Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
23 February 2012 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 23 February 2012 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-20120223-en.mp3
Presentation will be posted shortly on:
http://gnso.icann.org/calendar/#feb

Attendees on the call:

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

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

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

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

SSAC Members
. Jim Galvin (SSAC)

Experts

ICANN Staff:

Julie Hedlund
Glen de St Gery
Patrick Jones
Nathalie Peregrine

Apologies:
Greg Aaron - (RySG)
Don Blumenthal – (RySG)
Sean Copeland, .vi
Bart Boswinkel

Coordinator: Please go ahead; the call is now being recorded.

Nathalie Peregrine: Thank you, (Tim). Good morning, good afternoon, good evening. This is the DSSA call on the 23rd of February, 2012. On the call today we have Rafik Dammak, Mikey O'Connor, Cheryl Langdon-Orr, George Asare Sakyi, Andre Thompson, Olivier Crépin-LeBlond, Rosella Mattioli, Jim Galvin, Jörg Schweiger, Takayasu Matsuura and Katrina Sataki.

From staff we have Patrick Jones, Glen de Saint Géry, Julie Hedlund and myself, Nathalie Peregrine. And we have apologies from Sean Copland, Greg Aaron, Don Blumenthal and Bart Boswinkel.

I would like to remind you all to please state your names before speaking for transcription purposes. Thank you and over to you.

Mikey O'Connor: Thanks Nathalie. For those of you who are on the call you do not know the magic that Nathalie does to get this call working. And so I'm always in awe when this all works right.

Before we go on just a moment to give people a chance to update their statements of interest if there are any changes? Okay.

We've got a seemingly quite short agenda but I think we're going to cover a lot of ground today. And I'm pretty excited about this. The ops group had a very I think intense, lively, productive discussion on Monday. And so the first

agenda item is to sort of walk you through the conversation that we had and then actually do the analysis that we think we need to do.

And then - I'm not sure that we're quite ready to do the meeting schedule but we'll probably at least briefly touch on the meeting schedule for the DSSA in Costa Rica. So there's not a whole lot on the agenda in terms of number if items but I think quite a lot in terms of what we're going to cover.

Is there anything anybody wants to add to the agenda before we dive in?

Okay on your screen you see the newest version of the threats worksheet that we're going to be using. And there are several things that we want to highlight and there are actually two pages to this that I'm going to go through.

So I'm going to start with I think the most important part of the conversation that we had on Monday. For those of you who have been on recent calls you know that we're still struggling a bit to try and nail down the framework of this analysis.

And I think we had a bit of a breakthrough on Monday when we realized that our threat events list is too long. And so the one - the old list one is the one that we've been working with for quite some time. And the new one at the bottom, as you can see, is quite a bit shorter because what we realized is that we're combining a lot of stuff in our threat list - or at least our old one.

One of the things that we're combining is essentially the issue that Jim mentioned on the last call last Thursday but we picked that thread up again on Monday and that is that for any given - for people who use a given zone file no matter how big it is from the smallest, newest, most narrowly-focused gTLD all the way up to the broadest zone files of them all if that zone file fails for some reason, if it doesn't resolve or it's incorrect or its security is compromised, that is a catastrophic event for the people in that zone.

And so what we've been doing is trying to work our way around that dilemma in the way that we describe the threat events. So we have the business of global versus lesser zone files and we have major DNS SEC providers and, you know, etcetera, etcetera. But in fact what we have in this analysis is really three threat events which is that new list at the bottom.

If a zone file doesn't resolve, it's incorrect or its security is compromised. So those are really the three things that our charter has us looking at. And all of the things that cause that are vulnerabilities, weaknesses in controls, etcetera, etcetera.

And so what we've concluded - and I'm now going to switch to the scales page for just a minute - is that - and here's the note that summarizes really. I'm going to pull this out because it doesn't quite fit on the page. It still doesn't. I got to do a little mumbling for Cheryl.

Cheryl Langdon-Orr: Yeah, that's important.

Mikey O'Connor: Yeah. Yeah, I - you know, I've been falling down on that, Cheryl and so I...

((Crosstalk))

Cheryl Langdon-Orr: I have been taking notes, Mikey. I was going to bring it up in the final reporting but...

((Crosstalk))

Mikey O'Connor: Yeah, yeah well, you know, I'm feeling better now that I'm back to mumbling for you.

This is the note that covers the comment that I was just talking about. And this is I think a crucial observation for our analysis that what we're focusing on is that Internet-wide type failure. And the reason that we're focusing on

that is because that's really our charter. But we want to acknowledge that for the users of any given zone these failures are likely to be catastrophic.

The other thing that we observe - at least we observed on the ops call - and we want to confirm with you is that in the worst case, which is really what we I think need to focus in, all three of those threat events are catastrophic failures.

And I think that really what we want to do today is confirm that with you and then essentially put the threat event subject to bed and get into what we really think is the meat of the analysis which is the vulnerabilities that lead to it, the threat sources that exploit those vulnerabilities, etcetera, etcetera.

But we want to confirm this idea with you all today on the call. And then if there's agreement we'll essentially put the threat event topic to bed; we'll confirm it for consensus on the list on the next call, etcetera. But we think we're getting pretty close to nailing this one down.

So let me just walk through the tables. I think we've gone through these before but let me just go through them again. There are really three dimensions to the scales that we want to use to evaluate these threat events.

There's the kind of damage that's done when the threat event happens. And the highlighted part of the screen lists at least in very broad categories the kind of damage. And in a failure it's possible to have all of these happen at the same time.

And the next scale is the severity of impact scale. And it's saying in the worst case a 10 would be multiple, severe, catastrophic, adverse effects from this previous table. So a 10 would be if catastrophic versions of all or some of these happen, multiple effects, all the way down to a 1 which would be hardly any of those effects.

And then the final scale is this one that says what's the impact on the Internet? Not within the TLD but on the Internet as a whole for the failure of a given zone file. And that's the table that we've been having so much trouble getting our arms around.

And I think we've arrived at the way to sort of break through that trouble when we talk about this note that we will include in the report which is that we're really talking about the Internet-wide impact not the impact within a given zone.

So I've sort of rambled on for a while. I want to give the other folks on the ops team a chance to chime in with course corrections to what I said and clarifications if I've muddled anything and then spend some time with the whole group sort of working through this to make sure that we're on the right track. So any members of the ops team want to chime in with that? Jörg is saying that I did okay.

Jim, I know this is a topic that's near and dear to your heart; do you think I got it right this time?

Jim Galvin: I'm - thank you, Mikey. This is Jim Galvin for the transcript. But, no, I'm actually much more comfortable with where we're headed and what we're doing now. So I'm very interested in what others thing and how this is - about how this is shaping up so I'm good for now and let's hear what others have to say.

Mikey O'Connor: Okay. Olivier, I'll put you on the spot too just - I just want to make sure because this was a very, very, you know, if you want to listen to the transcript of a really great working group call go listen to the ops call from last Monday. We worked really hard and I think did a great job so I think we're pretty comfortable. And I mostly want to make sure that I've done a good job of describing where we arrived at.

Jim Galvin: So, Mikey, this is Jim again. Jacques got a question in the chat room asking about what, you know, what does greater than 1 million end users really mean. And I'll take a shot at answering that question and observe that scale - they're really just intended to be representative.

I mean, it's just a question of how to judge the effect of a particular threat event. And so to a first order some of those numbers there are just arbitrary; we just sort of stuck them out there. We can certainly make them anything that seems more appropriate or more reasonable to people. Just sort of trying to give a target point that seems to reflect a sensible scale.

So that's my answer to Jacques's question.

Mikey O'Connor: And I totally agree. We were - that was sort of an intermediate stop along the way to our final destination. And we were really using it to describe to ourselves and to everybody else this scale. Any other thoughts? I'll open it up to the whole group. Does this seem like a...

Olivier Crépin-LeBlond: Mikey, it's Olivier. You asked me earlier...

((Crosstalk))

Mikey O'Connor: Okay.

Olivier Crépin-LeBlond: Thanks for going through this. I think it's a lot - probably be a lot easier. It removes some ambiguities as to what we were doing previously. And certainly removing the ambiguities provides for a better, more stable answers I hope. So I'm all for the process now.

Mikey O'Connor: Great. Let me open it up to the whole group for thoughts, reactions, comments, course corrects, etcetera.

Jacques Latour: Hi, Jacques here.

Mikey O'Connor: Go ahead, Jacques.

Jacques Latour: So, yeah, I like this. It's like Olivier said it takes the ambiguity out. And the scope is on the whole Internet versus thinking of it specifically around domains or - I like it.

Mikey O'Connor: Cool. That's great.

((Crosstalk))

Mikey O'Connor: Cheryl, can I put you on the spot? I'm just curious what your reaction is. I count on your opinions a lot so.

Cheryl Langdon-Orr: No I'm happy.

Mikey O'Connor: Great. Well good. Sort of a last call and then I think what we're going to do is almost a pro forma vote...

Mark Kosters: Hey Mikey?

Mikey O'Connor: Yeah, go ahead Mark.

Mark Kosters: So this is Mark Kosters for the transcript record. Yeah, do you want a contrary view?

Mikey O'Connor: Of course.

Mark Kosters: I think that given the oscillations that could occur depending on the threat event and who's impacted, what zones are impacted, what the threat is that we can oscillate so much that we'll confuse everybody. And I said this before on the ops list. I just think listing the threats and leaving them along is good enough.

Mikey O'Connor: Oh rather than evaluating these scales?

Mark Kosters: Yeah, yeah.

Mikey O'Connor: Contrary view duly noted and I think in this particular case unless there's overwhelming support for Mark's view I'm going to push back that I think that what we need to be able to do is describe the impacts of these events.

Mark Kosters: You wanted a contrary opinion and I gave it.

Mikey O'Connor: I know. I sure wish you could have been on the ops call. Mark was on a - I think you were on a plane weren't you or something - had some spectacular...

((Crosstalk))

Jim Galvin: So I have a question for Mark.

Mikey O'Connor: ...that he couldn't - oh a vacation day or something. I don't know anyway.

Jim Galvin: So this is Jim. I have a question for Mark. You were talking about listing the threat events and not having a scale but it's not immediate obvious to me which scale you're talking about setting aside.

Mark Kosters: All these tables in terms of the damage it caused, the severity of the event, the effects.

Mikey O'Connor: You know, to take your point a little and treat it with a little bit more care than I did the last time. So the thing that I did to address that issue, Mark, was I made these - the worst case impact so that we could finesse the issue of - because, you know, the problem of it depends on the zone is a big one.

And that's the...

Jim Galvin: See, so, Mikey, this is Jim.

Mikey O'Connor: Yeah.

Jim Galvin: You know, you're falling into that trap again which is...

((Crosstalk))

Jim Galvin: ...the one which I think has been...

Mikey O'Connor: That's why I needed you guys.

Jim Galvin: ...which is the one I think, you know, it's been bothering me along on these discussions and why I'm just - I'm listening to Mark and I think I hear where he's going.

You know, to some extent I don't like these scales either. And I don't like the whole voting business because I think if I were to interpret what Mark is saying and the thing that I like about it is that the problem with each of these threat events is there is a range for each of them which one can accommodate in pose - in prose, rather - but it's much harder to get all of that information when you're looking at these votes.

So you're right, you put the scale up here as a worst case effect and so I've acknowledged that that's interesting and so I kind of went quiet and said okay this is getting more comfortable for me, you know.

But Mark's bringing up the point that I also was trying to make on Monday which is, you know, to some extent you have to look at these things in terms of the number of users affected or better put the user community that's affected.

This goes to the note at the bottom, right.

Mikey O'Connor: Right.

Jim Galvin: A zone file going offline is always a crisis for the users of that zone or in that zone but it might not matter a hoot to the Internet.

Mikey O'Connor: Right.

Jim Galvin: Okay. And it's a little hard to get that fact out of these votes that we keep taking. And that's where my comfort level is, you know, I get uncomfortable. Whereas I think if we were to write prose and talk about the range of user communities and now I'll put out here the one thing you don't have here that I did talk about on Monday which is I think there's always at least three user communities that one has to evaluate these threats against.

There's the users inside the zone who have registrations in there. There's the users who might use the zone and be directly related to it. And then of course there's the broad Internet community. You know, dotCom is sort of always the special case in that the user community for it is really always the entire Internet.

But for most country codes, you know, the people inside the zone they care a lot. There's probably some number of people in the regional area that care. And for the rest of the Internet probably doesn't matter that much. And I think that that's a subjective evaluation that applies in most cases and for most of these threats.

And I think that's what Mark is reaching towards. And he can correct me if I'm wrong; I don't want to put words in his mouth. But that's what I don't like about these votes is it does not actually gather all of that information. Thank you.

Mark Kosters: You said it really well, Jim, thank you. I guess, you know, when we were starting to go through this, Mikey, I was always like okay, I'm not sure if I like this. And I was willing to go along just to - because maybe I can learn something from this and maybe this is a useful exercise. I just - I keep in getting confused. And to me that's not a good sign.

Mikey O'Connor: That is a good sign.

Mark Kosters: Oh it is a good sign? I get confused, oh that's fine.

Mikey O'Connor: That's a good indicator that we're not quite right. Sorry about that.

((Crosstalk))

Mikey O'Connor: ...the sense of that. Here's the thing that I would say to respond. And that is - well several things. First of all I will not cling to this with my dying breath; this is not a pry these scales out of my cold dead hands kind of sentiment on my part.

I think the thing that's useful about this is the notion that we are slotting this analysis into a repeatable process. And what we're using is a repeatable process that we got from NIST and that we're, you know, as we go we're heavily tailoring it.

If we can arrive at a way to tailor that methodology so that it works for us given the extremely unique problem - puzzle that we're trying to solve it gives us the ability to hand on to the next generation of people who do this work a framework that's been hammered on pretty hard that works.

And so, you know, that's the reason that I keep banging away on this. You know, we could certainly make these points in prose. You know, we could essentially take all these words and stuff them into paragraphs zone file by zone file if that works better for you.

But I think the framework is important because it makes the analysis refinable, improvable, repeatable...

Cheryl Langdon-Orr: And understandable.

((Crosstalk))

Mikey O'Connor: Yeah and - take it away, Cheryl. I'm sorry I wasn't looking at the queue.

Cheryl Langdon-Orr: No, no, Mikey, I think it's important that we realize that the methodology used here and tailoring it to our own unique, as you suggested, needs is hugely important because that brings us the ability to have some benchmarking, some compare to what type scaling.

That doesn't mean that we can't use prose as well; they're not mutually exclusive systems. But one is the skeleton and the other is kind of a, you know, the pretty outfit that's put on the outside of the - what covers the muscle.

I'm less concerned than Jim is. It's not that I wouldn't want to have prose but as soon as we get into prose we have the equally significant criticism of how does that allow us to compare and react to changing state?

So it's back to - it's as good as a traditional nature and nurture argument, the value of qualitative versus quantitative data points. And I think to have the highly quantitative data points is what many people will be relieved about seeing in the output that we can manage with this.

That's not to say that the qualitative stuff is to be ignored. I think we probably should be heading towards (unintelligible). And I think the ability to have and the following notes are relevant in type riders over and over again really important.

But we keep also needing to I think remember that whilst this is a system that we're looking at right now and we can make the of course these special cases dotCom that's the snapshot for now. We don't know nor can we predict without some sort of quantitative measures, which this does give us, tied to repeatable and trackable criteria, which this does give us, what it might be in an expanded world of TLDs.

And I think we need to be really careful that we get the foundations right. So my comfort is still very high with this. Put more qualitative stuff around it? Sure, no problem. Thank you.

Mikey O'Connor: Thanks, Cheryl. Just a note from the chat and then I'll turn it over to Jim again. Rosella wrote, "I agree with Mike and Cheryl. This is the first of a periodic risk assessment of the DNS. Maybe it is taking a lot now but if we build the fundamentals well we will have fundamentals and metrics for the future."

And then Jörg mentioned, "I doubt that prose would be clearer or (can't) or have to be interpreted."

And, Jim, back to you.

Jim Galvin: Yeah, I was just - this is Jim Galvin for the transcript. I was just going to observe that although I do still, you know, feel somewhat strongly about what we've been talking about here and agree with Mark, you know, prior to Mark speaking up and making this a topic of discussion, which I do appreciate, I was okay with going forward with what you had proposed here.

You know, I think this is an improvement over what we've been doing; I really do. And focusing it on worst case severity and worst case range is, you know, something. And I understand the need and desire to want to have a

repeatable process. And doing it in this way does give us a repeatable process.

And I'm personally, you know, willing to go with this for a little while and see where this takes us and how it goes. I am kind of anxious for us to begin to produce a document and that's what I mean by prose, you know, let's produce our output and begin to look at it because I think that's where we're actually going to have to expand or back off depending on your point of view on this, you know, worst case analysis voting.

But I'm willing to give it a chance and wait and see how it goes. You know, I guess at this point I've just kind of gone on record with what my concern is and what makes me a little bit uncomfortable. But I'm not going to fall on my sword about it just yet.

Mikey O'Connor: I would offer one option to consider. See if this would help. And that is we could evaluate more cases than just the worst case. You know, we could pick representative cases of the types of zone file and evaluate their impact.

I captured your three-tier scale. And you're right, Jim, I - you always say it when I'm not in note-taking mode and so I finally captured it. And that is that there are really three tiers. There are the people who are essentially inside the zone. There are people who have sub-domains and use them within the zone.

There are people who use that zone so they're perhaps outside the zone but they go to sites that registered within it. And then there's' the Internet as a whole.

So what we could do is we could take a representative sample of zone files ranging all the way from the root through major ones like dotCom, through country codes, through, you know, generics and we could evaluate a few of them on these scales to flesh that out.

And that might be a useful way to give this a little bit more texture than simply splashing the whole discussion into the worst case. What do you think of that?

Jim Galvin: So this is Jim. My concern with that is the amount of time that it might take if we get too into that. I would almost rather do what you have here and try this for a few weeks. And then when we're having our face to face meeting in Costa Rica, you know, we can have another call like this one, another meeting like this one, and reevaluate and maybe try what you just proposed here.

Let's dig in a little bit on a couple cases and see what that does for us and see where that takes us. I am actually being a little sensitive to the fact that we've been in existence for, you know, roughly a year and, you know, we're still in this analysis phase. And while I realize that the work takes what it takes that's still kind of a long time.

And, you know, I don't want to do anything right now that's going to slow us down tremendously.

So we've made a change to our methodology just a little bit of one here. And I would prefer to just see us pick up and go with this and see where it takes us.

Mikey O'Connor: Fair enough. I think that where it will take us is essentially this evaluation becomes almost pro forma because I think what we do is we say okay in the worst case these are all tens these are all bad.

And in way Mark that gets back to the view that you've got which is we're just listing them, there's three of them and they're all really bad.

And now we need to dig in to why are they bad, where does the threat come from, what are the vulnerabilities et cetera, et cetera?

And so in a way this is accomplishing I think where you're headed which is putting the discussion of type of threat event behind us and getting on to the causes and cures in a really because basically we...

((Crosstalk))

Cheryl Langdon-Orr: Let me interrupt.

Mikey O'Connor: Pardon me Cheryl. Go ahead.

Cheryl Langdon-Orr: Risk management.

Mikey O'Connor: Risk management right. So I think that in a way we're all trying to accomplish the same thing which is let's get on to the rest of it and see if this works for us. And if it doesn't if it breaks we'll fix it.

Any other thoughts about this? I mean this is very hard work folks. And we are doing a very good job at it so I don't want to rush us out of this part of the conversation until we're comfortable that we've really gotten to the place we want to get.

I take that almost as the IETS hum and sort of do the pro forma voting which is does anybody disagree that if we take our three...

Cheryl Langdon-Orr: (Virus)?

Mikey O'Connor: ...threat events which are these three here. We basically say they're all three at the worst case catastrophic events.

There any particular - I mean I could take us through a vote if you want but another way to just say it is are we agreed that on all those scales if any of these things happened the worst case would be a catastrophic event?

Getting an agreement from Olivier. Maybe we just do the tick marks. If you think that's right hit the green checkmark in your Adobe Connect thing and we'll consider this done.

Mark Kosters: Hey Mikey.

Mikey O'Connor: Go ahead Mark.

Mark Kosters: What does zone file does not resolve? Is that does not load because it...

Mikey O'Connor: Greater minds than mine have to explain that one. I'm throwing the ball the Jim.

Jim Galvin: Thank you Mikey. I just kind of allowed the ambiguous terminology. But I guess in the spirit of being precise it really isn't about the zone file resolving. It really is about the zone.

You don't really talk about files that don't resolve. It's about whether or not the zone is working. The file is what builds the zone. I just kind of ignore that extra word there.

Mark Kosters: Oh okay.

Mikey O'Connor: I almost took that word out this morning. So I'm really glad you caught that Mark because I was thinking that zone itself might be a better term. Let me...

Man: Now I'm not so sure I would say zone file security is compromised. Zone is compromised well...

Man: That's (Andrew)'s...

Man: ...never mind.

Man: ...so I'm okay with that.

Man: Yes okay. We're good then. Thanks.

Mikey O'Connor: You want file back in there or not?

Man: No, no.

Mikey O'Connor: Okay. So this is the new version?

Cheryl Langdon-Orr: Can I share with you?

Mikey O'Connor: Go ahead Cheryl.

Cheryl Langdon-Orr: Yes. I think what's important too is we're sort of at this point in the digging through the trenches and I think it's important that we dig through the trenches albeit in a timely and efficient manner.

We do need to realize that, you know, when we get through all of this quagmire and start putting, you know, the pros and the reporting together we still are going to be looking at - gee I'm trying to find a term that works as a good metaphor.

We're still going to - there's a difference between a helicopter view and the deep and meaningful analysis. And all of those lines have to be attended to.

But some of them are alarm points and trigger points. And that's very much what we need to also make a note to bring out in the pros that gets wrapped around all of this.

Let me give you an example which is in no way shape or form hypothetical. A situation where a ccTLD might be aware of a particular stress and risk is

vastly different to and then the bad thing happens. It's like waiting for that second shoe to drop.

And if for example that second shoe never drops that's fine. But if that second shoe drops and in the way of that being observed its effect on the Internet then may not be at that, you know, everyone is effected type.com area issue I guess.

But what it means is the fact that it can happen is in itself an increased threat and risk to the whole security and stability of the Internet. It's like oops there's the hole and now everyone knows about it.

Mikey O'Connor: Right.

Cheryl Langdon-Orr: And we have to always remember to pick up those threats as well.

Mikey O'Connor: Yes and that's the difference between threat events and all of the other things that lead to them like vulnerabilities, lack of controls...

Cheryl Langdon-Orr: And so it's all of these tables and like it's almost like a (Tivid) analysis has been needed as well.

Mikey O'Connor: Right. Yes and I think that what we need to set as our goal is the first time through it and leave enough tracks behind that others can come along and refine and improve that.

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: Jacques go ahead.

Jacques Latour: Hey Jacques here. There is another aspect that we need to look at when you try to figure out what the impact of an incident is it's iteration, right?

If the zone file goes down for five minutes the impact is less than being down for 24 hours a day, two day, a week, right?

Mikey O'Connor: Right.

Jacques Latour: So there's a time factor to put in for each one of these things I guess.

Mikey O'Connor: We had a actually quite productive discussion about that on the ops call. And Jim brought this example up when he talked about caching.

The fact that, you know, if a zone file is not available for five minutes the impact is probably not too substantial because in most cases it's largely cached data that's being hit anyway.

And there is a chunk of the methodology to capture those dimensions of this called pre-existing or predetermined conditions -- I've forgotten which one it's called -- where there are some things that -- well some very powerful things that are built into the architecture of the DNS that mitigate many of the risks that we're going to be working on.

And we need to identify those clearly so that we can evaluate how effective those are. So I agree wholeheartedly Jacques we do have that.

But in terms of the - I mean one of the problems that we ran into with this quagmire is that we're trying to drive too many things into one scale.

And by breaking them into different kinds of things -- vulnerabilities, pre-existing conditions, et cetera controls, and so on -- we allow ourselves more granularity and flexibility in the analysis that follows.

So by no means do I want to leave that out of the discussion but I would propose that we leave it out of the threat event discussion and save it for another one.

Other thoughts from folks? Seeing two tick marks saying we're okay at calling these pretty darn severe threat events it would reassure me if a few more tick marks went up that we're on the right track.

Cheryl Langdon-Orr: Jim did have a tick but he may have recanted.

Mikey O'Connor: Yes Jim's back with a tick. How about some of the others? How about I'd like to see...

Cheryl Langdon-Orr: (Paul) we see lot. Come on, put your money where your mouths are.

Mikey O'Connor: I suppose I ought to lead by example. I ought to put my tick mark up.

Cheryl Langdon-Orr: Look at that.

Mikey O'Connor: There we go. Now we're getting there. Patrick you're sitting there quiet as a mouse. But you have a...

Cheryl Langdon-Orr: He's pulling the staff card.

Mikey O'Connor: I know but, you know, this is kind of important and I'm going to trump the staff card with my spades. I have the ace of spades, I'm running...

Cheryl Langdon-Orr: Oh boy okay.

Mikey O'Connor: Patrick I'd really like to hear your view on this stuff.

Patrick Jones: You know I think this is helpful and that the language, the change from last week I mean I still I want to see it in practice.

But what would be useful especially for some of these other groups that are looking or even beginning their look at DNS risks the more that this, you

know, the difficulty that the group has faced in coming up with this criteria and that the different scale if that can be explained in a way that either it's the updated deck or in Costa Rica it would be really valuable to those other groups.

Mikey O'Connor: Yes I have an action item that I've been sort of saving until we've had this conversation on this call to redo the deck because clearly the deck right now is quite out of whack with what we're doing and do plan to do that.

Cheryl Langdon-Orr: The deck was okay from then - to then but this is now.

Mikey O'Connor: Yes this is now. And, you know, we work on Internet time. I know it doesn't feel like it and I know (41 brief) is a long time...

((Crosstalk))

Cheryl Langdon-Orr: Oh yes it does.

Mikey O'Connor: ...but, you know, we are doing something very hard and very important and I think...

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: ...we're doing a fabulous job.

Man: So Mikey...

Mikey O'Connor: I'm now going to...

Man: Hey wait just a question.

Mikey O'Connor: Yes.

Man: Now that it sounds like the group is recalibrating and has a scale to work from what's the sense of the timing for this phase of, you know, how long to sort through the different threats that the group wants to focus on before you've got something to either present outward?

Mikey O'Connor: I think that at least from my perspective it's the proof will be in the next, I don't know four to six meetings.

I think if we can dive down one level taking a look of vulnerabilities, controls, predetermined conditions et cetera, et cetera, and make pretty good progress there we'll be able to make a much better guess as to when we'll be done based on that six weeks' worth of work.

It's still awfully hard to predict. I mean...

Man: Yes.

Mikey O'Connor: ...if we had done the full evaluation of the pairs that we had, you know, three weeks ago that giant tall stack, just that would have taken us six months.

And so I think we just taken six months off of our schedule with this change. But it's still we're still building the airplane while we're flying it. And it's...

Man: Okay.

Mikey O'Connor: ...really difficult to predict.

Man: And now that it - what do you think is the best use of the time in Costa Rica and if I missed that conversation apologies?

Mikey O'Connor: I think that I need to think about that quite frankly. You know, I've - I'm pretty focused on this particular decision point in the process treaty if you will.

Because if in fact we are at the point of being essentially able to say these are the three threats I need to step back then and take a look at the methodology again and figure out what to do for that meeting. But I've been so focused on getting through this that I don't really have a good answer quite yet.

Any other thoughts folks? Okay I think we're call this done. We'll put it out on the list as a tentative conclusion for a consensus call next week to give folks who weren't on the call a chance to react. And we'll put this hopefully to bed next week.

The only other thing that we really have on the agenda is the schedule of meetings in Costa Rica. And I think maybe Bart is not on the call.

Julie are you still with us and do you...

Julie Hedlund: I am indeed still with you.

Mikey O'Connor: Oh great.

Julie Hedlund: Did you think that you had...

Mikey O'Connor: Do you have a gist of sort of how that schedule...

Julie Hedlund: Why wouldn't I - how could I miss this scintillating discussion?

Mikey O'Connor: Oh get out of here.

Cheryl Langdon-Orr: I'm sorry (unintelligible) hey Julie, come on.

((Crosstalk))

Mikey O'Connor: Oh get out.

Julie Hedlund: So I have the schedule of meetings in front of me that Bart sent around into the ops DSSA list.

There's no reason why we can't send this around to of course the full DSSA list and I'll take care of that.

And I have actually I think some tentative location information, tentative room locations for these meetings as well that I can include. But would you like me to run through the schedule?

Mikey O'Connor: Yes. Just hit the highlights so that people kind of know...

Julie Hedlund: Sure.

Mikey O'Connor: ...what's coming. That would be helpful.

Julie Hedlund: Right so...

Mikey O'Connor: Oh Julie?

Julie Hedlund: ...the first meeting is on Sunday the 11th and it's with the ALAC from local time 1725 to 1745 or that's 5:25 to 5:45. And Olivier had agreed to give the update there.

Olivier Crepin-LeBlond: Yes it's Olivier here. That's fine.

Julie Hedlund: Excellent. The next meeting is Tuesday the 13th of March. And that is to the ccNSO from 1230 to 1245. (Jorge) had agreed to give that update.

This - there's a note that this follows the SSR Team meeting which is at and must be the ccNSO meeting with the SSR Team from 12:15 to 12:30.

And at the time that Bart had sent this around we didn't have confirmed the agenda for when we'd have the DSSA meet with the SSAC.

But right now that looks like that is going to happen on Tuesday afternoon during the full meeting of the SSAC that afternoon. And we have that scheduled from 4:30 to 5:15 or 1630 to 1715.

And Jim did you want to give that update there or did you want Mikey to give the update?

Jim Galvin: I can give the update. That would be fine.

Julie Hedlund: Great.

Jim Galvin: And certainly I would welcome well I guess you know that's all right, now I remember. I said this before.

I would welcome some number of other people who would like to come along to give that update but we do have room constraints that we have to worry about.

So anybody who wants to come along and be a part of that should identify themselves so that we can manage numbers.

Julie Hedlund: Right because we have a room - we've asked for a room for 30 people but we'll probably have about 20 SSAC members in there so we'll have space for another ten or so.

But there will also be...

Jim Galvin: Right but I would welcome others to come along. Anybody who wants to just, you know, volunteer and say so and identify yourself so that we can just keep track that's all.

Julie Hedlund: And we'll have an Adobe Connect room and also remote access via teleconference and I'll send that around to this list as well.

And actually we have that I think for all these meetings. I'll try to gather that information and send it.

The next meeting is Wednesday. That's with the GNSO. And I'll have to get the exact time of that for you. I - that agenda is still in production.

So that meeting is scheduled to go from 2 o'clock to 6 o'clock, the GNSO Council meeting.

And I'm not quite sure yet where the DSSA falls on that agenda. And that may be a little bit before we find that out but I will include it as soon as I have it.

And then Thursday we have a couple of meetings. The DSSA meets with the SSR Team in the morning from 7:30 to 8:30 and we've noted the request for copious amounts of coffee during that meeting.

And then we also have the open meeting. It's the meeting of the DSSA Working Group but it is also open to the public.

And that takes place in the afternoon - or not in the afternoon, from 11 o'clock to 12:30. And then there's a couple of other meetings of interest that day that I'll include, the SSAC has an open meeting, and the board, the board's DNS Risk Framework Working Group - Patrick you can correct me if I've got that right - wrong...

Patrick Jones: Got it.

Julie Hedlund: ...is also meeting. So I'll include that information as well. That's all the meetings I have.

Mikey O'Connor: Terrific. Thanks Julie. I was going to ask you to do that in a Minnesota accent but I forgot.

Julie Hedlund: Oh darn it.

Mikey O'Connor: Oh dang nab it.

Julie Hedlund: You bet you I sure could of done that then.

Mikey O'Connor: Yes me too. We could've done that together. Okay that's it. Thank you very much Julie for that update. Anything else that people want to talk about on this call otherwise I think we might end just a couple minutes early?

Cheryl Langdon-Orr: Cheryl here. Julie is it possible when you send it to the rest of us lot can you make sure that Gisella Gruber has also got a copy on that because she micromanages Olivier.

Julie Hedlund: Oh absolutely. I'll copy her on it. And actually what I'll do is I'll copy - we have a secretariat email that covers Gisella, Glen, and (Natalie) and everyone and, you know, (Christina) so that way they'll all have the same update and know everybody...

Cheryl Langdon-Orr: People will (unintelligible) in line up (please).

Julie Hedlund: Right, right, right.

Cheryl Langdon-Orr: Mikey’s going to lose an awful lot of his co-chairs otherwise.

Mikey O'Connor: Yes. I tell you...

Julie Hedlund: I will do that for Cheryl.

Mikey O'Connor: Okay. That's it for me. I thank everyone who has worked so hard on this. I know it's difficult work but I think it's worth it.

And I will put my thinking cap on and build a new version of the deck and run that through the ops group and we'll check this decision for consensus on the next call. Have a great remainder of your day and we'll see you in a week. Thanks.

Cheryl Langdon-Orr: Thanks Mikey.

Man: Thanks Mikey.

Man: Thanks very much Mikey.

Woman: Thanks everyone. Thanks Mikey.

Man: Bye.

Woman: Bye-bye.

Man: Bye.

Woman: Bye-bye.

Man: Bye.

Cheryl Langdon-Orr: And (Tim) (unintelligible) you may now stop the recording. Thank you very much.

END