ICANN Prague Meeting
DSSA Meeting - TRANSCRIPTION
Thursday 28th June 2012 at 09:00 local time

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.

Julie Hedlund: Good morning, everyone. This is the DNS Security and Stability Analysis Working Group Meeting. And please may we ask you to finish up your conversations and come on and take a seat so that we can start shortly. Thank you.

Okay, good morning, everyone. We are - for recording purposes, I do want to let everyone know that this meeting is being recorded. So when you do speak, please do state your name and use a microphone.

This is the DNS Security and Stability Analysis Working Group Meeting on today, June 28, 2012. And this is a public meeting, and we will just go ahead and get started here. And I think I shall just turn things over to Mikey O'Connor, who is one of the co-chairs of the group.

Mikey O'Connor: Thanks, Julie. Welcome, everybody. It's so weird to actually be able to see people's faces. The DSSA's been meeting for a couple of years. We do it all online. We do great tricks with Adobe rooms, and it's like sensory overload to be here and being able to see people's faces.

Today's agenda is pretty simple. We're going to step through the report basically, taking pauses along the way to get anybody's feedback or input or ideas. Normally we do a whole ritual of checking in on statements of interest. I think we'll skip that for today.

But, you know, we've got enough time. We've got an hour and a half. Why don't we just really quickly go around the room and introduce ourselves, partly because so many of us have worked online together and have no idea what we look like.

And so it'd be kind of a fun thing to see faces and names going together. So I'm going to go all the way down to the end and let Bill Manning kick us off with this.

Bill Manning: Hello. Bill Manning. I work for Booz Allen Hamilton, and contract work for Department of Defense.

(Mona Karen): Hi. I'm (Mona Karen). I'm a journalist.

David Cake: David Cake, NCUC chair, with Electronic Frontiers Australia. I was a member of the SSR Review Team.

Jay Daly: Hi. Jay Daly. I'm the chief executive of the .nz registry.

Cheryl Langdon-Orr: Good morning, all. My name's Cheryl Langdon-Orr, and I actually have a role here at the DSSA representing the at-large advisory committee, which in turn is the Internet end-user registrant, and that's who I get to be.

(Kenny Dernine): Hello. (Kenny Dernine), and I'm from (Ireland) (DNS).

Julie Hammer: Julie Hammer. I'm from .au domain administration, and I'm a member of the DSSA working group, too.

Cristian Hesselman: I am Cristian Hesselman. I'm the research manager of SIDN, the .nl registry.

Jeff Moss: Jeff Moss, chief security officer, ICANN.

Patrick Jones: Patrick Jones, ICANN staff and working with the DSSA group since the inception, and also with the SSR-RT.

Simon McCalla: Simon McCalla, Nominet, and formerly of the SR review team.

Jacques Latour: Jacques Latour with CIRA.

Warren Kumari: Warren Kumari with Google, and I've been part of the DSSA only since the last meeting in Costa Rica.

Don Blumenthal: Don Blumenthal, public interest registry, part of this from the beginning.

Man: (Paul) (Unintelligible), and also from (Netnog).

Mikey O'Connor: I'm Mikey O'Connor, co-chair of the DSSA, representing the GNSO, and in charge of jokes. I couldn't find an egg picture, but I do have an important update on the eggs once we get back around. So I'll get back to that.

Julie Hedlund: Julie Hedlund, ICANN staff and support for the DSSA working group.

Jörg Schweiger: Jörg Schweiger with DENIC, and co-chairing for the ccNSO.

Man: (Unintelligible), ICANN staff, and I work on the security team with Jeff Moss.

Suzanne Woolf: Suzanne Wolf, ISC and RSAC, and a couple of other hats, ICANN Board.

Jim Galvin: Hi. I'm the real Mikey O'Connor. No, I'm Jim Galvin, vice-chair of SSAC and also with affiliates.

Katrina Sataki: Good morning. Katrina Sataki, NIC.LV, member of the SSA.

(Vila): My name is (Vila) from Rwanda ICT Association, the RW Common Registry.

Douglas Maughan: Douglas Maughan, Department of Homeland Security and member of SSAC.

Wendy Seltzer: Wendy Seltzer, member of the non-commercial stakeholders group and GNSO Council, and an observer here.

Man: (Unintelligible), technical liaison to the ICANN Board, intrigued reader of reports.

Keith Drazek: Good morning. I'm Keith Drazek, VeriSign, alternate chair of the registry stakeholder group and the GNSO, and member of the working group.

Mark Seiden: I'm Mark Seiden. I'm a consultant and member of SSAC.

Mikey O'Connor: Do we have the roving mic available? I'd just like to bring in the folks on the side here, too. Oh, and the esteemed Mr. Graham.

Bill Graham: The late Mr. Graham.

((Crosstalk))

Mikey O'Connor: You want to introduce yourself?

Woman: And yet you look so healthy.

Man: (Unintelligible).

Man: Thank you.

Woman: (Unintelligible).

Man: (Unintelligible). Thank you.

Mikey O'Connor: I'm trying to follow the late Bill Graham but, you know, he moves awfully fast. It's like to co-chair following the audience around the room. You want to introduce yourself for the transcript? The late Bill Graham?

Bill Graham: It's Bill Graham.

Mikey O'Connor: Member of the Board and also chair, (unintelligible) board, committee (unintelligible). Thank you, sir.

Man: (Unintelligible) with AT&T.

Mikey O'Connor: And good friend. Okay, this is cool. I hadn't thought about it, and this is like those television shows where the host goes out into the audience. Who's the guy that did - there was some famous TV show guy that did that.

Man: (Unintelligible).

Mikey O'Connor: No.

Man: (Unintelligible).

Mikey O'Connor: Okay, so I think what we're going to do is churn through a bunch of slides in little chunks, and then stop. If we go through all these slides, you'll all be face down in laptops in front of you snoring. So we'll break this up a bit so that you can wake up and talk, and beat me up for things that are wrong, and so on and so forth.

Just sort of a personal note, this is an extraordinary group. And working with this group of people is so much fun it ought to be illegal. And so if you detect a certain kind of lightheartedness to the conversation, you have to realize that in a way this is the celebration of two hard years of work by an extraordinary group of people.

It works incredibly well together, and I include of course Julie Hedlund there, from Minnesota, because she's been a big part of the staff support. And of course Mr. Patrick over there, too.

The kind of traditional tensions in ICANN work don't exist in this working group. And one of the things that you who are sort of observing us should realize is that it's just fine to get pretty aggressive with your comments.

We are pretty frisky on these calls. And none of this is done. So if there's something in here that's wrong or that you think needs to change, don't be shy. Because we're not. And with that, I think we'll carry on.

Does anybody on the Adobe room - can somebody in the Adobe room sort of pound into the chat whether the audio is all working fine? Probably can't, because they wouldn't be able to hear us. So, Julie, could you - yeah. Could you pound something into the chat to ask them whether or not it's working again? Because we've had a little bumpy weather on audio this week.

Okay, off we go. Very quickly, we, over the last couple of years, have done five pretty big things. We're a cross-constituency working group, and that's a pretty unusual critter for ICANN. Usually we sit in our silos and we all know how to work in our silos.

And this group is comprised of five major silos -- the SSAC; the GAC, although we're having a little trouble figuring out how GAC people can participate; the GNSO; the ccNSO; and the at-large constituency.

And so that first bullet, it looks pretty trivial, but in fact it's kind of complicated getting five different working group methodologies to mesh. We worked a pretty good time on clarifying the scope of what we were doing.

I think it's safe to say that this is an airplane we built while we were flying it. And sometimes we find that we have five or six extra wings and no wheels, and for the most part we've got that ironed out. But that's not necessarily all done.

One of the things that we anticipated we needed was the ability to handle confidential information in a secure way. I'm actually quite delighted to say that we have so far, because that confidential information is pretty complicated stuff. But we have built a pretty good protocol for handling it, which might be a tool that other people can use in other constituencies.

In fact, we built a lot of tools in this working group that, for the most part, are out on the wiki page, and free for any and all to use.

We didn't know we had to do this, but we discovered that we needed to build a risk-assessment framework, and we'll take you through that as we go. And we built the first set of risk scenarios, and I want to make a very important distinction between a risk scenario -- which is essentially something that we, the working group, want to look more at; as opposed to risks.

Because those words can be misinterpreted, and we are not - when we get to those scenarios, some of them are kind of scary. We're not saying that those are risks. We're saying that we want to look at those.

What we're going to do, we think -- although we're open to conversation about this -- is we think we're going to finish that risk assessment; refine our methodology -- we've got some pretty cool methodology already, but we think we can make it a lot better -- and start taking the framework and the methodology and the conversations out to a broader audience.

The transitional moment that we're in right now is when we went to the meeting in Costa Rica, we asked our respective ACs and SOs, "Well, you want us to go really fast? Or do you want us to go really deep in our work?" And the ACs and SOs came back and said, "Yes, please."

And so this is the end of the go-fast part. And then it's also the beginning of the go-deep part. So this is essentially the work plan for going deep. It's simple in that it's a short list, but it's going to be complicated because these are big issues and there's lots of information to be collected.

That's kind of where we are and where we're going. The first thing that we had to do when we were building our airplane while we were flying it was to work both with the SSR-RT -- and Alejandro just walked in. That's cool. Welcome.

And also with the Board DNS risk management framework working group, we talked a lot about the scope boundaries between us and the SSR-RT a couple of meetings ago. So that particular picture's missing.

The one that's up on the screen is the one that we used to describe our thinking about where we fit, compared to what we think the DNRMF is doing. But of course we may have this all wrong. We know one thing for sure, and that is that we are only doing risk assessment.

And what's up on the screen is kind of a textbook picture of risk management, as opposed to risk assessment. Risk assessment is a subset of risk management, and let's see if my cool animation works. Oh, it worked. There's where we fit.

We're working on risk assessment. But after you assess the risks, you have to figure out what you're going to do about them. Some risks you may say, "Well we're going to accept that risk. It's pretty unlikely. It's not going to have a whole lot of impact. Not going to be a very big deal."

Other risks, we may want to transfer that risk for someone else. That's what I always try to do, you know? Hey, I didn't do it. It wasn't my fault. Sometimes you want to buy insurance. There are all kinds of strategies and techniques that people use to manage the risk, and that usually falls in sort of a jar called risk planning or mitigation, or something like that.

Then you go out and do those things. And the last chunk of a risk management framework is usually to collect information about how well your mitigation efforts worked. And then you cycle it back into the next round of the risk assessment, et cetera.

So our scope -- at least we think -- our scope is the first bit, but not the second two bits. And we can circle back. That's part of the reason I wanted to take this in chunks. We might want to have a bit of a chat about that.

Another way to think about scope emerged later in the conversation. And so this picture came out. And actually I stole this idea from the late Bill Graham. If you think about any endeavor, whether it's SSR or anything else, there are often things that happen at the core where that's - you know, one way to think about that is steering.

And there are other things that happen at the edge. And that is sometimes thought of as rowing. The work gets done at the edge. That's where people pick up the tools and deal with the problems and get through the day.

And in the middle, often there is sort of glue-ish type layers. In an ICANN context, it's often thought of as the constituency SO/AC kind of things. This is where the communication takes place between the core and the edge.

And from our DSSA standpoint, we think of ourselves as in that collaborative core. You know, this is a very cross-cutting, cross-silo type group. And the other way to think of things is the spokes around this wheel. And again we're sort of re-emphasizing this idea of risk assessment.

But as you work your way counterclockwise, then you'll see that the next chunk is risk planning. That's straight off the chart you just saw. Then we started to realize that there are other things to do in terms of standards, tools and techniques.

And we in the DSSA have created some pretty interesting tools that are available at no charge on our Web site, today and today only. They're downloadable. Some of them are spreadsheets that are pretty neat. I may download one and show it to you later, if we have time.

And then sort of directly opposite us on that chart is the people who actually are on the front lines dealing with risks every day; mitigating the risks; coping with whatever the issues are; having the experiences.

And another piece to this puzzle then below them is the education/training/awareness tools that they need and that the broader community needs in order to be aware of these risks and so on. And then at the very bottom of the chart again is monitoring.

So the stuff on sort of the rust side of that chart is the same as this preceding slide. And the stuff on the left side of the chart, we realized is another important piece of all this. And that the whole picture - this may not even have enough spokes.

But these were the things that we came up with fairly late in our conversation. And it's really an eye chart on the screen. I'm eating my own cooking here, realizing that the fonts are a little bit too small. But the (unintelligible) over on the left side is a very preliminary list of all of the people we thought up in one phone call that have a role to play on this chart.

This is clearly not a chart that just talks to ICANN. You know, there are certainly ICANN participants back in registry providers, the constituencies and so on. But first -- and IATF and ISOC and the NRO and RSAC and SSAC and the SSR-RT and, you know, the (NSOR) -- there are all sorts of people who have a stake in the game and a role to play when it comes to our charter, which is taking a look at the security and stability of the DNS at the root and TLD level.

And so we came up with this list, and then Julie Hammer just kind of casually said on the call, "Well, Mikey, why don't you put those people on this chart? Just place them on the chart?"

And I, like an idiot, ran off and said, "Sure, I'll do that," and absolutely hit a brick wall, because I don't really know those organizations well enough to know where they would place themselves on that chart -- what roles they would like to play. What roles they would not like to play.

And so I think one of the things that we may do in the next chunk of the work is go out and ask them, and see where they would envision themselves on that chart. And I think one of the important outcomes of that is likely to be a chart that has gaps and overlaps. And the overlaps are less concerning than the gaps. And so expect to see something going on in that area as we move forward.

But I mostly dwell on this just to give you a sense of how big this ecosystem is, and how many participants there are, and how many different roles there are for people to play.

And I think that one of the things that's really extraordinary about the DSSA group is that we have quite a lot of coverage already just from within the DSSA. And it's been a wonderful experience to sort of hear what people have to say in conversations and debates around this.

I think I'm going to stop here. This is sort of one of those big break points. Partly to let you wake up. Partly to let you tell us what you think. Tell us where we're going right. Where we're going wrong. Because the next chunk is actually to explore the methodology that we built. So that's a big topic change.

So I'll pause at this point and let people throw in their ideas, comments, suggestions, course corrections, ideas for what we ought to do in the future, et cetera, et cetera. Any thoughts?

For those of you who are not in the room and can't see what's going on, there are now roughly 40 faces splashed down into their notebooks, snoring after this scintillating presentation that I gave so far.

Cheryl Langdon-Orr: Thank you, Mikey. And because this is recorded and transcripted, it is Cheryl Langdon-Orr for the transcript record. I obviously don't have a question, because I've kind of been involved in this from the start. But I'd like to actually pose a question to those who are observers or involved in the other parts of this security and stability ecosystem space that we're in at the moment.

Is how we are presenting our work - which is we're trying to be very graphic. We're trying to not be too technobabble. We're trying to be something that, as many of us are doing, carrying around a one-page piece of paper which you can pull out of our back pocket and say, "This is what it means."

Have we hit the mark there? So if you don't have questions for us, we certainly have questions for you. And I'd like that one answered, Bill.

Bill Graham: Bill Graham for the transcript. I think this graphic presentation quite useful. The thing about the DNS risk management framework working group is that we're not - and I'll make this clear when we get to the next session. But we're not actually doing, developing, the frameworks so much.

What we're doing is ensuring that it gets done, and that it's incorporated into staff functions. So I think this work will be extremely valuable in that other trail work that's going on now. And I think for a non-techie such as myself, this kind of graphic presentation is certainly thought-provoking.

Mikey O'Connor: Thanks, Bill. Alejandro, go ahead. This is Alejandro Pisanty, the chair of the SSR-RT, just coming in now.

Alejandro Pisanty: Good morning, everybody. First, since there's a record, I would like to disassociate myself from your statement that said the late Bill Graham.

Woman: (Unintelligible).

Alejandro Pisanty: He is in here. He has already spoken. And he was here. I'd also like to commend the work that you have done. As a close witness from the SSR, I can say that for the SSR-RT, the stability, security and resiliency review team, it was first a potential tension which we perceived between the possible mandates of our two groups and the way they were structured.

But I think this was resolved very early, very well. And that this was very, very true to get the picture here, or else as soon as we know that this was not only a part of (unintelligible), but even the broad community effort.

But those (unintelligible) focused on a very specific task with great - I mean with great promise for results you have shown already that we are getting there. It was very useful, actually, to not have to concentrate at all on the details of the risk assessment, because it was being done.

We are recommending highly in our report that has just been delivered a week ago because it's now official and final, we're recommending highly the work that you are doing.

We believe that the way forward includes the DSSA work in many important ways, as a part - again, as a contribution to the most important task that we believe emerges from our recommendations, which is for ICANN, through the working group that Bill Graham chairs on the Board that ICANN established risk management framework for the (BMS) further to that recommendation and again, I say this to commend and support the work that you are doing there however we're able to contribute to it.

And that risk framework has to be done fast. It has to be done in a way that is both comprehensive and pragmatic and the contents, we mean that it doesn't have to be exhaustive before it's published.

We're recommending that ICANN get a (third chop) at that comprehensive risk framework and put it forward and start working upon it. We seem to agree that that timeframe will take us through early 2013, in the next six months or next six to nine months.

But we're at the most important of our recommendations. I believe it that (unintelligible). And as I said, I think that one way for the community to contribute is to support and correct (and add) or correct it if they think there's something amiss in that framework.

Mikey O'Connor: Thanks Alejandro. I just want to take sort of a personal moment. It has been an amazing experience to work with the DSSA. It has also been an amazing experience to meet and work with Alejandro. He and I have spent a lot of time together coordinating the work of our two groups and as I said earlier, this has been so much fun it probably ought to be illegal. So hat off to Alejandro and everybody on the SSRT for a fabulous job.

And it couldn't have been easier or more productive when we were sorting out who was going to do what working with Alejandro on that. Anything else in this chunk before we go on to the next chunk. Oh, a couple of people. Let's see, we'll go down sort of this side. Go ahead (Jeff). Go ahead.

(Jeff): For the record, (unintelligible). Thank you for the comments about SSRT. That's very kind. The thoughts as I was looking at this is I think there is I think - I commend this approach and I think it's really important everything that you do adds real clarity to the DSSA working group's doing particularly now we have an SSR RT report out in the wild.

And to a certain extent we have the security team now also asking for feedback on some of those recommendations. There's a danger that the community at large gets a little confused about what its commenting on and which of it is doing which.

And I think trying to provide some real clarity about whether there's clear air between what the DSSA is doing but also whether there is a clear overlap and particularly on risk management framework which we've made a big deal of in the (back). I think it's really important.

So whatever you did to even create that clarity to the community, it's great. I understand. I'm commenting over there on the security team or I'm seeing the recommendations in SSR or I'm seeing the great work the DSSA is doing. That's going to be really helpful too. Anything you can do I think this is a great start - would be really useful.

Mikey O'Connor: Let me jump over to Patrick. He sort of went up electrified and then I'll come back to you if that's okay. Okay, Patrick.

Patrick Jones: This is Patrick Jones from ICANN staff. Building on what (Simon) said, you know, I was looking at Recommendation 25, 26, 27 from the review team's report. And in looking at this chart, I think this is helpful for us in implementing those recommendations, so having something that's clear that we can point to that's not developed by staff but is from the community is useful.

Mikey O'Connor: Thanks Patrick. I am going to take an editorial note that this is something that I - this may be my only complaint in this meeting. And that is that I think we at ICANN as a community underutilize, underappreciate the role of the staff, the ICANN staff.

And certainly in the DSSA, we don't make a distinction between the opinions of the staff and the members of the group because clearly Patrick and (Julie) and all the others bring a lot and have many fingerprints on this document. And so I just want to take a moment to give you guys an atta-boy and I promise that I will not speak in Minnesota until the microphone's turned off, okay?

(Julie) and I share a heritage of coming from the same hometown. And boy, I tell you what, well, there goes the promise. When we get going into the local accent, you just have to watch out. Okay, (Jacques). Oh, I thought you had a hand up. Anything else? Anybody else?

Man: May I Mikey?

Mikey O'Connor: Certainly. Who's saying may I?

Man: This is (unintelligible) for the record. Well, let me just to present to you what we've been doing with the risk analysis management framework and this is just another part of a method we came up with. And the comments we've heard so far, they all sound like (kind of) vanilla and I just want to start up a conversation with you where there are really some (critic) comments as well so at least I received some critics about what we've been doing and I'd ask that we are all about process and that the community was (expecting) more analysis as itself.

So this is a group that says we are analyzing certain risks so this is what we're supposed to do and I just want to hear your feedback. Are we on the right track? Because we did so much process work. Are you expecting some (group) or us to go on with this work to really dive down deep and analyze? Or what is your perceived perception of how this is going to go on?

Mikey O'Connor: And that's a question to the group not to me, right? Right. So if anybody has thoughts about that, either now or on kind of pushing later, we are really interested in that. I think that, at least for me, this week has been a series of conversations about where are we now? What have we produced? How good is the result so far? Where do you want us to go? And certainly another sort of piece of inside baseball, is that the DSSA meets twice a week.

One a week, the whole group meets, but once a week, the leadership group meets which is Patrick and (Julie) and (Bart) and all the staff folks plus the five co-chairs, four co-chairs. And I know that we're going to have some conversations soon in the co-chair group about this and then we'll bring it out to the full group.

You know, how many of these are we going to analyze? How deep are we going to analyze them? How broadly are we going to engage the rest of the community? What sequence are we going to do that in? A whole lot of conversation about that.

I think it is important to highlight that this is pretty fluid still. This is still - we are still building the airplane and lots of room to maneuver. Dave, go ahead.

Dave Piscitello: I don't know exactly where you should go from here but I guess I do have an opinion about what the outcome, what a really positive outcome would be. And you know, part of trying to wrap your hands around this elephant is that people tend to focus at the top of the (pin) because it seems a little bit more manageable and I think that to really cut this off is actually very good.

So - but it would be really helpful if what the outcome would say is the (top) here is in pretty good shape because personally I think it is. It - but now that we've told you the top is in really good shape, could you please leave us alone and go fix the bottom, because so much of the badness is actually well below what you're focusing on.

And so I think that would be a very, very important conclusion to take certain (advice of) committees, and SOs and have them start to look at, you know, other systemic problems that have to do with how things are administered well below where you are, you know, all the way to the client and the (stub). Thank you. I'm sorry, for the record, it's Dave Piscitello from ICANN.

Mikey O'Connor: Yes, one of the things to - let me see if I can do this in one try. We - what you're seeing on the screen now is a mind map that we build as we were trying to figure out what was in and out of our scope because our charter says take a look at this stuff at the root and the TLD level only.

And so the reason that we're stopping where we're stopping, Dave, is because that's what we were chartered to do and so we very conscientiously drew the line there. And I think you're absolutely right. One of the things that I think will be useful is that the methods that we're developing and the tools that we're developing are quite (expensable) and modifiable and could be very easily tailored to take it out to those other places.

And one of the things that would be useful about knowing who is where on that, on this chart, is generally we would have essentially a way to reach people and let them know that these tools are out there and available and begin expanding that conversation outward from the root and the TLD level. But I think that's a really helpful thought. Oh sorry, go ahead (Bill).

(Bill): The response to the question what else either this group or some other group should do, I'll just respond generally and that is if this work isn't used in some way going forward, then it was a complete waste of time and I hate for good people to waste their time doing things, so either you should or some other group needs to be spun up to make use of the process and procedures you've put in place to ensure that something happens and I would argue that it needs to be done on a continual ongoing basis, that we don't just look at it once and say oh good, we're done. No more problems.

Mikey O'Connor: That's another really interesting part of the scope discussion. We are chartered as a project. We have a beginning, a middle and an end and then beer. One of the things that is clear and I can't agree with (Bill) more is that this is something that needs to go on after we're done.

And I think that's the beginning of the segue into the work that the board committee is doing to a certain extent because the board committee's charge is to establish an ongoing thing. And I think some of the work that we've done here can see right into that.

And again, another great working relationship is between us and (Bill Graham), the chair of that committee. You know, I think that there is very little conflict on that front either and I think we pretty strongly agree on the point that you just made, (Bill). But it is clear that beer is coming and we are not going to be an ongoing group.

Many of us may want to participate in an ongoing group. Certainly I'd be interested in doing that, but I don't like turning projects into functions because projects are managed one way and functions are managed a completely different way. And if you try and turn one into the other without thinking about it, you can wind up with some very peculiar problems. Okay, anybody else? Oh, go ahead.

Jeff Brueggeman: Hi, Jeff Brueggeman. Mikey, a question is something we wrestle with in the review team is - and I think you touch on it on the slide, is not only kind of what is the role of the DSSA but kind of what is ICANN's role in the overall obviously very broad set of DNS risks. And I think yours slide is (hinting) to that on the left in that how much are you thinking about that and framing that as well, because I think these sets of visuals are helpful on those types of issues as well.

Mikey O’Connor: Thanks Jeff. I actually stole some of these graphics and wrote a response for Patrick’s request for comment on the ICANN role and remit and actually editorialized quite a bit on that more from the ISP constituency vantage point. But the graphics were very helpful and the thinking in this group was very helpful in terms of framing that response.

And so if you go out to the public comment area for Patrick’s role and remit, then it’s a pretty sparse response so far so maybe I’ll put in an advertisement for Patrick to get the rest of you to start commenting on that. And my comment might get you pretty excited. You might want to put up your fists and beat me up on that one. Patrick, you want to jump in?

Patrick Jones: Yes, Patrick Jones. Just as an update, the public comment (unintelligible) apparently says that the reply period ends on the 16th of July. Based on our conversations with different communities here at this meeting, I expect that we’ll be announcing shortly an extension of the comment period through the end of August.

There’s no rush to complete the comment period and we really want to encourage a broader, more thorough community from discussion on the SSR role and remit. So I hope that extension of time is helpful.

Mikey O’Connor: That’s terrific. Thanks Jeff. Thanks Patrick. Go ahead (unintelligible).

Man: (Unintelligible). Mikey, it’s a question actually. And my understanding of one of the reasons for the genesis and formation of this group was to answer and perhaps respond to the issue of a need for the establishment of DNS because - and of course, I haven’t read the whole report yet but is that - yes, I know. I’m a bad guy. Is that going to be a question you guys plan to answer?

Mikey O’Connor: No, we’re not actually. Our formation was not that issue specific. You know, the - our charter was really frame primary by Chris Despain of the ccNSO and

Chuck Gnomes of the GNSO and we weren't asked to answer that question, however, the topic comes up periodically. And I think it's - well, I'll go ahead and say what I think we think and then you'll find that the DSSA is not shy about throwing their boots at me if I get it wrong.

We're not pursuing that topic very much. What we're focusing on is what are the risks? We're doing the risk assessment. In our charter we have we have sort of a backdoor that says if you find any gaps in the response to the risks, and you want to suggest some ideas about things to do, you can do that if you want to, but the charter is not terribly enthusiastic about having us come up with ideas like that.

You know, we have a little legalistic doorway that we can walk through but we are certainly not pursuing, you know, in a way the cert was sort of a solution looking for a problem to solve in a way. We're coming at it from the other direction and saying, you know, we're assessing the risks and we're pretty much going to stop there unless there's something that's - I mean, one of the - for example, the kind of thing that we might suggest is the sort of thing that I was talking about a minute ago where we contact all these people in the ecosystem and start a conversation just to improve the communication if we find that communication is not as good as it could be. But I think the odds of us coming out with a recommendation that even talks about a cert are almost (vanishingly) low. Sure, go ahead.

Joerg Schweiger: So Joerg Schweiger for the transcripts record. I'd just like to add my point of view or my understanding of the risk (factor) and the DNS cert. I think that basically this very group has been chartered and it's (in the effect) of ICANN CEO saying that the DNS is to be a danger. And so this is just a working group charter (unintelligible) as a reaction.

And secondly I think that this was - or the statement itself probably was calling for a DNS cert under the operation of ICANN but this is just a speculation. In other words, I think the answer, whether or not the DNS cert operated by ICANN should be established or not has already been given, so that's the current (space). Thanks.

Mikey O'Connor: Jim

Jim Galvin: Well, I'm the real Mikey O'Connor although some people call me Jim Galvin. And I just want to give my perspective on the question of DNS cert and just exert that from my personal opinion, I hope that there is no reference whatsoever to such an organization or thing in this document or any work that we do.

Our charter is about looking at the risk assessment, doing a risk assessment of the DNS and that's it. We'll speak to that and what people do with it after the fact is, you know, their response to that. Thank you.

Mikey O'Connor: (Unintelligible).

Cheryl Langdon-Orr: Thank you Mikey. Cheryl Langdon-Orr for the transcript record. I'll take you to task later Mikey. There were three chairs that sat and drafted and developed and...

Mikey O'Connor: I'm in big trouble. We're talking serious major thunderstorm beating with the cane kind of trouble.

Cheryl Langdon-Orr: Would you like to try and get yourself out of this hole before I go on?

Mikey O'Connor: I'm pleading for mercy.

Jim Galvin: Yes, just for (a quick clarification), I'm no longer the real Mikey O'Connor.

Man: You as (so the real) Mikey O'Connor.

Mikey O'Connor: Yes, we're taking the possibly late Mikey O'Connor. There's another tradition that I haven't quite gotten to yet but I mumble a lot and at some point during this meeting I will be corrected on that by Cheryl Langdon-Orr, the other third critical paramount co-chair of the founding group of chairs. I apologize.

Cheryl Langdon-Orr: Thank you Mikey. It was C to the power of 3 not C to the power of 2 that worked on it. But you are absolutely right. It was in response to the issue of the sky is falling. And there is always a situation of people saying but it is and but it isn't or you think it is or you think it isn't.

The answer to that is facts and this is something very clear that we have to look at facts. That's why the analysis part is in the charter, why it's specifically focused the way it is. And from my materialistic point of view on why this space, why this workgroup was created, (hasn't been) what to wear. I would like us to have been in the time given (no), absolutely not.

I actually thought it was an easier job than what it was when we got in it. But have we done the job required to be a professional and quality (app time) to answer the questions posed in our charter? Yes, and if we'd done it any other way I would've become very critical during the process.

I had - I'm so pleased that not only was I part of why it needed to happen but how it's gone on and worked because we've navigated as a group through some pretty tricky times and when you've gone down a hole and it's oh, no, we're going to be here for years, backed out, work well done, not wasted. We'll toss that to the side. You have quite literally built and airplane that's gone through five wings and no wheels but it's actually flying pretty well right now.

The next phase - you'll notice this is phase one record - the go deep, the next phase two in my view is a proof of concept of the tools developed and nothing more and it needs to be seen as that. It could be seen as a new project. It could be seen as a subset. It could be seen as a stop in a new (start).

Don’t care. Do care that it gets done. All right, but then it’s ongoing work as all good risk assessment in any quality management system is ongoing. And that’s where it definitely needs, you know, where (Bill) and his group are coming from.

I think - I won’t say we, because I guess I’ve hung around and annoyed you at the edges - we have built some really robust and I would suggest world class tools. And I’d really encourage anyone out there who’s, you know, running a country, a ccTLD or just a business and wants to do risk analysis, to have a look at what’s there because this is clever stuff and it’s a power of all the minds coming together.

It’s been a privilege to work with this group. I know Mikey said it, but from my perspective, it’s been just an amazing experience so risk (unintelligible) but do note where it’s come from, why we exist and yes, we took longer to grow up but we’re running. Well, almost ready to run.

Mikey O’Connor: It’s a good thing you corrected that you over to we since Cheryl shows up on every Thursday call at 1:00 am local time. So Alejandro, did you want to jump in? I saw your hand go up.

Alejandro Pisanty: (Unintelligible).

Mikey O’Connor: Okay, I think we’ll draw a line under this part. This has been very helpful. If there’s something that you want to add to this, by all means, let us know. We really want to hear from the community on this. But let’s go on and just spin through the tools for a minute.

What’s on the screen now - and you know, I do want to compliment (Jacques) because (Jacques) and his colleagues came up with this idea and it was, like, a lightning bolt for us. We realized pretty early on that we needed some sort of methodology to do this work. And we found one. And it’s 350 pages long and it's (daintily) typed. It's the NIST 800-30 methodology from the United States.

NIST stands for the National Institute for Standards and Technology. And it's a lovely methodology but it's 350 pages long and it's written by people that don't understand how useful it is to put white space in a document. It's an extremely dense, really hard to read, and we were really struggling tailoring that methodology to meet the needs that we had in doing our work.

And it was at Cartagena that (Jacques) said, "Well, why don't we make this into a compound sentence?" And so what you're seeing on the screen, and you know, you may want to log into the Adobe room because it may be easier to read on the Adobe room but for everybody, I'm going to - well, I hesitate - I'm going to try it.

But, yes, it's not the animation that's the problem. It's the size of the text. It's sort of an eye chart.

Man: (Unintelligible).

Mikey O'Connor: Oh, that's true. Some people have used these slides before as opposed to others who though they were going to give this presentation before but then were forced out of the agenda of their respective - anyway. So let's try that. Good plan. That's (Ulrich).

So see the cool animation. So the way you read this is from left to right. And it says an adversarial threat source, in other words, a bad person or group that has the capability and intent and targeting to go after us in the DNS, or a non-adversarial threat source like a natural disaster or some other event that doesn't have the intent side of things can in the context of predisposing conditions - predisposing conditions is one that took us a long time to learn about in the methodology.

So we just take a slight detour and talk about an example or two of a predisposing condition. One predisposing condition would be the architecture of the DNS.

That's just something that's here. It's a condition that exists. And predisposing conditions can positively or negatively impact risks, so in the case of the architecture of the DNS in many cases that actually reduces risk.

And you need to factor those things in that reduce risk as well as those things that increase risk. The scale on that is pervasiveness. You'll note that there are blue nouns and then black are the scales in this thing.

Another context is the controls that are in place - security controls, and in fact we borrowed from another NIST methodology to build this list. I think it's NIST 800-53A.

And there the scales are, you know, are they planned or are they implemented? And this is the kind of classic audit that a lot of us have gone through with our data centers, where people come in with checklists to see whether we've got the controls that we need.

And the last is vulnerabilities that range in severity. So now we have threat sources on the far left. Either adversarial or non-adversarial in a context could initiate a threat event.

And when they initiate there's a scale and it's the likelihood that they're going to initiate it. They or the non-adversarial thing will initiate the threat. In our case we narrowed the threat event pool down to two.

The two threat events that we look at are the root is - the zone - either the root or the TLD is down or it's inaccurate. Those are our only two threat events and there's plenty of debate about that, believe me, which could result in -- that's the last arrow in that trio -- bad things happening, adverse impacts.

And in the case of our analysis we are not evaluating adverse impacts. The scales for those are severity and range. What we're saying is that if a zone either at the root or the TLD is not available, that is a very severe impact.

Cheryl's giving me a signal that I'm - well hey, Olivier's here. Another Co-Chair arrived. Olivier Crepin-LeBlond, welcome. So when you take this whole pile, this whole compound sentence, and put it together that's creating a risk.

And the risk is a combination of the nature of the impact and the likelihood that its effect will be felt. And what we're saying is that if these threat events happen the impact is huge, and what we're really working on is the likelihood side of this.

And that's where we're headed in the next phase is to start evaluating in a much more granular level, and you'll see in a minute, the likelihood of these things happening.

And I think it is safe to say -- Dave Piscitello made the comment -- that for the most part things aren't too bad. We're going to document that and be able to come back and say, "And here's why."

And the path to that is through likelihood, so there. Okay, so I'm going to stop at this point and I just realized that I need to bring - I want to show off one of the tools that we don't - and so I'll show off our Web page, our wiki.

So this is the Joint DNS Security and Stability Analysis Working Group wiki page out on the community site. We're in the - let me drive up here and - we're in the cross-community part of the community page if you want to find us.

And the reason I’m highlighting this is because this front page is where we tend to post these tools. And the tool I want to show you is the Risk Scenario worksheet.

So this is an Excel spreadsheet. It’s at Version 6 right now. It’s going to pretty quickly crank up a couple more versions, because we’ve got a bunch of ideas that we’re going to drive into the next generation of this.

But I’m going to just go ahead and download it and show it to you, because I think this is a neat gizmo. If I can make it the right size - hang on for just a minute.

So the -we took that drawing that we just walked you through and turned it into a spreadsheet so that now we really have taken 350 pages of methodology and collapsed it down to one page.

So the way you use this spreadsheet - and as you can see it’s out on the wild on the Internet. You can download it today if you want it. Every green square is an - is - provides you the chance to answer the question that’s just above it.

So in this case the question is, “An adversarial threat source - well what are those?” And if you look over just on the right side and you click on that, you get the list that we’ve been using in our analysis.

Now those lists are buried in other tabs on this spreadsheet, so if you don’t like that list you can change it to meet your own needs. So especially when we get out in parts of the community besides the root that we’re looking at, people using this spreadsheet might want to tailor it for their own needs before they start using it, but they at least have a starting point.

I’m not going to go through the whole thing. I just want to let you know that this is here. But basically all of those nouns and all of those scales are embedded in this worksheet as it stands today.

And at the end after you've filled in all the blanks it does the arithmetic. And so it's very difficult to do this on a screen at this resolution and I apologize for jumping around like this.

But you can see this column. As you fill in, you know, let me just take one of these scales. Here's a pervasiveness scale. So it says the pervasiveness of this thing is - this is the preexisting condition one so this is the one that reduces risk.

And you can see that as you pick these it starts doing the arithmetic on the far right side of the screen. So one of the problems - I've been a customer of a lot of risk assessments because I've been the CE - CIO of several large organizations.

And usually when you go out and you get a risk assessment, you get this giant spreadsheet that's like 90 million cells wide, 4000 cells tall. It's got all kinds of different colors and you can't make sense of it, and as a customer it was very difficult for me to use these.

So I was interested in this project from that customer experience, and if you decide to try using this we are really interested in your feedback on this tool because we think that this is one of the big contributions that we've made in the community so far.

So I'm not going to go any further into this. If people want a little guided tour later I'm happy to do it. But I did want to show you the depth and texture of the work that this group has done, because it's pretty amazing.

This is the end of the methods part so I'm going to again draw a line, do a little conversation. (Patrick) wants to jump in. Go ahead (Patrick).

(Patrick): Just to keep you on track for timing there is a session right after this. And in order to provide the next session enough time to prepare for getting their slides up and everything, maybe provide a five minute cushion or so or a few minutes.

Mikey O'Connor: That's really helpful. I kind of forget about that. I'm actually going to leave a little more cushion because it took me at least ten to get set up. So we'll go till 20 after the hour and so given that I'm going to cut this off.

We've done enough process stuff. If anybody wants to talk methodology I'm around, blah blah blah. Unless there's something really urgent that you really feel needs to get injected at this point, we'll just jump right into the findings. Going once, going twice. Okay. Yes sir.

Don Blumenthal: Don Blumenthal. Clarification - what time is the next session starting?

Mikey O'Connor: Ten thirty and it's 10:05.

Don Blumenthal: I must have misread.

Mikey O'Connor: Yes. Okay, so here's our findings. Again you remember that pie chart diagram and we were the pie chart slice that sort of stuck off to the right and down?

This is that pie chart idea modified into our findings. What we've come up with is five broad - very broad scenarios that we want to take a look at in the next and final phase of our work.

And so I'm just going to step really quickly through those. I want to make it really, really, really clear that these are not findings that we say are true. These are findings that we want to go look at.

So if somebody - this first one for example is pretty incendiary and it says, “Gaps in policy, management or leadership splits the root.” I really want you all to have in your heads that the DSSA is not saying that this is true, because we have not analyzed this yet.

But we’re very interested in this topic and it’s one of the five that we’re going to look at in the next phase. So let me just step through those five things. When you look at this chart this is the standard consultant two-dimensional matrix.

At the top is strategic stuff. At the bottom is tactical stuff. On the left is long-range stuff. On the right is immediate short-range stuff. And then, you know, the sort of core edge thing superimposed on that.

The thought is that at the edge, and here we have the Cheryl-Langdon Orr memorial cloud diagram, yes, is that long-term - mostly what we’re interested in in the DSSA is the needs of the people at the edge, the people who are doing the work, the people who are mitigating the risks, the people who are actually solving problems.

And those folks have two kinds of needs. In the long-range they need tools and models and ideas and support and encouragement and direction and connections.

And in the short-term they need coordination and fast response and trust relationships and all that kind of stuff. That said this particular scenario tends to be more strategic.

It tends to be slower moving. It’s more of a long-range thing. It tends to be one that’s probably more of concern at the core than it is at the edge, so that just gives you a sense of where we placed these scenarios on this diagram.

And I'll quickly step through the rest. The next one is stolen lock, stock and barrel from the ISOC work on this, and it's combining a couple of their scenarios about the future of the Internet.

And we compressed all that to say that our reductive forces, security, risk mitigation, control through rules and so on - that could split the root. This is something we're really interested in exploring again with facts in granular detail.

But it's still pretty strategic and it's still pretty long-term kind of stuff. The next one is starting to get into the more familiar territory of a traditional risk assessment that says, "A widespread natural disaster brings down the root or the root - or the zone of a major TLD."

Stepping through this, this is the classic adversarial threat source attacks. "Exploiting technical vulnerabilities of a DNS bring down the root or a major TLD."

This is the scary stuff. And then finally an inadvertent technical mishap - somebody makes a mistake and does something that brings down the root or a major TLD.

These are the sort of super broad categories that emerged from our first pass through that methodology as topic areas that we want to grind into in a whole lot more detail.

A question for you - I'm going to push through to the rest of this pretty long slide deck. I'm pretty close to done but file this question away. If we've missed something that - in these broad scenarios we really want to hear from you.

And if that something is extraordinarily embarrassing so that if you tell us about it, you're actually revealing something about you or your organization, you can - Paul Vixie is an adjunct member of our (Hardy) band, and he has agreed to be the anonymizer.

If you want to contact Paul with your embarrassing idea and do an NDA with him, he will then scrub off your identity and pass that embarrassing idea along to us.

This is part of that process that we built to handle confidential information, and Paul has volunteered to be the sort of public face on that. That's the end of go fast.

Two minutes on go deep and we'll take some questions for about ten minutes and then we'll wrap up so that the next group can get in. Our plan is to look more deeply into these five areas.

See, cool animation. I love that. Okay, so the - we're going to pick one. Now in this drawing we picked that particular one. That is not actually a decision we consciously made.

It just worked out really well on the diagram, so I'm not sure that this is the first one we're going to do. We'll talk about that as a group. But our thought was that we would pick one of these and use it to really beat up this methodology.

We've got a pretty good first draft. We've already got a whole bunch of ideas about how to make it better. That spreadsheet is going to get changed to do a few things better than it does right now.

And then we'll grind through one and, you know, our thought was we'll refine by doing. Once we've done one then -- cool animation -- we'll finish. And our thought was that as we finish we'll get broader.

We'll get more people involved. It won't just be the DSSA. You know, we'll start reaching out and we may use this in conjunction with that thing I was talking about with the pie chart earlier, where we start reaching out into the broader ecosystem to bring them into a conversation, introduce them to the tools, get their feedback, get their ideas, get their fact, et cetera, et cetera and finish this off.

We have left ourself a little wiggle room in terms of whether we're going to do all this stuff. And especially we need to coordinate pretty closely with the Board DNS Risk Management Framework Committee, because it may turn out that some of the stuff that's going on in there overlaps with this, and if that's true we will iron that out so that we don't do the same work twice.

I think that's it. There's all the pictures just as a reminder on the screen, but we've got, I don't know, seven, eight, ten minutes maybe for sort of broad question and answer and then we'll wrap up and let people transition in and out. Go ahead Bill.

Bill Smith: Bill Smith, PayPal. Mikey the - at the top of the pyramid there or triangle, whatever, the core, I think the issue that you had highlighted was are there gaps in policy management or whatever that could split the root?

Is there also a consideration for external activities independent of management/policy gaps that could split the root, for example the IETF draft on the autonomous Internet or without naming institutions international organizations and nation states that might wish to make some changes?

Mikey O'Connor: Thanks Bill. That's part of the reason I laid down all that foam on the runway about incendiary, because that's very much within the scope of what we are going to work on.

We're going to have to tread fairly carefully there clearly. But I think that's one of the differences between what we're doing and what the Board Risk Management Committee is focusing on.

We are not bounding our analysis to the walls defined by ICANN the corporation. We are looking at risks to the DNS period and so absolutely. Anything else? Go ahead Simon.

Simon McCalla: Simon McCalla. I'm sure that possibly Jeff or Alejandro may want to comment on this too, but I applaud you for that top bullet and for dealing with what will be a tricky subject.

It is something that we debated quite significantly within the SSR Review Team as to whether we should tackle organizational risk as a security threat. And it was a conscious decision actually we made to mention it but not to try and tackle it, because we felt we'd get stuck in the weeds for two years of doing that and not deal with other issues.

So I think the fact that you've got it there and the fact there's a chart to analyze that I think is really important, so I think top marks. Even though it is incendiary I think it's a really good thing.

Mikey O'Connor: Thanks Simon. Alejandro, go ahead.

Alejandro Pisanty: Thanks. I will just associate myself with the statement Simon has made. The SSR Team didn't have any submission, charge, structure, population and timeline - the - a charge to do that kind of assessment.

We do believe it is important, I mean, individually concerned but they remember found it important but not within our mission, and also able to derail us forever in a very bad way.

But the reason I asked you for the use of the microphone is also to mention that there's - in a conversation I had with Dr. Steve Crocker during the process in several interviews that they - we held for the SSR teamwork, he put forward the classification scheme for the risk.

That is particularly useful in one sense that I think that you can take up, which is how important is a risk for ICANN, how much attention it actually has to require and from which part of ICANN?

And that's very important. That's a little bit missing in your tool set. The grading of the risks seems a little bit too generic and I think it's very, very important to make it specific.

That's also along the lines of some of, I mean, that's very well within the frame of some of our recommendations. And then the risk analysis you provide from the DSSA would be a lot more useful for the different parts of ICANN that's going to pick up the work, including the - in my opinion advancing the - I guess the Board Working Group and certainly from our interactions with Staff and the vision that ICANN has to deal with risks very differently depending on whether they can be managed by - within the payroll, with the Supporting Organizations, Contracted Parties and so forth or just out there in the West.

Those are - a classification will be like breaks the root, stops resolution for a few hours. That kind of effect specific for the DNS and specific for ICANN's mandate would be very useful.

And I offer myself as a legal for this but eventually you have to talk to Steve Crocker himself, because he has a - an amazingly comprehensive view there.

Mikey O'Connor: Thanks Alejandro. Go ahead Bill.

Bill Smith: Bill Smith, PayPal. I want to support Alejandro's comment there. But I think that's critical because there - we really need to be sure that we separate ICANN the corporation from ICANN the community and also external players.

Each of us can be an external player where we sit in meetings here potentially and decide action needs to be taken, but it's best if that action might be taken separately, independently but in support of a larger goal.

But we may not know the goal or know the risk unless we sit down together, but the only way to effectively combat it is as individuals.

Mikey O'Connor: Just to build a little bit on what you're saying Bill, you know, I was watching the DSSA Alejandro as you were speaking and I think we go, "Oh yes, that's a good one.

We're going to steal that idea for sure." But I think what we want to do is vote. I think we want to - as we find these risks and as we analyze them, one of the things that we want to do is sort of try and figure out where on that pie chart the mitigation should take place.

In many cases the mitigation probably happens outside of ICANN because it's a pretty limited box that ICANN the corporation occupies. But maybe we can help the coordination side of that. Alejandro, go ahead.

Alejandro Pisanty: I think that it's a very interesting piece of territory you have just stepped into. I am - I think that it's useful for all to consider very carefully how mitigation is a word that comes into the work of the DSSA, because you're assessing the risk, not necessarily planning for the whole management.

And mitigation is typically, I mean, it's the - what comes top of mind a lot of times when you're speaking of management of risk. On the other hand if you don't consider what is the cost or the difficulty or the cost benefits ratio of managing the risk, then you may be working too much in the abstract.

So I would urge careful consideration of how much and just how much doing two things like mitigation transfer, evasion and all the other techniques for risk management.

Mikey O'Connor: Couldn't agree more Alejandro. This is exactly what happens on the DSSA. I go and say something stupid and then somebody fixes it, so you're right. You know, we will pay very close attention to our charter, but I'm still going to stick with the notion that as we analyze risks and determine the relevance to ICANN the corporation or ICANN the community, that it's useful to know both of those and then make it clearer.

We have a comment from Rosella. Hey Rosella - a big shout out to Rosella. She's a key contributor to the DSSA. She's coming through the chat room and so we'll let Julie be her voice.

Julie Hedlund: So I'm actually - Rosella has two comments. The first is, "Threats do not separate ICANN corporate and ICANN community, so we have to define the whole scenario and provide operational answers for ICANN corporate and environment."

And the second comment is - she says, "I agree with Mikey's mitigation answer."

Mikey O'Connor: I sure wish that we could have Rosella on the speakers but she's a big contributor. And with that I - I've just been nudged by the folks who manage the - do an exquisite job of managing the remote participation, that they need to get set up for the next meeting.

So we're going to draw this one to a close. I thank you all a whole lot for coming. Please stay in the conversation with us. It's very helpful. Olivier gets the last word.

Olivier Crepin-LeBlond: Thank you Mikey. Just a small comment to thank you for your great leadership, for all of the Chairs and for the whole Working Group. Without you there wouldn't have been such results achieved so thanks very much.

Mikey O'Connor: Beer for Mikey. I'm for that. Okay we're done. Thanks all.

END