Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
01 December 2011 at 14:00 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 01 December 2011 at 14:00 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-20111201-en.mp3
On page: http://gnso.icann.org/calendar/#dec (transcripts and recordings are found on the calendar page)

Attendees on the call:

At Large Members

- Cheryl Langdon-Orr (ALAC)
- Olivier Crépin-Leblond (ALAC) (co-chair)

ccNSO Members

- Takayasu Matsuura, .jp

NRO Members

GNSO Members

- Mikey O'Connor – (CBUC) (co-chair)
- Rafik Dammak, GNSO
- Don Blumenthal – (RySG)
- Scott McCormick (IPC)

SSAC Members

- Jim Galvin (SSAC)

ICANN Staff:

Patrick Jones
Julie Hedlund
Nathalie Peregrine

Apology:

Jorg Schweiger

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

Nathalie Peregrine: Thank you, (Tim). Good morning, good afternoon, good evening, this is the DSSA call on the 1st of December, 2011. On the call today we have Takayasu Matsuura, Don Blumenthal, Rafik Dammak, Cheryl Langdon-Orr, Mike O'Connor, Scott McCormick, Olivier Crépin-LeBlond and Jim Galvin.

From staff we have Julie Hedlund, Patrick Jones and myself, Nathalie Peregrine. We have apologies from Jörg Schweiger. I would like to remind you all to please state your name before speaking for transcription purposes. Thank you.

Mikey O'Connor: Thanks, Nathalie. As always getting that complicated audio going way in advance. Welcome all. First thing up of course is the momentary pause to see if anybody has an update to their statement of interest.

And just a reminder we're getting a little echo on the line so if somebody's got their speaker on or their microphone on do please mute that so that we don't - Cheryl and I took echo to new heights before the call started. And so I'm especially aware of that today.

Anybody got changes to their statement of interest that they want to tell us about? Okay.

Today is a one-topic call really zeroing in on the methods discussion that we started on last week's call; we've actually been having for several calls now. And I think that what I'd like to do is treat this as a consensus call and we'll repeat it very briefly next week just to nail down this decision that we're going to go ahead and use the methodology that's outlined in the NIST 800-30 document that we've been reviewing and talking about for the last couple of weeks.

But I think it's good to let the working group actually come to a formal consensus on that. So as we're going through the call today do think of it that way and if there are any issues that you want to raise feel free to do that and then we'll very quickly repeat that to the list first during the course of the week and then next week we'll come back and just check with people to make sure that this is okay.

I have a question for those of you on the call I'm curious - I can't remember who has seen this stuff and who has not. Last week I walked us through this NIST methodology using an extremely large document which may blank out some of your screens.

And I'm happy to do that again but I just thought I'd check and see if I needed to or if people are familiar with that document in which case I'd jump forward one notch to a standard Mikey mine map that I've started making that's based on that document.

So a quick poll of folks who are on the call today just use your little hand raising gizmo or your agree gizmo. Who would like to have a brief tour of the NIST document just to get brought up to speed on what this mythology is all about? Not seeing any hands go up so I'm going to assume that you either - I sent it to the list and I haven't posted it to the site.

I'm going to take a moment and make myself another note. I'll post that link out to the wiki as well so that people can quickly get to it. That would have been something handy to have done before the call. Sorry about that.

And instead I will go ahead and jump into a document that I've started preparing. It's not done; it turns out this methodology is pretty rich and it's also pretty hard to read so it's taking me a while to get this project done. But

I've got a fair amount of it done and enough of it done so that you can see sort of what I've come up with.

Oh that's interesting got a gray screen. Does everybody have a gray screen?

Cheryl Langdon-Orr: Yeah, more of a blue-turquoise but...

Mikey O'Connor: Yeah, kind of a bluish gray; kind of a nice bluish gray but definitely not - definitely not the stuff I want to show you. That's interesting. I wonder what's going on with that. Try that again. That's a dud.

Cheryl Langdon-Orr: Maybe we really did break it, Mikey.

Mikey O'Connor: Yeah maybe we did. Cheryl and I were having a great time fooling around with the settings in the room before the meeting. And maybe we just killed it.

Cheryl Langdon-Orr: Are you now running it from the modem seat?

Mikey O'Connor: Yeah that could be it. It could be that it's just not uploading. Let me try toggling that preference back to the faster one - that does. Boy that's just broken, broken. One more try, sorry folks. This has never happened to me before. I'm in frantic - oh user error. Tee-hee, sorry.

In the US there's a word that's very helpful to me; it's expanded my vocabulary a lot, the word is Doh. Sorry about that. Hang on a minute.

Cheryl Langdon-Orr: The Canadians have spread that further than the US thank you to...

Mikey O'Connor: Oh yeah well I, you know...

((Crosstalk))

Mikey O'Connor: ...acutely conscious that I don't know the borders that certain words have traveled to yet and that particular one is one I use a lot. Olivier, go ahead while I'm fixing my mistake.

Olivier Crépin-LeBlond: Thank you, Mikey. It's Olivier for the record. Are you using a fruit-based computer?

Mikey O'Connor: I am using a fruit-based computer. And - but that's not the problem.

Olivier Crépin-LeBlond: Because we had problems with uploading some PowerPoints using a fruit-based computer onto Adobe so it might be a bug.

Mikey O'Connor: No it's a - this is what's called a user error. I was busily sharing the Adobe Connect application on the screen.

Olivier Crépin-LeBlond: Nice one.

Cheryl Langdon-Orr: Oh thank you for that, Mikey that's...

((Crosstalk))

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: ...that was good of you to do that. Have you toggled it back to modem speed though now?

Mikey O'Connor: Yeah it's back to modem speed.

Cheryl Langdon-Orr: Good.

Mikey O'Connor: That's what took me so long. So we're on the slow speed connection thing and sharing my screen which is a little small I can see.

Cheryl Langdon-Orr: At least we can all see it.

Mikey O'Connor: Yeah, oops that's not what I was expecting to have happen. Got a little bigger, I can sort of shrink this a little bit. Let me show you what I'm up to here. I decided to just - for those of you who've actually read or even started to read that methodology know that it's very dense.

And I think that this is an unintended consequence of a law in the US that punishes bureaucrats for writing documents that are very long. And so the unintended consequence of that is that bureaucrats now write sentences and documents that are extremely dense and they don't put any line breaks in the paragraphs.

And as a result this methodology that we're using is quite good but it's really hard to read. And so I've been breaking it into chunks so that I can understand it better. And I just want to walk you through sort of what I’m up to and where I'm at and get your reactions to it. So feel free to criticize.

Remember that this is sort of a consensus review of whether this document - this methodology is going to be the right approach for us. But I'm also sort of moving forward into the next phase which is where we'll actually start using the methodology.

So as you can see there are really three major phases to the methodology. And I’m happy to report that the work that we did between - leading up to Senegal, to the Dakar meeting, I think has moved us way down the road in terms of this first step, this prepare step.

I think we've got a little bit of work that we might want to do but I'm not sure because it - as I get deeper into this I think that the actual work/work just repeats a lot of the work that's in the prepare step. And so I'll have a better feel for this next week but I think we may be able to just jump right into the actual work. And we may even be able to get a fairly substantial amount of this work done by Costa Rica. I'm at least tentatively holding myself to that schedule.

So let me just open this up and show you what I've done. In the methodology each of these major tasks has a little description of what to do. And so in the identify purpose section they have a question and that is is this an initial assessment or is it an updated assessment. And then within those two questions there are some sub questions.

And so what I've started to do is extremely tentatively, only Mikey, entirely open to change I've started making guesses as to what I think our answers are. And my first round of guessing is that this is an initial assessment, it's not an updated one. And that we're in the - we're not really doing a baseline assessment we're identifying current threats, vulnerabilities, impacts and other risk factors.

This is - this part of the methodology is really aimed at the chartering group. And I think that one of the things that may fall out of this is that we'll suggest to people that they keep doing this over and over again on some interval. And the chartering group could then walk through this part of the methodology and update these things appropriately. But, you know, that's my first guess is that this is an initial assessment and we're doing threats and vulnerabilities.

Then it says well what's the scope? And in there - in the methodology they really say okay tell us about the kinds of organizations that this applies to. And that's a puzzler that I think we want to come back to. I made this up but, you know, it's an interesting question because in our charter what we say is something to the tune of do all this good stuff to the extent that it applies to ICANN's mission in maintaining the global DNS.

But I think it's safe to say that really what our scope is is organizations that provide pieces of - and then I put the DNS in quotes to sort of reflect that conversation we had about how far down the hierarchy we want to go and so on.

And so I think that we could circle back and just confirm that we're probably going to want to include at least a discussion of root server and TLD server operators and maybe even some TLD-like third level operators like some of the CCs in the scope of organizations that this work applies to.

Again all of this to be circled back to and confirmed. But I sort of want to scream through this pretty quick just to give you a sense of what I've been up to and see whether you think this is the right thing.

The next thing that the methodology calls out is essentially three tiers of essentially detail, Tier 1 being very broad, general, managerial sort of detail; Tier 2 being sort of a business unit level of detail and Tier 3 being a front line security service delivery organization like a CERT or, you know, front line organizations like the security people in a registry or something like that.

And again tentatively I'm pegging us at Tier 1 although we had a pretty lively discussion during the co-chairs' call. And we may contemplate sort of a hybrid where we do the very broad high level one but we may pick a couple topics to sort of drill all the way down to Tier 3 on.

An early candidate in that would maybe be DDoS attacks partly because it's very interesting and partly because it would give us good experience at both doing a very broad assessment at Tier 1 and a more detailed assessment at Tier 3. That decision hasn't been made yet and it's partly because I'm still a little bit uncomfortable with how well I know this methodology and whether we can actually do that. But that's the current thinking of the co chairs.

And again a third chunk in the scope question that is posed in the methodology is talk to us about what architecture and technology is in scope.

And again this is the DNS discussion that we had. And I sort of paraphrased our charter on that.

Then - and this is the part that's going to explode on your screen so let me just take this down a little bit. I got to get some mumbling in for Cheryl. There we go.

Okay so one of the things that confuses me a little bit - I haven't really worked my way all the way through this - is that this first stage almost repeats the whole - almost covers the whole methodology in the chartering mode. And it leaves me scratching my head just a little bit.

And that's why I think that what we can do is rather than go backwards and do this preparation step I think we can just dive into the actual risk assessment with a fairly sketchy job done here because I started working my way through this and you'll see that it's - eventually at the end you sort of go well wait a minute I just did the whole risk assessment; that's not right.

What the methodology does is it says okay first decision is how broad a range of sources of threats do you want to consider in your study? Do you want it to be really broad, all sources adversarial and non adversarial or do you want to really narrow in on one specific source of threats. And, you know, presumably there would be some sort of middle ground.

And as - I'm sort of putting myself in the heads of our charterers I think that they're thinking was that we in this first one would be very broad in what we did. You know, we're talking about the whole DNS, we're, you know, we really have a pretty wide range of opportunity there. And so that's my initial pick on that one and we can circle back and see whether we want to tear that down at all.

This is the one that starts to really explode. What the methodology does is it breaks - it has a sample taxonomy of threats in one of the tables at the back of the methodology table D2. And they, in that series of tables - excuse me - break this down into four chunks. They say well there are adversarial threats, there are accidental threats, there are structural threats and there are environmental threats.

And I'll just expand this a bit to give you a sense of how detailed this gets. In the adversarial threats what they're saying is an adversarial threat is individuals, groups, organizations or states that seek to exploit the organization's dependence on cyber resources.

And in our analysis one of the things that we are going to do very early on is once we've described which sources of threats we want to look at we're going to come up with an initial assessment of the - of those threat sources, capability, intent and targeting. You know, these are adversaries so that, you know, how good are they, what are they trying to do, what are they zeroing on to accomplish their evil deed.

And then they have this technology that - or this taxonomy that they split the adversaries into individuals; outsiders, insiders, trusted insiders and privileged insiders which is - those last three are sort of a taxonomy of, you know, how close to the core operation are these people.

And then they put all other threat sources that are adversarial in a group category - ad hoc groups that just form casually, established groups that are sort of missioned to do this, an organization that's actually formally out there and then a nation state.

And so you can see from my little green work that I don't think that our threat sources - this is just a preliminary thing; we can go back and fix this. But I don't think that we've seen a lot of insider action in terms of threats. So I took this as an opportunity to show the kind of choice that we might want to make. But again it's all - it's all on the table we can circle back and change all this.

On the accidental front I left this one out. I decided that most of the things that we tended to look at aren't accidental. And we can certainly come back and change this if we want.

But, you know, these are just errors. You know, I can remember back in the old days somebody would mis-configure their router and it would start flapping and pretty soon, you know, the Minnesota regional network would fall down. And, you know, I think that's the kind of thing that's going in here.

And in terms of the whole DNS at least thinking back to our conversations I haven't seen a lot of those. But if we find one this is where we would put it in the taxonomy.

Structural threats are the equipment stuff. And again this methodology is pretty good. It comes with an awful lot of definitional words and phrases which I think makes writing our report a lot easier because while I think we will probably want to go through and edit some of these at least we've got the starting point for some words and phrases that we can put in our report.

And again I made some guesses that to the extent there are structural problems they tend to fall in the storage processing communications kinds of gear rather than displays or sensors. You know, sensors and controllers strike me as more of a process control system failure, a SCADA system failure, something like that.

Same with environmental, I sort of left that out. I thought that most of the things we talked about tend to not fall in there. And then we seem to have a lot of conversation in our existing work about software errors in mostly, you know, the DNS software. And I didn't know exactly where to put that in there so I sort of threw them all in. I think that we probably will wind up narrowing that down a bit as we go.

And at first I was thinking that I would staple all of our work into this part of the document but I've pretty much convinced myself that we can go through at this level in the preparation and just highlight what we've already done. And because the actual methodology we're going to drill into this as you'll see in quite a bit of detail.

And then finally this is the final one, natural and manmade disasters. And they get pretty excited about making distinctions between fires, floods, hurricanes, bombings, etcetera. I'm not sure that we will want to go into that much detail.

And then I left sun spots out although I'm not sure; we can - there may be a debate there. And then infrastructure failures; we did have some conversations about that so I left those out.

So that's kind of the taxonomy of threats. And you'd be surprised how well the work that we did fits into this taxonomy. I haven't mapped it yet but I'm pretty comfortable with the way that it's going to turn out.

Then we get into the actual threat events. Now remember the first part was the sources of the threats. Then we get to think about what the actual threat events are.

And again in this preparation phase the methodology is saying okay you project charterers determine what level of detail you want to go into because if we're very broad and we also go into a great deal of detail in the threat events we can wind up with a gigantic number of threat sources and threat events to evaluate. So they're sort of saying be careful how detailed and granular you get when you go into the threat events.

So the way I reminded myself of that was I said well for sure we're going to want to describe the general ones, phishing, DDoS, so on, that's certainly the level at which the work we've done so far is at.

We may want to get a bit more descriptive at least on some of them, for example DDoS, and that's why I made that one light green. And I think that if we went down to the most granular, you know, names of systems, the actual technologies, the actual organizations at least in this first round that we might retire before we got this project done.

And I think that we might do a much greater good to the community if we did a first pass at a pretty high level and then in the process of doing that identified some places to drill down maybe even drilling down a bit. But again this is all subject to debate.

To show you how detailed this could get - brace yourself - this list was spectacular. This is an alphabetical list. I'm just going to scroll by, I'm not going to - we are not going to go through this in any detail.

But as I started reading this I started saying, you know, somebody wrote down every conceivable threat event and put them in this list. And it would have been nice if they'd put some in some clumps because they didn't; they just put them in an alphabetical order. And it is pretty tough to use. I think if we want to go to this...

((Crosstalk))

Cheryl Langdon-Orr: ...not a librarian trained one.

Mikey O'Connor: Yeah, just one more layer would have helped because...

Cheryl Langdon-Orr: Yeah.

Mikey O'Connor: ...this is - I think a great resource. I don't want to in any way say this is not good stuff or useful. But it would be a lot more useful if they'd just given us a little bit more taxonomy help.

And so if you're ever looking for a list of threat sources I heartily recommend this table; it's a great list. You can see that somebody has put an awful lot of work into this. And the nice thing about it is that as we get close to one of these we've got a pretty good set of language that we can use where, you know, somebody has already thought through these things and written them out.

So I loved it for that. But in terms of way it's organized it's pretty overwhelming. So...

Cheryl Langdon-Orr: We get to tweak it that way.

Mikey O'Connor: Yeah we do. And I think that we...

Cheryl Langdon-Orr: That was Cheryl for the record, by the way.

Mikey O'Connor: Yeah, I think at a minimum we got to tweak it. And I also think that tweaking may be a great good for the whole rest of the Internet community because I think it would make it a lot easier to use. So anyway that's that. And that gives you a sense of the resource that we've got going into our analysis.

Now to contrast the non-adversarial threats that's it; that's all they've got. And here I think it's a little sketchy. I don't think this is quite at the level of detail that we want to go. So it's sort of, you know, I chugged my way through that first giant list; it took me a couple hours to pound that into this spreadsheet thing. And I was not looking forward to this one. And I went oh a gift. This one I can do in 10 minutes.

So the nice thing about this is that it - both of these give us a really good starting point and a good framework for discussion so I like them a lot. But, you know, I think that the work we've done is great. We may want to revise our taxonomy a little bit to fit into this but other than that I think that the work we've done is terrific here.

And then finally one of the interesting questions that the methodology raises is whether we want to review only threat events that have been seen in the wild that people have actually experienced or whether we want to go into all hypothetical threat events.

And again on a preliminary basis I thought that our first pass it might be a good idea to just stay with things that have been seen. But you can see why I'm constantly saying we probably need to take a look at this and make some choices.

I'm conscious of the time so I'm going to push a little bit faster through the rest of this. They have the same - you know, once you've got these threat sources and threat events then they've got another nice list of vulnerabilities.

And it's the same sort of thing. The work that we've done is - fits nicely in the taxonomy that they've identified. But they have got a table that has a pretty good - this is a little; let me just shrink down one layer of detail here.

Basically the - their taxonomy is pretty close to ours. They start with sort of the detailed technical stuff. They talk about the kinds of, you know, the ability to handle information. And it's - then what they go into is technical vulnerabilities.

And again when they put examples out there I made some guesses as to what I thought our focus would be. They confused me a little bit with these descriptions. And so for those of you that have used these methodologies before as we get into this phase of the work at least I could use a little schooling on how they mean these words because I did emerge from this part of the summarizing a little bit confused about what they meant.

But I did, you know, knowledge - lack of knowledge is never a barrier for me; I go ahead and make guesses even when I don't know what I'm doing and so these are the guesses that I made.

And then finally I really got confused on this one and so I didn't make any guesses I just put it in. And again rather than do this once in sort of a preliminary mode I decided we might want to just dive into the analysis. And so you can see sort of how this works. I'll post this whole hierarchy out toe the list so that you can see. Whoa, hold on a minute.

So the next stage is to walk through sort of the impacts of this series of threats and, you know, we have a threat source, we have a threat event, we have a vulnerability. Who gets harmed? Is it just within the organizational constraint? And again we have to go and define who those organizations are, in other words is it just within ICANN and providers of TLD and root services? Is it other organizations too? And/or is it the nations and the world? And in each case what kinds of harms are affected there.

And I - at this point had stopped. I was just - I was running out of time to get this call prepared for so I haven't made any guesses from now on. But I think that during the analysis we get to make those choices.

I think - just personally - that we've probably got harms happening at all three of those levels. I think if the DNS, you know, goes away that's a worldwide harm that's not just a harm to ICANN or the registries and registrars. But we have that bridge yet to cross.

And here are - again they have some representative samples that we can take a look at in terms of the kinds of harms that happen. And again the nice thing is that we - it's a multiple choice test rather than having to invent all these things ourselves. I feel a lot more comfortable that we will have covered a lot of the bases when we get through all this.

And I think we can very safely go back to the community and say look we've - we may not have got them all but we sure got most of them because we had this preexisting guide to go look at. So - and this I don't think we've done much on at all. I think we get to do this in the analysis.

Okay that was a mouthful and let me shrink back to one of - getting close to the end of the preliminary thing - one of the things that they suggest that charterers do is they identify where the information that we're going to use comes from.

And I think that it's safe to say that most of our information is going to come from us and that we are a cross community organization. We may want to reach out to some other ones as we go.

We may want to - especially when we - if we get into a more detailed one we may want to dive into the internal records of some of our organizations, ICANN, IANA, some of the big registries and registrars.

And I'm - I think that this is the kind of information that our confidential information process is going to be really helpful for if we decide to get this detailed. So I was just looking at that and going oh another piece of work that we can use pretty much without modification.

And then finally I got to the end and they said define the risk model. And I just burst out laughing. When you get to this part of that section it's the sketchiest paragraph I've ever seen. It was basically one sentence long and basically they say a miracle happens and you figure this out on your own.

I'm starting to get a feel for what they mean from the actual work plan that's coming up. But I think they were working on a deadline to get this document out and they just skipped this. So...

Cheryl Langdon-Orr: Could be the draft.

Mikey O'Connor: You know, it was good. Everybody needs a chuckle every once in a while and this is what gave me a chuckle on doing this work. So that's the get ready work. And I'm - as I've been saying over and over again I think that the work that we've done although it certainly wasn't organized this way it covers a lot of these bases pretty well.

And so I went ahead then and pounded in the actual work to come. And I'm - for today's call since we're getting pretty close to the end I'm going to just focus on the first task in the actual assessment because I think this is the work that we do first and that's to circle back and, you know, identify these threat sources.

And so the first thing is in each of these tasks they have like many methodologies they have a - before they actually launch you on the work they say well here are the inputs that you need in order to do the work so make sure that you've got these things handy before you actually start working.

And they run back up into the earlier tests and they say well do you have your information sources? And I think the answer is yes we do; we have us. I think we, for this first round, we are the information sources.

The next one is that taxonomy of threat sources. And I think we have got some tailoring that we need to do to that one. I think that's our first job is to narrow that down. And I stapled that whole table back in, adversarial, accidental, blah, blah, blah. I think this is where we are. I think...

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: ...we need to tune this up, make sure that we are comfortable with the work that we've done, make some, you know, understand where it fits in this taxonomy. I think it'll go pretty quickly but that's clearly the first job to do.

And then we dive into this business of for the adversarial threat sources understand their capability, intend and targeting and for the non adversarial sources describe the range of affects of those events - the accidents and floods and tornadoes and so on.

What that produces is, you know, remember these are inputs. And this is where we get to do the remedial work. Now that's - when I discovered this is when I realized that we didn't need to go back and actually finish that preliminary work because they give us a chance to finish it at each stage along the way.

Once we've done that which I think we can do pretty quickly then what they are driving us towards is really two tables. And you will remember that for the last several weeks we've been working on that worksheet of mine about threats. And you'll note that it's dropped off of the agenda and it's because these tables make arriving and that destination much more logical, much easier to do.

So I love the work that we did on that table. And Cheryl I think has added something when - on the last call when she talked about a column that we would add that talks about in addition to the effectiveness of the controls also assess or at least guess how capable the organizations out there are of actually doing it, you know, how even, how uniform is the implementation of the controls.

So this is part of the tailoring that we get to do. And part of why I love what we did on that worksheet. But I think we have to step back from that and do this a step at a time. These two tables are the first step. And the headings on the table are the same. Well they're not the same; they correspond to the work that's up above them.

So, you know, there would be a column that says here are the threat sources then there'd be a column beside that threat source that says well where did we identify that threat source. Do we feel that threat source is in scope or not? And this is where we could decide, you know, this is where we document the scope boundaries discussion that we've already had.

And then we would do those three capability, intent and targeting exercises and put those in subsequent columns of that adversarial table; this first one here. And then in the non-adversarial threat sources we'd do the same thing; we'd run through all the threat sources that we've identified, we'd say whether they're in scope or not and then we'd describe the affects of those. And we'd then be done with this first step which is identify our threat sources.

From there in the interest of time and I apologize profusely to having given you a 50-minute lecture. But I think it's useful to sort of have that background as we decide on a preliminary basis sort of once and for all whether this is a methodology that we're comfortable with and whether we want to use it.

So the rest of these basically keeps building tables on the tables that we've already built. You'll note that I haven't documented them because I ran out of time. That's another reason why I'm stopping here. But I will.

And as I get deeper and deeper into this I'm feeling more and more comfortable that this is at least an adequate methodology for us to use. And I find a lot of things in it pretty helpful.

So with that I'm going to stop ranting at you and let you talk for a while and just see if we can sort of arrive at a sense of this group as to whether this is the way that we want to proceed and if so then I'll go ahead and post that to the list, encourage discussion for a week and then we'll circle back to this discussion next week having given people a chance to think about it.

And if we're still okay with this go ahead and formally arrive at consensus on this and then drive right into that task 2.1 that I just described this one here. So I'm done. Any thoughts, comments? I'm all ears.

Jim Galvin: Fabulous, Mikey, just fabulous.

Mikey O'Connor: Thanks Jim. That was Jim Galvin.

Jim Galvin: Just echoing what Patrick Jones said in the chat room.

Mikey O'Connor: Oh I haven't been watching the chat. Thanks Pat...

((Crosstalk))

Cheryl Langdon-Orr: That's because you've been lecturing us, Mikey, but...

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: ...we were complimentary.

Mikey O'Connor: Yeah thanks.

Patrick Jones: Yeah, I just said nicely done for translating it into this. It's really - I wish other documents were explained this way.

Mikey O'Connor: Well, you know, I have to admit that there is almost nothing original in this mine map. But, you know, all these words and phrases are in that sequence in that structure in that document. I didn't change anything. But it's so hard to read because they have these huge paragraphs where it's one giant blob of very wordy text.

So I did two things, I broke it into pieces like this and I took about half the words out. And it just makes it, at least for me, it makes it a lot easier to understand what they're doing. So I’m glad that people are comfortable with this and - well with my homework.

Anything else? Any other thoughts? If not I'll - I haven't got anything else for today - I'll go back and finish the rest of the tasks and sort of get the word out on the list and post all this to the wiki and so on.

But again I think - and I think the co chairs will echo this - we think this is a pretty important part of our work and I think a big contribution to the community just picking this and sort of laying out this work this way. So we thought it was worthy of a consensus conversation because of all that.

Okay I won't belabor it but I'm interpreting this...

Cheryl Langdon-Orr: Oh good.

Mikey O'Connor: Oh good. Okay. Any other business other than that? Otherwise we'll let Cheryl get to bed. I'm also conscious of how late it is for her. And I'll see you all next week. And I'll see you on the list. That's it for me.

Cheryl Langdon-Orr: Fantastic. Thanks, Mikey.

Mikey O'Connor: All right then.

Olivier Crépin-LeBlond: Thanks.

Jim Galvin: Thanks again, Mikey.

Mikey O'Connor: Nathalie, I think we're done with the recording. Fabulous job as always. Thanks again for shepherding our call so well.

Nathalie Peregrine: Thank you, Mike. (Tim), could you please stop the recordings? Thank you.

Coordinator: Certainly, one moment please.

END