TLD. And so we're going to take a look at that one.

And then the last sort of work product page is a list of the vulnerabilities that we're going to take a look at. And the way to think about this page is at the top are a bunch of operational issues, infrastructure vulnerabilities, technical process vulnerabilities and so on.

At the bottom are a series of managerial choices which may induce vulnerabilities. And in the middle is a pretty broad topic that aims to look at the issues around registry failure and continuity. And we put that in the middle because it really contains both operational and managerial issues.

So that gives you sort of a sense of what we've been doing between Singapore and Dakar. Hopefully that's useful. Maybe I'll turn it back to Julie and listen in as - if there are questions or comments from the room. We'd love to hear those and get them on our record and we'll pull them into our analysis as we go forward. Julie, you want to take over for a minute?

Luis Espinoza: Yes, Mikey, Luis Espinoza from (unintelligible). I was thinking about threats out of the scope because like example registration abuse could be in scope if that threat could affect IANA by example.

They mention many of the things are out of scope if we analyze against root or top level domains issues or entities. Now we can - getting the scope but specifically talking about this organization by example. That's my comment.

Mikey O'Connor: Yeah, I think that's a good point. And I - we - one of the issues that we've got as a group is that we do have to draw some sort of boundaries around what we do in order to get done because as you can see from this list we've got a pretty gigantic piece of work to do.

But our goal is not to be so ruthless in narrowing our scope that we miss something important. And that's part of the reason why the co chairs are

characterizing this as not done yet because we do have some issues like that to still work through. Thanks Luis.

Julie Hedlund: Hang on, Mikey, we do have a question and I'm getting a mic over to this person. Hold on.

Mikey O'Connor: Okay thanks.

(Zimame Bakhoum): Okay sorry. Another question but is in a different - okay - okay, another question (unintelligible). For this important section I think you must - you have to make some (translation) this would be for someone who don't speak really English. But it's an important (session) we have to participate. Thank you.

Mikey O'Connor: Julie, if you could get the person's name it's good to get that in the transcript. I agree with you a lot. One of the problems with this particular session is that this is really a face to face session for the working group itself. And as a result I bet there is not transcription - live transcription going on in the room.

Julie Hedlund: Mikey, this is Julie. There isn't live transcription but it is being - it is being recorded. The gentleman's name was (Zimame Bakhoum).

Mikey O'Connor: (Zimame). Thank you very much for that thought. And I think one of the things that we will do for our next session is plan a little bit better for participation by people outside the working group. Any other questions from the room, Julie?

Julie Hedlund: Yes there is, Rod Rasmussen and then the other gentlemen.

Mikey O'Connor: Okay. Uh-oh, Rod Rasmussen is really smart. I'm in trouble now.

Rod Rasmussen: More of a - well I won't say it - a smart something. This will be in the transcript. Anyway, Mikey, good to hear from you. I wish you could be here.

Mikey O'Connor: Me too.

Rod Rasmussen: The - I saw this earlier in a couple other sessions and I've been chatting with this - with these definitions and scope issues with a few people. And as you might imagine I have a different opinion.

And I just got a couple of observations and specific examples. And I think the biggest thing I have an issue with is calling TLDs and the root the DNS because the DNS is - it includes everything.

So just the terminology I would suggest coming up with a different terminology set there or you're going to have a lot of people discounting some of the things that are going on. And I appreciate that you need to have a bright line somewhere given the scope of work.

A couple of the interactions I see here too is everything above the root has - is defined based on second, third and fourth label via the name servers, right? So you can't get away from looking at vulnerabilities without looking at vulnerabilities in those levels anyways if you're just talking about TLDs because they all have name server definitions somewhere in the hierarchy of this farther down.

And another concern I have - and I'm sorry there is a volume of work there and I haven't been able to go through it all. But was there consideration given to - especially ccTLD registries but I'm assuming that some of the new gTLDs will do the same thing in that they create sub - you know, they create second level labels within the ccTLD that are then run by the registry themselves so co-UK, com.au, those kinds of things are second level.

But basically considered, you know, for all intense and purposes first level for people doing registrations underneath them. So those are - I think that's a consideration if you define TLD as just the two - the first part of the - first word in the DNS string you're going to miss a lot of what is practically considered a TLD.

And then just my last comment on this was that I would say that if you are - if you define it as narrowly as you are as far as TLD and root - and a lot of the vulnerabilities and risks and things that are mentioned are really pretty well taken care of at least for major operators.

The big TLDs and the - obviously root are being run and a lot of these things have been baked in the process already. So it becomes a lot easier to solve the - or put together a report that - I'm not sure that you're capturing the essence of where we're going to see risk. So there's my comments.

And if you could answer that question I had on the registry subdivisions that - I'd appreciate that if you can. I'm not sure whether or can or not but I appreciate it.

Mikey O'Connor: Well, yeah, Rod, you're going to get the standard co chair process guy answer on this one which was - which is this, and that - darn good question. I'm not sure I have an answer.

We - as far as I know we haven't explicitly thought of that. And so I think it's - it's this kind of conversation that's really important. Jörg may want to jump in on this one. I'm not sure if that's the one that...

((Crosstalk))

Jörg Schweiger: Yeah, that is exactly the one I was...

((Crosstalk))

Jörg Schweiger: ...I was trying to answer. And first, Rod, thanks a lot for mentioning that once again because there have been intensive discussions whether or not it does make sense to just take a look at the root level and the TLD level.

I, speaking in my own capacity, do not think that we are deep enough in that respect, myself. But the decision to stated that way was just due to the fact that we have been chartered that way so we would have really to amend or broaden the charter saying we're not only concerned with TLDs and the root.

And I think the charter has been drawn the way it actually has been because that's ICANN's role. And that's the reason why I do see that the charter is the way it currently is.

And if we really feel that the complete work is simply going to go nowhere or is leaving the major - the major issue out of scope and out of concern we would really appreciate a strong word of the community towards that. And we just might want to approach our charterer to see what we can do with that.

Mikey O'Connor: This is Mikey. Let me follow up on that. I think there are several courses available but one is to head back to our respective ACs and SOs for a revision of our charter. Another is to finish this round of work under the charter we've got and include in our recommendations observations about major issues that fall outside our scope but which need consideration.

I think there are lots of ways to handle this that we can explore. And I'm back to my original response to Rod which is I'm not sure that the question the way you framed it has - we've certainly talked a lot about the scope in terms of TLD and root. But I'm not sure that we ever brought up the subtlety of what your point was which is essentially TLD-like sub domains under ccTLDs like co.uk just to pick on them.

So, you know, I think this goes in the good feedback let us go back and chew on it pile. And, you know, a heartfelt thanks on that one.

Julie Hedlund: And, Mikey, we have a question from Andrew Sullivan.

Mikey O'Connor: Okay.

Andrew Sullivan: Hi, this is Andrew Sullivan. On the topic of the name servers for TLDs and you're quite right of course that most of them are inside some TLD. But surely within the charter, at least as I read it, you could include that as in scope even though you're not including all the things below that because it goes directly to the operational conditions of the name servers themselves.

So I think that - I think that that can be considered completely in scope. And I completely agree with you, however, that it darn well better be looked at.

Mikey O'Connor: Yeah, I think that there's probably pretty broad agreement. What's your experiencing here is the balancing act between sort of the right thing to do and the limits of running a project.

One of the issues that I as a former project manager always worry about is that the work gets so big that we never finish. And that's part of the reason that I'm tip toeing around this so carefully is I want to make sure that we get something out to the community in a reasonable amount of time.

Andrew Sullivan: So I - this is Andrew again - I appreciate that. But I do think that compared to some of the threats that you've identified like for instance, I mean, you know, the sort of physical infrastructure threats to most TLD name servers (unintelligible) the entire set are considerably lower than screw ups in the delegation chain which happen, you know, practically weekly if you look at the logs.

So, I mean, you know, that's a kind of threat that I think is sort of super important. And if I were having to make that choice then I would - there are some things here that I would deemphasize as compared to that delegation chain issue for the name servers themselves which has been a long-standing thorn.

Mikey O'Connor: Yeah, yeah, I hear you. Well this is perfect. Let's keep this going. You know, I'm going to try and b e as transparent and neutral on this as I can because I think I ought to. But, you know, this is good stuff.

Rod Rasmussen: Hey, Mikey, this is Rod again. And I want to just elaborate on that last point as well - well two things; one is that unfortunately because if you're looking at vulnerabilities or issues within the name server space you kind of bring in all those other vulnerabilities - well how does that become vulnerable? Is it because of all these things that you've put out of scope? So it's a tough dilemma there.

The other thing too that I would point out that...

Mikey O'Connor: Oh, Rod...

((Crosstalk))

Mikey O'Connor: ...on one thing because there is an important clarification that I need to make. And that is that if one of those things in red is a threat factor to the root or a TLD then that's in scope. What we're not going to do is all of those threats to all layers of the DNS.

Rod Rasmussen: Right. I realize that. And it's a curse of nature of DNS, you can define things in a higher level than you're actually at.

Mikey O'Connor: Yeah.

Rod Rasmussen: The other thing I would point out is that because of the way the TLD operations - the name servers are set up you often have cross-TLD and now we have DNSSEC added to that mix. So there's a vulnerability introduced around DNSSEC operations that are going across name servers that are supporting other TLDs.

I don't know that we've seen anything happen - yeah, okay I'm getting a yes we have. And we've certainly seen some issues within TLDs themselves of, you know, of problems where they've taken themselves offline because of DNSSEC update issues and things like that.

((Crosstalk))

Rod Rasmussen: And if you could imagine...

Mikey O'Connor: ...links to any of that we've got a pile of places to put that kind of information. That's extremely valuable.

Rod Rasmussen: Okay.

Mikey O'Connor: And, you know, anybody who's got links to examples of things like that or even theoretical possibilities that people are concerned about we're really interested in that sort of stuff. Sorry to interrupt you. You were onto another point. I just wanted to halt you there.

Rod Rasmussen: No I was done.

Mikey O'Connor: Okay.

Keith Drasek: Hey, Mikey, this is Keith Drasek with VeriSign. I'm here also representing the Registry Stakeholder Group.

Mikey O'Connor: Oh.

Keith Drasek: I just wanted to make a general comment. And not nearly as specific as some of the others that have been made here so far. But I think we - you and we as a group have done a lot of work, a lot of very good work, in terms of sort of the - identifying the scope.

And, you know, we cast a very, very wide net in the very early days and then sort of we went through the process of narrowing it down appropriately. So - and I think what we're hearing and I think what you've said - I'd like to reiterate - is that, you know, we'd be better off having a little bit too much than not enough in terms of the items and the things that we've identified.

And completely agree with your comment about having to, you know, keep our focus to be able to, you know, basically to get the project done and keep it moving and, you know, be responsive to the community. But, you know, if there's ever, you know, sort of that challenge where we have to make a decision I would submit that it's better to include something and maybe go a little too far than not go far enough.

Mikey O'Connor: Yeah that's - I really appreciate that thought, Keith, because I think the thing that we're all trying to do is avoid a situation where we trot out our report at the end and Rod stands up and says well you missed this giant thing; it's really important. That's clearly not our goal.

So at the same time we are a little bit peculiar in that we were chartered by five different ACs and SOs. And so we have to be fairly careful that we don't adventure too far off of the mission that we were given by these groups.

But I think in there is plenty of room to maneuver, plenty of gray area to make sure that we get the right stuff in. And if nothing else we get it in there as such a way as a reminder to the next group that hey here's a huge issue that we just didn't feel was appropriate for our gang.

Keith Drasek: Yeah, agreed, Mikey. This is Keith again for the scribes. Yeah and I think that if we ever find ourselves in that situation or as we probably will where we've got something that we're including that may have been a little bit beyond the strict reading of the scope is that we simply acknowledge that in the report or in the documentation and say, you know, we've, you know, this is, you know, we recognize that this, you know, may have been a bit out of the scope but

here is why we're including it. You know, sort of just make that acknowledgment.

Mikey O'Connor: Yeah that's a good idea too. I see a person named SOW with their hand raised in the chat room. Are you on the call as well? I don't know. SOW also asked the question what can we do to become a member of this group. And this is a group that was chartered by five ACs and SOs and so each of those groups picked membership for the group.

And the one caveat to that is that we are keeping an eye out for folks with expertise such as the external DNS providers and so on. So depending on where you come from and what your expertise is probably the best way to do this is to work through your respective AC or SO because there is a certain amount of turnover in the group. And then if you don't fall in any of those silos send me or any of the co chairs a note and we'll take it up in our co chair group.

Andrew is going crazy in the chat. Oh good there's...

((Crosstalk))

Mikey O'Connor: This is good.

Andrew Sullivan: Sorry that was just some background stuff and I didn't want to talk.

((Crosstalk))

Mikey O'Connor: Yeah, no I get that. And, you know, for those of you who don't want to talk but have ideas and links this is a great use of the chat. We transcribe the chat and, you know, treat it just like spoken stuff. And especially links and reasoned arguments like Andrew is doing is fair game; feel free to bang away in the chat. And then if you actually have a question that you want to put to the group just capitalize that somewhere in there so that I see it.

Anything else in the room, Julie?

Julie Hedlund: I'm not seeing any other questions in the room, Mikey.

Mikey O'Connor: Okay. I think at this point we'll very - we're running a little over on my half-
                 hour schedule but let me very briefly update the group. And Jörg was in the
                 meeting as well can - and anybody else, Julie, Jim Galvin, anybody else who
                 was there.

                 We met with the SSRRT Affirmation of Commitments Review Team this
                 morning because they're working on security and stability as well. And the
                 question becomes, you know, are you competing with each other? Are you
                 duplicating each other's work? How can you collaborate better, etcetera,
                 etcetera.

                 And so we - the two groups set up a meeting for ourselves this morning to
                 just check in and make sure that we weren't stepping on each other's work or
                 reinventing the wheel.

                 Had a pretty productive meeting. I think that the three topics that came
                 through for me, transcribing them at 3:00 am in the morning my time, were
                 that the clients of the two projects are slightly different. The client or the
                 customer of the SSRRT is a much more - a much broader managerial kind of
                 client.

                 The SSRRT is really doing I think sort of a managerial review of security and
                 stability across ICANN. And so their scope is very broad, very managerial in
                 focus. And the expectation is that they are going to make recommendations,
                 managerial recommendations, to ICANN as a result of their work.

                 Our scope is very narrow by comparison. We are looking at threats and
                 vulnerabilities to the DNS, pick your definition of the DNS, with the goal of

really understanding what's going on in a very deep way. But we are not doing anything in terms of that much broader managerial topic at this time.

In our charter the way our work is described is we are supposed to conduct a very deep analysis and if we find gaps we are encouraged to identify ideas to fill those gaps. But it's not in any way conflicting with the SSRRT work.

They are the ones that are really charged with the job of making managerial recommendations to ICANN as to the future handling of this kind of stuff. And our goal is really much narrower than theirs.

Our timing is also different than theirs in that we're in a - be at our work considerably longer than the target dates for the SSRRT which I think SSRRT is supposed to be done at the next meeting in Costa Rica where as we will not for sure.

Another topic that we talked a bit about was the degree to which we need to coordinate and collaborate at sort of a managerial level. And I think that we're going to take a topic amongst the co chairs about that. I think that the message that we want to send to the SSRRT folks is that if they would like a more active liaisons with us we're very open to that.

But they're on a very tight schedule. And I think the sense that I got from Alejandro is we don't have a lot of time to be doing an elaborate coordination with you folks. We're comfortable that what DSSA is doing is not conflicting with what we're doing and may enrich our findings. But we don't' have the cycles to spare to spend a lot of time cross coordinating with you.

So that's sort of the summary of what I heard at the joint meeting. I thought it was a great meeting although I was pretty sleepy and I may have missed some important points there. Anybody in the room want to add to that that was at the meeting?

Jörg Schweiger: Hi, this is Jörg again. Just want to add some comment to make it clearer for the folks around here and I hope I can do so. As far as I understood the SSRRT is more process-focused. And it's a little bit something like a security framework. So if one of you knows ISO 27001 or (Triple O) or they're calling (Bricker) Standards.

So to me it appeared that they are a little bit more on this kind of level working at a security framework according to those standards but transfer to the needs of ICANN. Where the work of the DSSA might fit in very nicely just being a very specific part or a very specific detail that can easily feed in one of their sub-points.

Mikey O'Connor: Yeah, I think that's right. One of the points that Alejandro made was that simply by our existence and by the work that we're doing we're addressing one of the issues that they may raise. And so, you know, there was a pretty high level of comfort with that. Okay anything else about SSRRT? Going once, going twice.

All right I'm going to take a quick process checkpoint because it dawns on me that with folks in the room as engaged as Rod the next chunk of work what I was imaging because when I was setting the agenda up for this I was thinking that this was going to be primarily a working session for the DSSA folks.

But another way to do this as long as folks are in the room and interested is we could do the face to face work with everybody in the room rather than kicking the observers out of the process.

The next piece of work that I was thinking we would do is break into small groups, I don't know, four to seven people, huddle around a piece of paper and a scribe.

Take that one pager - hopefully there are copies of the one page summary in the room - and pick one as sort of the - to give you a sense of the process update while we're fairly close on getting our topics identified and so on there is a pretty strong sense in the group that we need to get on to doing some real analysis here. We are actually chartered to do analysis not to make lists of things to analyze.

And our thought amongst the co chairs was that what we would do is at Dakar we would pick on, not all of them, but pick one that would be a good sort of test case for our analysis.

And when I put this agenda together I was thinking that the DSSA members would be doing that. But I'm not sure that we need to be so exclusionary. And so Jörg and anybody else in the ops team who wants to chime in on this - or anybody in the working group for that matter - what's the sense of people if we just said anybody that's there in the room right now could join this conversation?

Any tremendous objection to that? It seems to me that anybody that's interested enough to show up at this meeting could certainly make a big contribution to the work. And it'd be a lot more interesting than just watching us work.

And then Rossella is raising the question well what about the people on Adobe? And what I thought I would so is break the telephone call off from the room and we would do the same thing on the conference bridge in the Adobe room and then rejoin the room in about - oh I don't know...

Cheryl Langdon-Orr: Mikey?

Mikey O'Connor: Yeah, go ahead.

Cheryl Langdon-Orr: Cheryl talking.

Mikey O'Connor: Yeah, I know.

Cheryl Langdon-Orr: Guess what, darling? This room, the dynamics, the people you've got in the room, the number of people you've got in the room - think of another idea. It's just not...

Mikey O'Connor: Oh bad idea, okay. Well then I'm going to go back to my original plan which is that the DSSA group should huddle in small groups in the room. And apologies to you observers; the next time we schedule this meeting at ICANN we'll make it clearer that this is really a working group session.

You've now sort of lived though the interesting part. You're certainly welcome to stay but I think what we'll do is go back to the original plan which is DSSA members will huddle in small groups to do this priority setting stuff. And the same goes for the folks in the Adobe room and on the phone call.

Folks are welcome to stay and listen but...

Cheryl Langdon-Orr: Okay.

Mikey O'Connor: ...limit to DSSA...

Cheryl Langdon-Orr: Mikey, Mikey?

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: Cheryl here.

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: Just help me with this, will you?

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: You want us to gather together in small groups of a number - it doesn't matter how large or small.

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: Then look at our list that we've all discussed with the community as a whole. And then (severally) pick one to...

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: ...discuss? Or are we going to jointly pick one to discuss in small groups? Because it's two different things and I'm not sure which way we're going at the moment.

Mikey O'Connor: Well you mean I haven't been perfectly clear? Dang.

Cheryl Langdon-Orr: Astonishing as that may be...

Mikey O'Connor: I am shocked.

((Crosstalk))

Cheryl Langdon-Orr: No.

Mikey O'Connor: Gracious. So my thought is this - let me replay that tape in a different way - is that the goal for today - a pretty aggressive goal, by the way, is to pick one topic that we would use as a test case for our analysis work. So let me just scroll the slides down to one of these pages. Hang on a minute.

Cheryl will also now criticize me for mumbling. I mumble when I'm multitasking and Cheryl keeps me honest on that. But what I was thinking is

that if we took the one pager, which I don't have up on the screen, but these topics are on that one pager.

And the goal would be to pick one of these topics, not just from this page but from the whole one pager so all of those four pages - that everybody agrees or at least a lot of people agree is very, very, very important. It's not that anything is going to get left off it's just that rather than do the analysis on everything right away, especially the co chairs think it'd be a good idea if we focused on one to try out how we're going to do analysis.

So the idea for the small groups goes like this. Take the one pager, sit in a small group. Everybody takes a moment to maybe pick their top three then share your respective views about what you think the top three most important things are.

See if there's a trend. And if there is identify the number one most important thing on the one pager. Bring that back to the whole group for a quick discussion at the end of this call. I think I'm going to jettison - I think we're going to do one of these sessions, not two since we're nearly done with the second half hour already.

Julie Hedlund: Yeah, Mikey, Mikey, just I'm sorry to interrupt. This is Julie. But just on that point we do only have 35 minutes left of this session and some of us actually have other sessions we have to go to from this meeting at 12:30. Cheryl wants to speak.

Cheryl Langdon-Orr: Mikey?

Mikey O'Connor: Yes ma'am.

Cheryl Langdon-Orr: Time for me to brutally honest. If you break us up into small groups even I'm leaving.

Mikey O'Connor: Okay fine.

Jörg Schweiger: Mikey, this is Jörg, let me jump in also. I doubt that we are going to get this organized in a straightforward way. But if you really want to take advantage of everybody who is here and being a part of this discussion what I would like to suggest is that we at least get some input not according to analyzing threats but according to the importance of certain points on our list from the audience. Just soliciting what people think what might be the most important one.

And that could really be easy done on the one pager and that could include everybody who's in the room. And just to make it a little bit more conclusionary I would sort of try to do it in a little bit different way so just like everybody has got three points and he can concentrate those three points on any point on the list or he can just spread them as he wants to.

And we're going to get those sheets back and analyze what, according to the people who are currently taking part in this discussion, think it's really the most important thing. And I doubt that we're going to get any further than this in this very meeting.

Mikey O'Connor: I think you're probably right.

Jörg Schweiger: Good plan for you as well?

Mikey O'Connor: Yeah, that's fine. For those of you who are observing you can tell that the co chairs have a pretty robust, pretty collaborative relationship. And Cheryl beats me up all the time.

So taking Jörg's idea, hopefully there are enough copies of the one pager that everybody in the room has got one and can get one.

Julie Hedlund: Yeah, Mikey, this is Julie. I did - we did circulate them at the beginning and I just went around and waved them - we do have extra copies. Everybody assured me that they have one if they want one.

Mikey O'Connor: Okay so here's out it works; scribble your name and email address on the top of your one pager. And as Jörg said you get three votes; you get to vote for - and you get to distribute those votes against that one pager either putting all your votes one thing or spreading them across three.

Cheryl Langdon-Orr: Mikey...

Mikey O'Connor: Yes, ma'am.

((Crosstalk))

Cheryl Langdon-Orr: We - just let us do it...

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: ...without distributing votes and...

Mikey O'Connor: Oh okay well I was just, you know, trying to back up my co chair there; that's what he said to do. I was just, you know, trying to hang in there. You want to just talk?

Jörg Schweiger: No I thought I was clear with me suggestion. I think Cheryl just reacted on your - asking everybody to put his name on the sheet. And I was content myself to write up on it .xxx or something.

Mikey O'Connor: Oh dear.

Jörg Schweiger: Feel free to just take your favorite three.

Mikey O'Connor: Anonymously if you want.

Jörg Schweiger: So, Mikey, just to inform you the process is just taking place.

Mikey O'Connor: Oh good, okay.

Julie Hedlund: Yes I was going to say the silence that you're hearing is people diligently doing their jobs. And I would remind everyone not to cheat off your neighbor.

Mikey O'Connor: Yes.

((Crosstalk))

Julie Hedlund: And be sure to send your papers to the front of the class.

Mikey O'Connor: And the proctors will be checking. And those of you who are on the call this is homework because there's no way that I can figure out how to do this on the call. But everybody gets to contribute their votes; you can do it by email. So if you want to take a moment and break off.

                   And maybe that's the thing to do given the fact that it's the top of the hour right now. So I'll go back to Jörg; so Jörg are you thinking that maybe we then tally these yet today in the meeting or do we just collect them and tally them later?

Jörg Schweiger: Mikey, I can hardly understand you. I heard you've been addressing me but there's so much battling going on I'll just write it down in the chat.

Julie Hedlund: Sorry, Cheryl.

Mikey O'Connor: Let me do it in the chat.

Julie Hedlund: Yeah so just for clarification for those on the phone we are trying to do a little bit of prioritization here looking at just the threats. So for those of you looking at the one pager skip the vulnerability side and look at the threat side. And this is to help us to prioritize where to start.

Jörg Schweiger: Just another brief hint to the audience in the room I hope that I would not see too many votes for the red ones.

((Crosstalk))

Mikey O'Connor: Yeah.

((Crosstalk))

Julie Hedlund: So for those on the phone and Mikey we did get a nice collection of the one pagers with priorities or the sort of the top three indicated depending on how people did that. And I was wondering how you might want to proceed at this point although we'll need a little bit of time to tally these. And that might have to really take place after this meeting because I don't think we really have time to get them tallied up and so on right now.

                   So what did you envision was the next step, Mikey?

Mikey O'Connor: This implies that I am envisioning. We're making this up as we go. I think if there's - sometime when you look at those kinds of sheets there's sort of an overwhelming trend that you can just see by flipping through them. And if there is such a trend it would be nice to just flip through them really quick, don't actually do all the arithmetic and tally them up, but just see if there are one or two topics that seem to get a whole lot of attention from folks.

                   I think it's useful for people in the room just to get a sense of what their feedback was. If there isn't any trend like that then I think Jörg's suggestion in

the chat is probably right which is we should probably just wrap the meeting up, let people get onto the next thing.

So I'll leave it to those of you who can actually see the sheets to see if there's kind of an overwhelming clustering around one or two topics that people would like to hear about. And then if not we'll call it a day.

Rod Rasmussen: So, Mikey, this is Rod. While they're busy tallying I'm going to grab the mic and ask a question. Is that looking carefully at that sheet there was something on there that kind of stuck out at me as being very odd and that was the spam category.

Is that something very specific or - I'm - since we're waiting we could fill the space with actually - we might be able to illuminate what that is.

Mikey O'Connor: I am just going to have to - this implies that I actually have the one sheeter. Oh look at that. Have to go look at the sheet because I can't really remember what we had on there.

Rod Rasmussen: And all the sheets are now in the possession of the...

Mikey O'Connor: Yeah.

Rod Rasmussen: ...people at the head of the table so I can't look at it either.

((Crosstalk))

Mikey O'Connor: ...the actual document so I think that what we were...

Julie Hedlund: And so, Mikey, this is Julie. Jörg and I were just kind of glancing through the sheets. With just a quick look it's very hard to identify a trend. I mean, we might be able to see one if we could break the items out and kind of see in a way like how many votes each one got, you know, how many people picked -

because not everybody prioritized, some people just circled three, some people did 1, 2, 3 so we don't have...

Mikey O'Connor: Yeah.

Julie Hedlund: ...the exact same methodology for making the choices. So just at a glance the final...

Mikey O'Connor: Okay.

Julie Hedlund: ...point is that it - hard to say at this point.

Mikey O'Connor: All right. So which spam one - oh in scope email spam on the one pager. That's the - let me take you to the slide - that's the one where as IPv6 comes in spammers may start suddenly hopping across a lot of IPv6 addresses and causing a lot of load on DNS as a result.

Rod Rasmussen: Got it, thanks.

Mikey O'Connor: I'm quickly running out of gas. This is, you know, if John Levine was on the call or in the room I'd throw the ball to him at this point.

Rod Rasmussen: No I understand. Thanks.

Julie Hedlund: And, Mikey, that email - the last spam one was only picked by one person out of...

Mikey O'Connor: Yeah.

Julie Hedlund: ...20-some that we have.

Mikey O'Connor: Oh I'm sure that Rod's question is the what in the heck are you talking about question and so. Okay well thanks all for a lively and somewhat fluid meeting.

I think this accomplished a lot of what I was hoping to accomplish anyway even though it turned out a little different than what I was planning.

And I think at this point I'll sort of step back and let Julie and Jörg wrap the meeting up and send you on your way. And I'll see the rest of you DSSA folks in a couple of weeks.

Cheryl Langdon-Orr: Yes, thank you, Mikey.

((Crosstalk))

Cheryl Langdon-Orr: Cheryl here for the transcript record. The amount of work you've put in prepping this work group for this meeting and indeed inter-sessionaly and at all the meetings I think should be noted at these rather formal gatherings of the ICANN meeting where the work group gets together. You are a chairman extraordinaire despite the fact that I will take advantage of you whenever I possibly can. But we know each other well enough there.

You are a hero; you're certainly my hero and this work group wouldn't be where it is today without you so I just wanted to have on the formal record my personal thanks. And I suspect that of many around the table if not all.

Mikey O'Connor: Well I also have to echo back that I think that this working group has an extraordinary group of people in it that, you know, Churchill's phrase is the one that comes to mind which is I'm not the lion; I just get to give the roar. This is a very hard working group that's produced an enormous body of work and that blame or credit should be shared very broadly. So thanks for the kind words, Cheryl, but back on you on that one.

Edmon Chung: Yeah, this is Edmon. I - before we close I just wanted to bring sort of an information into this. At the ALAC we had some discussion about what's in scope, out scope. I just want to bring it back. I guess Olivier or Cheryl can add to that or correct me.

But we felt that - at lest the ALAC felt that the business failure should be in scope. So this might be one of the things that we want to talk about later, not in this session but - I don't know if Olivier or - want to add.

Mikey O'Connor: Perfect that's great because that's one of the ones that's still under discussion and it's great to get that feedback. I think the, you know, Olivier and Cheryl weren't in the room when I called to that so it's really helpful that you came back to that, Edmon, thanks.

Olivier Crépin-LeBlond: Mikey, Olivier here. Actually what we will do is we will go over the transcript of our sessions. Much was discussed and what we will do is to summarize and feed into this working group with our findings from the transcripts.

Mikey O'Connor: Oh great; that's even better.

Julie Hedlund: Is there anybody else in the room who would like to make a comment or have a question? Then I think that we're complete here. I want to thank everybody for attending this session today. And there will indeed be a transcript on this meeting. It will be posted on the site and we'll send it around to the work group when it's available. And there also has been a recording made.

And I have captured the votes on the threats and I will try to transcribe them in some way and send them around to the work group. Anything else you want to add, Mikey?

Mikey O'Connor: Nope that's it for me. Thanks all. See you all soon.

Julie Hedlund: Thanks to you too. Bye-bye.

Mikey O'Connor: Bye-bye.

Julie Hedlund: This session is - oh, yes? No, okay, this session is adjourned.

END