Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
19 April 2012 at 13:00 UTC

Note: The following is the output of transcribing from an audio recording of the DNS Security and Stability Analysis Working Group (DSSA WG) teleconference on 19 April 2012 at 13:00 UTC. . 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. The audio is also available at:
http://audio.icann.org/gnso/gnso-dssa-20120419-en.mp3
Presentation will be posted shortly on:
http://gnso.icann.org/calendar/#apr

Attendees on the call:

At Large Members
. Cheryl Langdon-Orr (ALAC)
. Olivier Crépin-Leblond (ALAC) (co-chair)
. Andre Thompson (At-Large)
. Julie Hammer (ALAC)

ccNSO Members
. Jacques Latour, .ca (CIRA)
. Jörg Schweiger, .de (co-chair)
. Takayasu Matsuura, .jp

NRO Members
. Mark Kosters (ARIN); (co-chair)

GNSO Members
. Mikey O'Connor - (CBUC) (co-chair)
. Rosella Mattioli (NCSG)
. George Asare-Sakyi - (NCSG)

SSAC Members
. Jim Galvin (SSAC)

ICANN Staff:

Kristina Nordstrom
Julie Hedlund
Bart Boswinkel
Nathalie Peregrine

Apologies:
Warren Kumari (SSAC)
Scott Algeier

Coordinator: Please go ahead. This afternoon's conference call is now being recorded.

Nathalie Peregrine: Thank you very much (Tim). Good morning, good afternoon, good evening this is the DSSA call on the 19th of April 2012.

On the call today we have Mikey O'Connor, Cheryl Langdon-Orr, Andre Thompson, George Asare Sakyi, Olivier Crepin-LeBlond, Takayasu Matsuura, Jacques Latour, Julie Hammer, Rossella Mattioli and Jorge Schweiger.

From staff we have Julie Hedlund, Kristina Nordstrom, and myself Nathalie Peregrine. We have apologies from Scott Algeier and Warren Kumari

I would like to remind you all to please state your name before speaking for transcription purposes. Thank you very much and over to you Mikey.

Mickey O’Connor: Thanks Nathalie and thanks all for joining us. We'll take our moment to see if anybody has a statement of interest update that they want to share?

Oh good (Mark)’s on. Good, good. Okay it's a pretty short agenda today. We’ve got a pretty nice crop of risk scenarios that folks have submitted, hats off to all of you who did.

And it’s on your screens in pretty small type so if it's too small let me know. But based on my screen it looks about the same size as everything else.

Is the list of scenarios on the DSSA Web site? And I commend these to you. I'm not exactly sure how we want to go through them but I think it might be useful to at least visit some of the highlights of each one and encourage anybody else who's got some more in their mind to go ahead and submit them.

And so anyway that's the first part of the agenda is to sort of take a look at those.

And then the second part I think at about quarter to the hour we'll break off the risk scenario discussion and take about 15 minutes to take a look at the latest version of the confidential information draft that I pushed out yesterday to the list.

So that's sort of the agenda, anything else on people's minds that you want to add to this before we dive in?

Okay well as you can see on the screen we've got a pretty nice collection of risk scenarios. And I'm sort of the organizer and chief of them I've read them all and I think they're pretty good.

I like them a lot. And I'm not exactly sure where we’re going to go with these but I think that what we want to do - the way I've set up the process on the wiki anyway is that this page that you're looking at has all the risk scenarios on it.

And I'm going to just scroll down a little bit so that A, you can see the rest of the risk scenarios and you can see that there are newer versions that are coming in.

(Rosella) for example has updated hers and so you can see underneath hers there’s a newer version. I'll just increment the versions as we go so that people can see the old versions if they want.

And the idea that I had when I laid out this Web page was that somehow we would review them as a group and promote them to this sort of stage II where there are scenarios that we as a working group support.

I'm not sure that we absolutely have to get to consensus about them in this first pass because as I read them they’re very interesting and very, I think they're very rich.

I think they were going to wind up having a hard time choosing which one’s we want to go into depth on.

But I think what we may want to do is go through them and at least, you know, determine that there isn't some huge error or mistake in them.

And then at some point fairly soon within the next couple three weeks decide on which ones we'd like to take into the go deep phase presumably is going to start after Prague.

So I think before I start going in to these I'd just like people's ideas on how we could review these.

I mean have people been in the process either in ICANN or elsewhere where there are a whole bunch of different documents like this that needed to be reviewed and evaluated and used a process that worked really well to get that done?

One way to do it would be to just start at the beginning and go through them all. I think if we went through them all we've got enough of them already that it would take several weeks just to walk through each one, one at a time because presuming it would take five to ten minutes per scenario we could probably only do three or four per call.

So I'm wondering if there’s a better, easier, faster way to do some sort of review or not. If not that's fine. And what we could do is maybe give them a very fast review and then push the actual deep review back into the go deep phase.

But before we go anywhere at all I’d kind of like to hear from people about ideas on how we could talk about these and review them, any thoughts?

You're in the same boat I am, a little puzzled by this.

Cheryl Langdon-Orr: Mikey it's Cheryl here. I can't put my hand up as you (really) know.

Mickey O’Connor: Right.

Cheryl Langdon-Orr: The first thing I would do if I was looking to I guess package them in some sort of way would be to cluster them together and perhaps the advantage is going from the top to the bottom do them in sort of groupings.

I mean we do have things which tend to be more or even this relatively short list, you know, (imagined) (self) can get it together as opposed to, you know, (unintelligible) could go together as opposed to disgruntled or met. So...

Mickey O’Connor: Yes.

Cheryl Langdon-Orr: ...(unintelligible) out first and then go through them and (what is their order) take (unintelligible).

Mickey O’Connor: Yes that's an idea that's - as I was reading them I was starting to see those clusters and idea. I could easily do that.

Take a moment and talk about clusters. To me that Cheryl has pointed out a couple of them. One is the large scale outage one.

Another is the...

Cheryl Langdon-Orr: Nations state and individual.

Mickey O’Connor: Nation state one and then - wait there’s a continuum from sort of technical attacks technical issues so outages, DDOS attacks then all the way to the other end of the continuum which is sort of the policy nation state. There are some clusters in there.

So maybe that's one thing to do is for me to take an action to cluster (unintelligible).

((Crosstalk))

Mickey O’Connor: Oh Olivier’s got his hand up. Sorry about that, didn't mean to talk right through you Olivier. Go ahead.

Olivier Crepin-LeBlond: Thanks Mikey. It's Olivier for the transcript. I was going to say the same thing as Cheryl but also suggest that prior to treating a specific cluster perhaps we can decide in advance on what cluster we go with and have everyone study that cluster prior to looking at it.

So we don't need to actually go through it line by line but we are already all come with our points of view about the cluster rather than actually reviewing it as you would do holding our hands. Thanks.

Mickey O’Connor: Yes I think that's another really good idea because I think going through these line by line is going to be a long painful process.

So that is a friendly addition to this (review). (Jacque) go ahead.

(Jacque Asamatzo): Yes one idea I had was maybe we create a spreadsheet that summarizes all of the scenarios like a description and then the number at the end so that we can put things in perspective to see if a DDOS is bigger in fact than policy or stuff like that? Like a summary table.

Mickey O’Connor: I have one of those. Let me show it to you. It's pretty rugged to see on the screen. And it’s still in draft but I did start doing that. Let me just shrink - this is prior to - I did this after the first round came in.

So (Jacque) be not annoyed that yours isn't in here yet but this is maybe - I totally forgot about this until you mentioned it. Let me make this just a little bit bigger so you can see it.

And what I think I need to do oh, make the framework right, hold on a bit. Sorry to bewilder your eyeballs with all this.

No, that's part of my job is to bewilder your eyeballs right? So anyway what I did in this one is just put the sequence number. And that makes this pretty hard to understand because you can't really see the summary that I put into -

you know, I kind of like these summaries that it put into the Web page because it sort of makes it easier to understand.

So I think what I'll do is stick those summaries into this table and I think I pushed this table out to the Web page if you want to read it. No I haven't. So you can't, sorry. I'll take an action to do that too. It's Mike stumbling along fine form.

I do this to provide entertainment for Cheryl late at night. I’m sorry, act a little more...

Cheryl Langdon-Orr: And you do it so well Mikey.

Mickey O’Connor: Anyway I agree with you (Jacque). It's I think going to be useful to have a summary that we can sort of cast our eye across it.

So maybe what I'll do is take an action to redo this summary with some clumping and some additions of hints as to what's going on and push that out to the list soon because this is isn't that far from done. It won't take long to update this.

If we were to - we can sort of predict some clumps. One clump is going to be the outage clump. Another is going to be the nation states clump and another is going to be the DDOS attack.

Does anybody have a favorite of those three that maybe we could pick what we’re going to review next week as a trial run clump.

Now there's somebody that's got their phone not muted. Nathalie can you tell who the noise is coming from?

Nathalie Peregrine: I'm just waiting for the operator to pick on (up).

Mickey O’Connor: Okay terrific. So let me put the three choices in there, clump choices, clump choice -- nation state, choice outage, abbreviation clump choice.

Any strong feelings about which of those two do on next week's call just as sort of a trial run? Clumps, I kind of like that.

Maybe it's coming in through Adobe. Maybe it's Cheryl. That's Cheryl.

Cheryl Langdon-Orr: Why would it be me?

Mickey O’Connor: It's always you just like it's always me. If it's not me you’re the next best choice, culprit. Well I don't see anybody just global thermal nuclear - what.

That's, okay that sounds good. See that everybody's treating this...

Cheryl Langdon-Orr: Like they said there'll be an outage?

Mickey O’Connor: Yes. It sounded like outage to me. Treat it with the appropriate level...

Cheryl Langdon-Orr: Outage wins.

Mickey O’Connor: Okay. I think that's kind of enough on this. I don't want to drag us through a whole lot of detail today. That was what I was really frightened of actually was that we would dive way too deep too fast. Let me take these ideas and push them into another generation of this chart.

But you see it on your screen and I'll get that out pretty soon and encourage, you know, we’re still in a reasonable time window to add some more scenarios.

So I would ask that we, if you've got any new ones to try and get them into me soon. Because we are starting to get up against not crushing but reasonable report writing deadlines that would be good to get this part of it done well within the next few weeks.

But I'm really liking them a lot. I think that at a minimum they will provide lots of food for conversation.

Let me use a topic as sort of a segue into the next part of the agenda. I'm actually going to go on to the next half of the agenda now which is the confidential information thing.

And one of the - that’s really weird artifact. One of the things that we have been discussing a lot in Ops Leadership Group is the confidential information process that we’re using.

And we’re still in draft on that but we'd like to get to an approved draft for the report. And one of the things that came out on the chat on the last call that I didn't have time to get to because I lost track of time I think (Jacque) brought it up but others did too.

It was the one about well what about really embarrassing scenarios, scenarios that if you wrote the scenario you would give away confidential information just by writing it?

And that dovetailed really nicely into a conversation that we were already in the Operations Group which is sort of the yes right problem, you know, where we march in and say give us your confidential information.

And the sort of security technical leaders of these organizations say yes right no way I'm giving you that information.

And so what we did is we came up with a couple of things. One - and we'll go through the - this one in a minute. One we've beefed up this draft document just a little bit. And I want to take you through the ideas that we came up with.

But the other idea that we came up with was that if you have, you know, a scenario that you don't want attributed to yourself because having it attributed to you would give away something about your organization that you don’t want to give away.

We thought it might be useful to offer sort of a trusted intermediary that you could send your scenario to and then they can submit it for you.

And you could go you could even go so far as to enter into a confidentiality agreement with them so that they would promise not to reveal the source of embarrassing scenario.

I mean the third option is the one that I sort of hinted at on the phone which is try and write it in such a way that it's not embarrassing.

But it may be that it's impossible to do that. And so I sort of wanted to circle back to (Mark) for just a second and see if you had a chance to reach out to the person we identified on Monday as our possible intermediary.

Can I go ahead and name that person and...

(Mark): You certainly can and I will be seeing him face to face this coming week.

Mickey O’Connor: Oh great. Okay. Well our thought was that if you wanted a trusted obfuscator, a trusted person who could (anonymize) your embarrassing scenario that you could get in touch with Paul Vixie and as soon as I hate to put his contact information out here until we've actually had a chance to talk to him. So let's postpone that till next week.

But know that you've at least got an option for this if you've got a scenario that you really feel you can't submit directly. That's another way to get it into the queue.

(Mark) did I hear you take a breath to start saying something because if you did...

(Mark): I was. We’ll have a - like you said, we'll have an answer for the group. It'll either be Paul or someone that he thinks is a good replacement for him for next week's call.

Mickey O’Connor: Perfect. That's great. You know, and one of the things that - I mean this group is plowing all sorts of new ground, that's for sure.

But this confidential information one is new ground as well. And so I'm really interested in working on making this work because it may be something that's useful to other groups in other places.

So I just sort of wanted to use that idea as the segue into the changes that we made to this draft.

And part of the reason that I - I'm so delicately introducing this is because the last conversation we had about this draft on the list, it's too bad that Don’s not on the call.

Don Blumenthal was saying that he had concerns about this maybe being a little too harsh.

And unfortunately in the context of that conversation this draft has gotten even more harsh because what we've realized is that the primary goal of this process is to protect this information.

And we actually went back to a couple of the charters, Chuck Gomes from VeriSign and (Chris Despane) from the board to sort of confirmed that we were on the right track with this.

And we got a pretty strong endorsement from those two charters as well that the goal of this is really - and this is the first change. I’ll start highlighting stuff in here.

Is that the goal of these guidelines is really to make sure that the people sharing information are confident that their information will remain confidential.

And then that if we have to be a little bit nontransparent and a little bit unfair we are - we have actually got a charter that says that it's all right to do that.

So unlike most things in ICANN this is not a come one come all everybody is welcome kind of affair.

This is really designed to make sure that a small group of people who are instilling the confidence of the information providers are the folks that work on these things.

And so unfortunately as you'll see in a minute these guidelines have actually gotten a little bit more tilted towards the information providers in order to get over this problem, the yes right problem.

Because that's really our goal is to make sure that information providers feel confident enough that they can share their information.

And we’re still not sure that this is actually going to work but this is our latest try.

So let me scurry down here. Sorry I'll make your eyeballs hurt as I scroll. Let me put this in context.

So one of the parts of this talks about how the subgroups are formed and this is mostly out of our charter.

But one of the things that we added is that information providers may get into one of these groups feeling okay, feeling confident that their information is being protected.

And then when they're in it discover that there's something missing in what we've drafted. Because, you know, we’re getting more and more comfortable that this draft is right but we may have missed something huge.

And we wanted to give the information providers a way to modify these in process so that they didn't find themselves trapped in something that's insecure.

So this is the first tilt towards information provider change that you're going to see in this draft.

The next one - this is our chart. You've seen that before. I'm going to scroll through a few more pages. Sorry to blur your eyes.

The next part is in the way that people are added to the subgroups. And this is the change right here.

When we checked back with the charter as (Chuck) and (Chris Despane) both of them said that what they had envisioned when they were describing the subgroups was that information providers would get together with a small trusted - I think (Chris Despane) used the word group of friends to do this work.

And so we added them to the process of add of forming the group. In the first draft of this the co-chairs formed a seed group and then we used a vouching process to expand the group.

In this version the coachers and the information providers do that together.

Once again in all of the goal of all of this is to make the information providers more comfortable.

We've also revised...this section just a bit...to...again focus the sub group to make it unfortunately for many of the values of ICANN this is making these more exclusive but again the overriding goal is not transparency it's the ability for information providers to share sensitive information safely.

And so the -- another thing that we've added here is that we're going to focus these sub groups on being as small as possible. I think it was Chuck Gomes who said the more people in these groups the more likely or the more risk that you're going to see exposed information.

Oh Don's on the call, great. Don I'm sorry to be right in the middle of this for you but we're talking about confidential information draft and unfortunately the draft has gone opposite direction that you wanted us to go.

So bear with me for a few minutes as I kind of finish walking through this draft and then I'll circle back to the top and just highlight some of the points that I made right at the beginning of this and then we can discuss all this on the call.

One of the things that we added was a section about leaving the sub group...which really just expanded the language that we had before and again we've tilted this further towards the information provider community and said essentially that an information provider can eject anybody on the group at any time...for any reason.

And again this is all about protecting the confidential information. And so we're tilting even further towards exclusivity and information provider comfort.

But we also added this section at the end that says anybody can leave if they want. But we especially want to make it clear to the information providers that they're not trapped in these groups.

If they are in any way uncomfortable with what's going on they can exit at any time. And again it's because the goal of this is not to put information providers on the spot and perform an inquisition of whatever topic it is.

This is considered at least by us and the (ops) group as a great gift and a great contribution to this effort by the information providers.

And if at any time they feel uncomfortable providing this information they have the right to leave and at the same time departure does not relieve anybody of the responsibilities that they have incurred under their confidentiality agreement.

So if an information provider leaves that does not mean that the rest of the group is suddenly unbound from those confidentiality agreements those stay in place it's...in tilting towards the information providers.

I think those are the big changes. Don just to get back to the top of this thing real quickly. Basically in summary what we in the operations group have been doing is talking a lot about this draft of the confidentiality information or confidential information stuff.

Partly because we're driving to the final report and we want to get a consensus version of this if we can in, you know, ready to insert into the report.

But also because partly due to conversation on last call but really due to prior conversations as well. We were concerned that this draft doesn't quite go far enough and so we beefed it up a bit.

And the part that really highlights that and summarizes what we're really trying to do is to make it clear that these are for primarily for information providers they're not transparent they're not inclusive they're not the usual ICANN value set this is really a very narrow case where in our charter we are allowed to deviate from some of those ICANN norms.

So with that rant and a little circle back just to bring Don up to speed I'd like to hear comments from the rest of you on this and thoughts about where we're heading with this.

Everybody's typing. You can speak.

Don Blumenthal: Okay I will...

Mikey O'Connor: Oh good.

Don Blumenthal: ...as I appreciate that...

((Crosstalk))

Mikey O'Connor: This is Don with speaking by the way for the transcript.

Don Blumenthal: Thank you. Yes one of the reasons I (unintelligible) is I just woke up so I guess I'm not awake yet. Long story in that.

Any event thanks I appreciate the quick look back. I'll go ahead and take a look at the and listen to the transcript they go out and just go the full details.

Yes I certainly have no concern with just that (unintelligible) briefs (unintelligible).

Mikey O'Connor: Yes I think the thing that you were concerned about is the part right at the end and let me go back to that and remind you of your concern because we've been thinking about it, you know.

Don Blumenthal: It has been awhile hasn't it.

Mikey O'Connor: Yes. That the concern that you had was around this sentence and saying really if they lose the people that to vouch for them that causes the members to have to leave the group, really?

Don Blumenthal: I did have that concern, yes.

Mikey O'Connor: Yes and so we thought about that and the conclusion we've arrived at is yes that is in fact true. That again this is all about tilting this towards the needs of information providers and if people don't have sufficient vouched or vouch and, you know, people vouching for them they should either find some more people to vouch for them or they should leave the group.

And we actually stole this idea from (Orak). We stole a lot of ideas from (Orak) in this document and this is one of them.

This is the way that (Orak) does this I think although Jim's raised his hand and knows more about this than I do and maybe getting ready to set me straight.

But anyway that's the idea.

Don Blumenthal: Okay it's Don again. I just when you said or find other people about for the you answered the question I had. This is fine and I do remember the concern but it they can just ask (NomCom) and to prove whoever it is has shown their value and shown your trust and that's (unintelligible) no concern at all.

Mikey O'Connor: Okay good deal and, you know, I suppose we could highlight that in this draft because if it left you with that concern that might have that vagueness might have left that concern for others as well.

Jim go ahead.

Jim Galvin: So I'm not going to claim to, you know, anything about the details of how (Orak) does things I just wanted -- this is Jim Galvin so the transcript I just wanted to go on record as saying that, you know, I had the same concern that Don did.

I'm actually not fond of this rule but I'm just agreeing to it based on what you said which was that it's the way this is phrased that you have to have at least two other members who have vouched for you and you can change who those two people are so if you're, you know, starting two people should leave as long as you can find two others you can stick around in the group.

And so I was comfortable with that as an answer although I would prefer that we didn't have this rule altogether.

So anyway I just wanted to put that on record. Thanks.

Mikey O'Connor: Thank you sir and I stole your words and pounded them into the draft so I may clean that up just a little bit (unintelligible) sorry I'm mumbling for sure it's the daily mumbling quotient I just want to highlight that so I don't forget to tidy that up.

Any other thoughts about where we're headed with this, you know, I think we're pretty close but we'll follow our usual rule which is we'll talk about it today and we'll announce that we're half way to consensus if we get there today and then we'll review it again on next week's call for people who missed this call for final consensus.

Julie go ahead.

I'm not hearing you. You may be muted in some way Julie. Still not hearing you Julie.

This is the third and final call so it's not muted on the bridge. Do you have a mute button your phone Julie? Maybe your phone is muted.

Oh Julie is typing. Well let's see I can't imagine what else would do that.

Okay I'll just read your comment in Julie and tell you what since you tend to come on the call a bit early let's next week we'll test your phone and figure this one out that's too bad that you can't speak.

Anyway Julie in the chat said if in an information provider leaves a sub group then perhaps they should specify whether the information already provided can continue to be used or is withdrawn -- oh that's a very good one.

I'm going to steal that and staple it in to the draft now here...highlight it although I tidy it up. But I think that's a good edition to our idea.

And I'll take that as a friendly amendment. Olivier go ahead.

Olivier Crepin-LeBlond: Thank you Mikey and (unintelligible) for the transcript record. I know we've discussed this system of two people vouching for another person we've discussed this ad infinitum but to this date I still don't understand the rationale behind it.

If two people vouch someone then that person then comes on the group and starts work and so on certainly that trust has now been extended to that person.

Why would one take the trust away if one of the people vouching for them has to get on with their life and do other things? It seems to be that you're constantly putting people into question with this sort of system.

And I just find it a little bizarre.

Mikey O'Connor: I think that's exactly right. I think that the -- and remember I've never participated in a group like this so I'm sort of parroting back what others have said.

But we had somebody from the (Orak) on one of the (ops) calls and -- like having a senior moment on their name and they described sort of why and how the (Orak) does this.

It's essentially this notion that it's a continuously maintained level of trust and that it's extremely high...in this particular circumstance.

And beyond that I'm sort of playing back what others have said but I tend to agree with it that this is about reassuring the information providers that the trust level is maintained at an extremely high level at all times and that if...that can't be maintained then the comfort level of the information provider goes down and they don't participate.

And, you know, as soon as they don't participate for any reason if they're in any way uncomfortable then we lose the value or their participation.

And so, you know, I think that it's reasonable to ask people to, you know, if one of their vouching folks goes away that they hunt around for another one and reaffirm that indeed there's still a high level of trust there.

That's a, you know, that's kind of repeating I'm sort of repeating myself at this point. But, you know, that's my understanding of the rationale for it.

And I think that, you know, the opposite, you know, the opposite approach which is clearly to remove this runs the risk of losing information provider confidence in this process.

And as soon as lose that we get the yes right problem. And we thus don't get the information that we're on the lookout for.

Oh that's interesting when Nathalie left all the little -- oh no I guess not. Dubious is fine but I want to move on I don't want to I'm sorry Olivier typed I remain dubious in the chat.

But, you know, I think we need to get over this one way or another and I'm very skeptical that we can get information providers to participate without this.

Cheryl Langdon-Orr: (Unintelligible) here.

Mikey O'Connor: Go ahead Cheryl.

Cheryl Langdon-Orr: Just coming back to something that was disused before we got into the specifics on the (liquidity) the leading of the and Julie's amendment of information provider list sub group and their requirements specify what you see (unintelligible) may be as to put to.

If we're going to be using what I think is very (unintelligible) to be able to use this proxy system so that the there is an even greater distance between the information source and then they can even from how it gets into these sub groups.

(Then) we going to have a slightly different model where we may in fact have sub group that does not have the actual information provided in its (unintelligible) at all.

So can you put your thinking cap on and see whether that six is vouching system in some way that is unpredictable?

Mikey O'Connor: Yes my, you know, and now I'm inventing this entirely on my own because ops group hasn't talked about this. But my sense is that if the information came in through a trusted third party that it would not be confidential information at all and would not be subject to this process because the third party would essentially be the confidential sub team.

Cheryl Langdon-Orr: Gotcha. I disagree. I think -- this is Cheryl for the record -- if you are using a proxy you were using proxy for a reason and the proxy should still be able to maintain the harsh integrity of confidentiality but it maybe the point where it simply me being in the room making it into the sub group would make it obvious that it’s, you know, my company that’s (unintelligible) you or my (unintelligible) is the issue.

Mikey O’Connor: Right.

Cheryl Langdon-Orr: And so if wanted to ask Olivier to put this piece of information...

((Crosstalk))

Mikey O’Connor: Oh I see what you’re...

Cheryl Langdon-Orr: ...risk and analysis being I still want the confidentiality I’m just already putting enough of distancing between it being all it’s Cheryl (unintelligible) know the rest.

Mikey O’Connor: Yes I understand now. So that’s a whole different concept. So you’re saying something like that, right?

That there’s a proxy member if of the sub group that’s there throughout the life of the sub group...not just providing information at the beginning, correct?

This is back to Cheryl.

Cheryl Langdon-Orr: Yes.

Mikey O’Connor: I think I need to cogitate about that one.

Cheryl Langdon-Orr: For example if I may -- Cheryl for the record Olivier may end up being the trusted proxy for four different information sources.

Mikey O'Connor: Right.

Cheryl Langdon-Orr: Because four different information sources made for very good reasons not wish to talk to each other public or privately for, you know, not wanting to disclose what he asks but if they all trust Olivier to bring the data (unintelligible) then that's great.

If an advocacy in proxy (unintelligible) but the advocacy part normal it would be that you'd be trying to do the best interest for the person you're representing in this case the best interest it's confidential.

And you'll get the information out for analysis, you know, not attributed fault.

Mikey O'Connor: That's a really interesting thought. Let me cogitate about that. Feed that back into the operations group and see what we come up with on that.

Julie you want to take another...

Julie Hedlund: Can you hear me this time?

Mikey O'Connor: Oh it's lovely.

Julie Hedlund: Yes. Correct okay. I'm just wondering with regard to the management of all of this sensitive information whether this document should have any words about a data repository and what sort of information ought to be stored in that like a piece of sensitive information what the source was if that source is able to be recorded what's the release ability if the information is at attribution just that whole data repository where all of this information is actually understood or recorded and it's release ability it's attribution it's sensitivity understood.

Mikey O'Connor: We -- I'm typing and speaking at the same time.

We had some conversations about that and tip toed around that topic in this draft...because we immediately fell down the rabbit hole of trying to design that system and...I think we need to circle back to that topic as you were speaking I was going oh yes we I remember this conversation.

And so I think...

((Crosstalk))

Mikey O'Connor: ...I need to go back to our notes and dredge up some of the ideas and conclusions we came to because I can't remember them...at this point.

Julie Hedlund: Yes because I think one of the most important things about protecting information is understanding all of its features and what needs to be protected and within what circles.

Mikey O'Connor: Right I've got that. Let me take an action to circle back on that one. I can't remember unless one of the other (ops) folks can -- has a better memory of this discussion that I do.

I have to go back to the notes which I will...on that one...because I know that we consciously did not put that in here and I can't remember how we arrived at that conclusion.

And then what -- and the other thing I can't remember is what we were going to do about it instead. So let me just punt on that whole thing and circle back.

Good one. Any other thoughts on this? Got some pretty good work coming from the Australian contingent I don't know. Awfully -- unless you're not in your native time zone you guys you're awfully sharp for this hour of the day.

Julie Hedlund: We're midnight owls.

Mikey O'Connor: That's great. Anything else? I think, you know, we're getting greatly close to the top of the hour so I don't want to belabor this and we'll wrap up but this is a very helpful conversation and no indeed we are not a consensus yet so I'll take this stuff back and grind it into a new draft and run it by the (ops) group on Monday and maybe be back next week.

Blood flow to the head, yes, upside down, nice chat.

Okay people (Nathalie)'s not on the call so I'm not going to speak to her but (Tim) are you our Operator today? I wasn't paying attention if you are I think we can end the recording.

Coordinator: Yes I am and thank you I'll take the call and you can stand down Mikey.

Mikey O'Connor: Oh great it's always good to have a familiar voice on the other end of the phone. That's the call for today. I'll see you all in a week. Thanks a lot.

Man: Thanks Mikey. Thanks everyone.

END