So the title of this session is Security Issues and we will have 2 parts in this current session. In the first part, Greg (last name) will brief us on the ICANN's strategic initiative for security and stability and resiliency. The presentation will take about 15 minutes and we will have another 15 to 20 minutes to ask questions and comment. Afterwards we will turn to Steve Crocker and SSAC and we will continue our dialogue with SSAC on root scaling study and lessons learned from this study.

I would now like to invite Greg to walk us through his presentation.

Greg:

Thank you Janis and I thank the GAC for allowing me to make this presentation. This is part of what I think is a very important interaction between the ICANN staff and its security team and the GAC given the broad range of concerns related to internet security, stability and resiliency.

I'll focus this morning on 2 initiatives that we've posted for public comment in the past month. The public comment period runs through the 29th of March as listed on the slide. Again, my name is Greg (last name) and I'm the Chief Security Advisor and head of ICANN's security team.

With that I'll press right into it and I will mention I'll also have a final slide that just gives you an update on some related activities that I think are of interest to the GAC.

So background related to the 2 initiatives, the last year but probably the last few years have seen growing risks in cyber security generally but also specifically to domain name security and resiliency. I would hope that most of the GAC members are aware of the growing emergence or depth in numbers of bot.net's out there and the size of those bot.nets probably the highest profile of those was one that was formed around something called Conficor and a set of malicious code that had disseminated itself through the internet through a number of variants.

That code specifically in some of its variants use a domain name system as its potential command and control mechanisms and therefore very much involved the DNS operators as well as the ICANN staff in the broader cyber security research community vendors in a collaborative effort to try to stop the spread of Conficor. That effort is ongoing but that effort certainly highlighted the need for collaborative response by the domain name system operators with ICANN playing hopefully an effective information sharing role in responding to this sort of threat.

Additionally, we've seen growing instances of domain hijacking through both technical and social vulnerabilities in the provisioning of domain names and therefore the ability of malicious actors to change domain names and have resolution go to the wrong type of sites. So we have growing practical security risks.

We've seen as a result mainly of these risks and particularly the Conficor situation the community calls for systemic DNS security planning and response. We held a fairly large symposium last February in cooperation with Georgia Tech where the primary resultants of that symposium which was composed of DNS operators, government officials, security people, members of large corporations that as they looked at what is weak in the security in the domain name site, the risks and the ability to respond effectively in a structured fashion was among the findings of that. And as we've done after action reports on Conficor and the dialogue is discussed with the Computer Emergency Response community, the notion of a hub for coordinating security activities related to domain name system is a pretty constant theme we've received.

ICANN as members of this committee should be well aware recently signed its Affirmation of Commitments and among the principle commitments is security, stability and resiliency. Those commitments specifically call for ICANN to coordinate contingency planning in a domain name system and we do believe that having structured response in the event of contingency is a logical portion of ICANN's obligation under the AOC.

The 2 initiatives we'll discuss today were identified in the recently concluded ICANN strategic planning process and they are listed in again 1 of 4 major areas ICANN's strategic plan is security, stability and resiliency in both the notion of contingency planning and exercising. And the establishment of a DNS SERT are specially identified in the strategic plan.

As I brief these 2 initiatives and if you read the paper associated with the initiatives and then the business case associated with the DNS SERT, they specifically identify at this point ICANN hasn't proposed a specific organizational approach nor are the resources identified to support the initiatives. It is important to note that as we look also at the operational plan and budget because these initiatives aren't currently budgeted in the ICANN FY 11 operational plan. And I wanted to make that clear.

So the first initiative, the title is System Wide DNS Risk Analysis Contingency Planning and Exercises. In my mind, these things are a netted set of activities and if you do not know what the fundamental risks are to the DNS as a system it's hard to both plan proactively and then react through a SERT to different sorts of contingencies. So it starts with the ability to understand risk, plan for those risks, practice the responses and having the capacity for a response.

We certainly envision this not as an ICANN staff driven analysis that is given to the community but right from the inception that the risk analysis should be comprised of experts and appropriate stakeholders from the community. But to do a professional, thorough job of this that it wouldn't have to be supported by professional staff and the role and vision for ICANN is staffing such an effort.

The types of things we would plan to do is establish a common risk framework. The initiative itself actually lays out some basic parameters for one to think about domain system risks. We

would believe the community needs to validate and have a common risk framework as well as conduct regular risk assessments and it was suggested that an annual cycle would be very useful. It would certainly be useful in driving ICANN's activities related to DNS security and resiliency but I imagine it can also feed governmental efforts and critical infrastructure protection efforts as well.

One of the things that it specifically calls out as a need is to create a root server information sharing system, as I think the committee is well aware. We had the root scaling study last summer and while the SSAC and RSAC are still considering the study and their findings, it is pretty clear in all the dialogue that increase information sharing among the elements of the root server operator system is a very important element of a better understanding of the risks to that system as part of the broader domain name system as well as being able to plan responses.

The paper outlines the need for contingency planning based on key scenarios. I think it's very important for the community to understand what are the threatening sorts of situations that need to be planned for and go that step of trying to do some community based planning on what at an operational level would be an adequate, so do the right thing response to different sorts of scenarios. Then as a person with a wide range of operational experiences, plans are only as good as your ability to practice and execute those plans. So we suggest the initiation of a system wide DNS exercise program. This should incorporate as with contingency planning a number of efforts that go on within the community at a number of levels from organizational levels within Registries and Registrars to national levels where there are exercise programs that involve players and domain name system security. So build on existing efforts but try to as with ICANN's role as the coordinator of DNS security and resiliency activities to meet its commitments, put those into a system wide exercise program and try to collaborate and facilitate that sort of activity.

The second initiative focuses on the creation of a domain name system computer emergency response team. We just had Rod Beckstram the CEO strongly discuss with the SSAC the utility of using the SERT label for this activity in that it resonates very easily with people, people understand SERTS and they understand the domain name system. The notion of a hub around which response activities to malicious activities and threats can be orchestrated, coordinated, facilitated is hopefully a powerful notion.

What ICANN is doing at this point is trying to outline the initial concept for what such a DNS SERT would be responsible for, its basic operational focus areas. We understand that this is a community based activity and it's trying to meet the need for a standing, i.e... 24/7 full time accountable set of actors that can response to these situations.

Having been part of the Conficor working group and still part of the Conficor working group the voluntary collaboration in those sorts of efforts is very useful, however, it is pretty ad hoc and we

believe the domain name system needs probably a higher level of standing accountable coordination in terms of the situations that might confront its security and resiliency.

Certainly this should be done in coordination with existing capabilities. If you look at the DNS SERT business case we've mapped out a number of ongoing efforts we believe will be part of the set of players that collaborate with the DNS SERT in trying to achieve what it can do to serve its objectives.

The other major point here is that while many of them, some of the operators of the domain name system are highly attentive to security, they have well resources teams; they react quickly and effectively to a wide range of situations. However, the domain name system is made up of actors that do not have the same depth of resources and experience with security and resiliency activity and one of the primary purposes of such a SERT and we've heard much from certainly regions of the world where this is more prevalent that they need assistance and this would be a place where they could reach for help and see the situations as they emerge and if they are effected by certain situations seek assistance.

The operational focus of such an operation we believe must be determined in collaboration with people who both operate the system as well as those who currently provide cyber security and domain name system security capabilities. We actually plan a workshop where we bring all these people together and define operational requirements in the procedures for collaboration relatively quickly as part of working out how this will work and being very specific about that.

Again, it's listed at the bottom of the slide. This is more fully developed in terms of an initiative in the DNS SERT business case which is posted for public comment at this time as well.

The way forward, we are very much in that portion of the ICANN process where for the reason explained we've tabled these initiatives for the community to consider and we are seeking actively public feedback. We already have done some consultation. We had a call with a number of GAC members and we've received the SSAC's feedback on this.

We had a consultation yesterday here at the Nairobi meeting. The public comment period is open to the 29th of March and we're certainly willing to discuss with any individual stakeholder the intent of this and how we see this evolving and get feedback about either of the initiatives and what is the proper approach to those.

Again, I mentioned at the top that the organizational and funding models for these things are not determined, so we're taking feedback on that as well. And I certainly will have the proposed different approaches to that and I believe that will be a major aspect to the next phase of working on these initiatives.

Quickly, I just wanted to highlight a few things just for information. Independent of the DNS SERT initiative specifically, ICANN has established a very close working relationship with

FIRST, the global forum for incident response and security teams, as well as, working with national SERT communities.

We held a training session here in conjunction with FIRST. We had 35 students and most of those students are engaged in different national or regional effort to set up an East African SERT. We see increasing the capacity of the SERT community and their understanding of DNS security issues, which they very clearly identified as something they would like to have help with, enables CCTLD's and others at a national level to get better service, better capability from SERTS. So we hope that CCTLD's and national SERTS build strong relationships. It's a much more scalable model for us to strengthen SERTS at the national level then to solve all problems at a centralized level.

We also in that regard plan a survey on CCTLD National SERT collaboration in the near future. We continue the CCTLD training program that we have in association with Regional Training Associations. We had a session here at Nairobi of all 25 people and 8 CCTLD's. this is probably the 10th training session we've had in the past 1 ½ years and I had I think over 75 CCTLD's with both managerial level contingency planning training and increasingly in conjunction with ISOC technical training for DNS operators to include security issues.

We're still engaged, as I mentioned, containing the spread of the Conficor worm. Important for the committee as with last year when we initiated the ICANN plan for enhancing internet security and stability and resiliency. We're going to do an annual update to that plan and I would Janis that we can again get the GAC's input on that plan. That will occur between this meeting and we hope to have the plan ready for review at the Brussels meeting. So relatively soon we would like to present to the GAC a version of that plan for comment.

I do note importantly that this plan is specifically identified in the Affirmation of Commitments as the base line document for accountability. So the contents of that plan in my mind is someone working with the ICANN CEO Board about how we approach the reviews, very focused on the content of that plan as kind of what ICANN has signed up to in terms of its activities and programs related to security activities.

So with that Janis I'll close and see if there are questions for feedback.

Janis:

Thank you Greg for your presentation. I'm looking there are 2 or 3 questions and I will start in that order. Sri Lanka, European Commission, Italy and then the Netherlands.

Sri Lanka:

First and foremost I would like to thank the ICANN team for the excellent presentation. From the Sri Lankan point of view we warmly welcome the initiative that will perhaps lead to the establishment of a DNS SERT. We hope that in the long term there will be closer collaboration

between national SERTS, I know Sri Lanka has one, India has one and some of the Sri Lankan regional countries in Southeast Asia we have one. And some of our national SERTS have already been admitted into the FIRST as full members.

In that context we hope there will be closer collaboration with the national SERTS ongoing work that you are planning to have. My question would be whether you plan to have collaborative links with national SERTS and your plan for DNS SERT in the long term.

Greg:

The answer is probably yes at 2 levels. As I mentioned, mostly through work with FIRST but also working just as the ICANN staff we want to both understand and then strengthen the linkages between national CERTS and the CCTLD operators. To the extent to which we proceed with a DNS SERT, certainly we want to build on the capabilities of national SERTS. We need to understand how national SERTS could use such a DNS SERT as a resource, the mechanisms for communication and collaboration on specific sorts of contingencies but again to the extent national SERTS will become a key stakeholder and we would want to map that in a very practical operational way.

European Commission:

First of all, I want to say how much we welcome this initiative. It is the first time we have real global vision there. But at the same time it is highly ambitious when you talk about business cases and you talk about funding, you are really a full plate with the program you have. Because it's not a technical issue, it's very much an issue of trust and working together and working in an area where we have a number of countries and organizations.

I think that is something I really appreciate and I wonder how you are thinking in this system because basically you are operating in a peer system but you have a hierarchal root. Are you going to try to deal with that issue?

The second issue I wanted to point out and here we're in the GAC you mentioned some kind of coordination collaboration, information exchange with countries that have their own CIIP protection programs, which of course are not only restricted to DNS. So how do you see these relationships?

Greg:

Starting with the first issue about the relative ambitiousness of such an undertaking and how to proceed in a practical manner. I think I concur with the notion that this is ambitious. I think an issue related to that is the scale, what scale is necessary to initiate something of value at a global level? So we've put down a marker in terms of the size of the staff, which is 15 and the resources required which is estimated at $4 million for a certain vision of how this thing would work.

More importantly the next step which we plan to take rapidly is to understand who are partners and stakeholders would be, sit them together and I'm sympathetic to using scenario based analysis of 3 or 4 key scenarios and go how would this SERT service existing other SERTS, those the DNS ORAC which is an operational research center that does analysis that currently does some of these things.

The needs of existing Registries both well resources and less well resourced and try to define operational requirements as the basis for where we would initiative efforts. I think we'll have to do, if a DNS SERT was created it would also have to phase in what things to focus on first and try to work on the most practical problems initially.

So we plan to post prior to Brussels the results of this analysis as an operational requirement and concept of operations document. Hopefully that will provide some more fidelity into how we're going to address this ambitious challenge.

On the second one, which is the more specifically the information exchanges with the existing critical infrastructure protection programs, I actually see this more as part of an initiative one, the risk analysis and contingency planning exercising portion of this.

My notion would be that if we were to conduct some sort of community based risk analysis that nationally based and other critical infrastructure protection efforts that sees in DNS as a major portion, as a major aspect of the critical infrastructure would be aware that we were conducting these analysis and bring that in, consult and collaborate with them as to feeding this information into other critical infrastructure based analysis.

I think this is probably a pretty doable proposition. In terms of multi-national exercise programs, we would like to participate in as experts on the domain name system so as these sorts of things move forward the results of the efforts that we're conducting here under initiative one are rolled into other sorts of efforts related to securing the DNS.

Italy:

Thank you for the presentation and I want to note a few things. First of all, certainly the program that has been presented in the 2 reports that are under a comment period right now, it is very ambitious because it is not only dealing about the best effort in order to assure that also in the new GTLD program the continuation is guaranteed with a certain assurance. But here the intention is to make studies also looking forward. Certainly the DNS is one very crucial structure of the internet and also what is important to note is that in the 2 documents we see that there are certain sums, conspicuous sums in order to start this effort.

The more visible and the one more elaborative up to now is the one concerning the DNS SERT. There have been already some confrontation with the public here yesterday and so there is a curiosity from those present about how to integrate the effort with the present SERTS also

managed by the Registry. For example in Europe there is a coordination about this kind of problems.

So then the other point that is to be examined is the future how this will be, the future of funding more. How then this DNS SERT will be able to be able to be funded after ICANN provided the initial start up fees? So this is quite relevant and I think the GAC should welcome this move and then continue participating in the debate.

Then we discussed the process and how the consultation period will end by the 29th of March. Then there will be a new version of the 2 documents after further interaction with those that are involved. Of course, this will give the chance then to also for the comments. So okay this is only to signify that the GAC should appreciate this move. Thank you.

Janis:

Thank you and since time is running I have Netherlands, Canada, Sweden and UK and Kenya and Norway and then we're closing this. If you have a question please formulate it immediately and if you have a comment please try to be brief.

Netherlands:

Echoing the other members that this is almost not needed but almost inevitable to have such a function given the inherent vulnerability of the DNS system and the design. A question I have is more about the structuring of these 2 initiatives.

I was wondering if because we had a pre-consultation on this with the stakeholders back home, we have a SERT that is trying to modify into a net SERT, one question I think is important and I think Stefano mentioned it in how much effort you set into having expert institute and people just in one place versus the effort you put into string and knowledge exchange and networks between the already SERTS who are there. I think the second point is the most important asset of the SERT, the way they quickly exchange information and they have knowledge about threats and how to overcome them.

So for me it's more the balance which should be kept in mind. Thank you.

Greg:

In quick response we definitely are inclined and believe it will be more the second model where this is an information sharing. For example, a key component of what SERTS can do is malware analysis. They understand the technical characteristics of a bad piece of code. We would think that there are plenty of people out there that do that but the question is how does this SERT leverage existing malware analysis in other national SERTS or in a research community? And bring that information to bear and share it rapidly with the right set of people, not to create a technical staff that does all the things that are already ongoing.

Again, we plan a session to bring all the people who are working on these sorts of problems together to really define what the value added of this staff and this SERT would be and not to recreate existing capabilities.

Heather:

Thank you and my comments are actually very much along the lines of some of the previous speakers. I think that it is wise to really consider respective roles regarding what you're proposing to do apparently at the global level versus drawing upon regional or national competencies. You would want to ensure you're not duplicating and what you're doing is really a valuable contribution to what we all agree I think is important for DNS security.

So I would urge you to think very carefully about the arrangements that are appropriate. And in particular to receive feedback on what you're proposing to do from SERTS and from the organizations that some colleagues have listed that would have I think valuable comments to add.

Greg:

We hear that voice. Yuri if you'll stand up real quick. Yuri is the staff lead and he was the technical director for the Japanese SERT before she joined the ICANN staff. So we're familiar both in our own staff and in our collaboration with FIRST about the need to work closely with the SERT community and will definitely plan to do so.

Maria:

I also have some comments that are actually very much in line with my other colleagues. It is actually about the added value and creating this ICANN global SERT because of the activities and contacts and trust on the national level. I would like to ask you instead why don't you focus more on capacity building or activities in parts of the world that actually might need more knowledge instead of doing things that is already going on in the national SERTS?

I also want to know if you've had a discussion with the ccNSO and the SERTS at the national level and in that case I want to know their comments.

Greg:

We've had discussion with a number of national SERTs through our engagement with FIRST. I briefed the annual meeting there of probably 200 attendees. The domain name system is a pretty complex entity, so even as well staffed an organization as the US SERT has said their depth on specifics of DNS security is not what they would like it to be and the notion they would have a collaborative operational partner to deal with issues specifically related to the domain name system is useful. In East Africa there is no current national SERT that is validated and the

operators we had in the room this week definitely saw the need for assistance on domain name systems.

Now to the end of capacity building we are out there at the CCTLD level trying to train on DNS security issues. We do plan to continue to train national SERTS on the issues as the first line of response for DNS operators in a given country. It's much better if they can reach to their national level. I think our analysis to this point is that there is a gap of knowledge on DNS security issues and having some sort of collaborative hub of expertise would service both SERT operators and CCTLD operators or DNS operators in being able to respond effectively to situations.

UK:

Thank you Greg for coming to our meeting to provide a summary and update on the initiative. The UK regards this as a major step forward for ICANN. It is consistent with what we said in our digital written repot where our Ministers really looked to ICANN to take the leadership role in improving standards of the security and the key protocols process and technology that under pins the DNS. It is really appreciated to see this is moving forward in such a determined and comprehensive manner.

I've consulted within my administration and there is a lot of interest in these 2 documents. They're looking at this now and mindful of the deadline of March 29th that you pointed out. We're also considering how we might engage with your expert group that you are setting up.

With regard to the DNS SERT that is going to be I suppose at the sharp end of ICANN's security efforts. So it is important that that's got right and we look forward to more information about the scope and scale of the DNS SERT. I think you mentioned there was a workshop planned to engage with people to feed into that. So if you have more details about the date and plans for the workshop that would be very helpful. Thanks.

Kenya:

Mine is just to say thank you very much to the ICANN team. As you know we're going to have increased access to the internet so we really do appreciate and welcome the various initiatives and do look forward to working towards a global initiative. Thank you.

Janis:

Thank you, United States.

United States:

We're currently consulting all the various stakeholders in the US which takes quite a long time, so I'll be formalizing our views in terms of the specifics of this. But I think at this point we just want to flag that similar to others who have raised concerns about how it would work with the national SERTS, potentially duplicity of work and others we do have those concerns and really

want to be informed. The GAC should want to be informed of the views of the other stakeholders in ICANN whether it's the Registrars, Registries, the ccNSO, and really hope that going forward the GAC discussion is informed by that view as well.

Janis:

Thank you and last is Norway.

Norway:

We would also like to express support in this really important initiative regarding some sharing information and some sort of dealing with the increasing risks in the DNS space. One thing is that I just wanted to know if you have considered what the relationship will be with this initiative and the SSAC. Some of these activities kind of is already under the charter of the SSAC but this is more operational activity. So that would be nice to hear your views on that.

The other thing is what the US said if you sort of contact our national SERTS it would be nice to get information to the GAC for their country. So it would be nice to know if ICANN is contacting the national entities in dealing with this. Thanks.

Greg:

So we'll just take that as a point of order if we're in contact with the national SERT that we will probably use Max to provide that information to any GAC member where that occurs. To the first point, we have a Chair of the SSAC to my left so my view is as you put this is an operational focused initiative. SSAC is the technical advisory committee and certainly provides essential input to the Board and the community about emerging issues and challenges and advice on those challenges. But the formation of an operational entity is a staff and implementation matter and now we're working on what the strategic plan calls for ICANN to do. We see it that way but I would welcome Steve's views if he has any on the topic.

Steve:

Thank you Greg. I think the first and most straightforward thing to say is that we're talking about an operational capability here and the first thing to say about SSAC is it is not an operational entity comprised of volunteers provide part time out of their own excess capacity. So we're capable of providing a degree of advice but definitely not operational standing up of a facility or control of it or so forth.

Greg tries to consult with us, we try to provide some advice and I think all of that is appropriate. So I appreciate the pointing to us and asking what our role might be in it. But I can tell you absolutely we're not going to stand up a SERT. Among the many competitors subtract us from that list.

Janis:

Thank you Greg. I think this was an interesting exchange. I believe it was useful for both sides. I noted in general there is support of this initiative with certain reservations. Certainly we need more information. The reservations were expressed about coordination and cooperation with national SERTS. What I didn't hear was the issue on funding.

I understand the initiative has a really big budget and as you said yourself this is not budgeted in ICANN. So where you will be looking for these resources in the next budget cycle or looking for funding outside. In the first slide, you referred there were a number of surveys among national CCTLD's and you said this was very useful. Certainly it is if you ask the question whether activity related to security is useful; the natural answer is yes of course it is. But if you ask question do you think this initiative is useful and are you ready to pay for it? Then immediately the answer will be depending on service we will receive as a return.

I think you have general support and the devil is in the details. I'm looking forward to hearing more details after the round of public comment. I'm looking forward to future engagement with you.

Greg:

Thank you Janis and I thank the members of the committee. We will certainly stay in close contact and provide information as we discussed here and further information as this proceeds.

Janis:

Now Steve you had already a slight training answering one question. Now the mike is all yours. You have a presentation as I stated at the beginning. We had a very interesting conversation in Seoul. The feeling from there was conclusions of SSAC on the report were not conclusive and we decided to continue this engagement and exchange of views. This is the right moment and I'm turning the mike to you.

Steve:

Thank you very much Janis and it's a pleasure and privilege to be invited back. I want to demonstrate my growing skill in dealing with these complex questions by passing the buck here. Julie Headland is going to be running the slides and Rom Mohan will actually be giving the briefing here. I will sit back and arm myself deal with some of the questions I know are going to come from the presentation. So with that let me turn things over to Rom.

Rom:

Thank you Steve and thank you GAC for having us. We're here to speak what SSAC is on the root scaling study. So as a very quick background last February the ICANN Board asked SSAC and RSAC to coordinate a study with some general goals. The concern was that there were

several things planned to be introduced into the root at more or less the same time, DNS SEC, IPV 6, IDN TLD's as well as new TLD's.

The question was will doing this set of changes; does it cause a security instability concern? So the SSAC commissioned a study got a response back and in September of last year we began consideration of 2 reports. One is what we call the Root Scaling Study Team's report, the RSST report and as well as the TNO report. The TNO report was about the technical model used and SSAC has already published its comments on the TNO report.

Since September SSAC has been deeply engaged in reviewing the RSST report and attempting to come to a set of crisp recommendations for the community.

So in summary, this is where we're at. We don't have a final set of recommendations yet. But on signing the root DNS SEC and that's a big change and that is a game changer in terms of what goes into the root and how much care we should take for that.

On new TLD's where SSAC is at right now we're thinking issues might have to do with the rate of change of introduction of new TLD's into the root zone. On IDN's in general they're like new TLD's except there are some special issues and I'll get to it in the next slides. And adding IPV 6 addresses we think is a small impact and there is a new issue that is a new consideration that is come up, which is any cast server locations, the global nodes that are spread out for the root servers, the server locations is a new consideration that we're looking into.

The next slide, on signing the root, DNS SEC itself, that is under way. It is anticipated to be in full operation in July of this year. There is a lot of testing that is in progress. Some of the root servers already have the signed zone, we're seeing there are large responses being returned and so far so good, nothing bad has happened so far. At this point, it seems like it's moving along in a and safe way. And the informal conclusion is among the multiple factors we're considering DNS SEC was the biggest change and so far it seems to be going fine. If it continues to go fine then we might be in good shape.

The next slide, which is new TLD's the headliner there is really the security and stability concern, much of the discussion in SSAC tends to be about, it's dependent on the rate of change. The questions that have come up inside of SSAC are when you add new TLD's into the root system; will it overwhelm any part of the root system? If so, how many new TLD's? Is there a rate there? When and at what point will there be a trigger or threshold event that will have the system go from good to bad? And how will we know there is a problem?

So these are the kinds of questions that SSAC is looking at. ICANN itself is preparing to ramp up the capacity to evaluate and approve new TLD's and ICANN has indicated, there is a report up on the public area, ICANN has reported that they have the capacity to evaluate up to 924 TLD's a year or more after the new GTLD program starts up.

Now inside of SSAC one of the things we've been looking at is while that may be a capacity issue, in reality it's not clear that ICANN's own legal department, the Board, there are multiple steps of having a TLD approved, delegated and actually be in the root. We're not sure that those pieces have enough capacity to handle a large volume.

So in conclusion and also can the root server operators accommodate that many new TLD's? We don't know yet and some communication has started with the root server ops. The informal conclusion or at least the direction that we're converging is probably yes they can handle that many TLD's but again it depends on the rate of change, the rate of introduction of the TLD's.

The next slide, IDN TLD's in general it is a non-issue. We already have IDN TLD's that have been introduced into the root zone from a couple of years ago and we know it works. So that process is not something we're worried about except the requests for IDN TLD variants to be delegated to the root zone. For those who are not technical, the variant is considered to be a string that is considered to be identical to another string that is applied for. So you apply for a string and you have another label that is considered to be equivalent and identical to the other.

The request for variants to be delegated and to be active and work in the root zone and there we have quite a bit of study and work to be done. The technical and operational issues related to delegation of variants into the root zone are not thoroughly worked out. The desired behavior seems to be that we want to insure the variants of a TLD point to the same locations as the primary TLD. But how to do it, how to insure that this will actually work, what to do if it doesn't work. What happens if the convergence we want starts to diverge? Those things are not yet figured out.

But this issue is separate from scaling the root itself. So from a pure scaling the root, adding IDN TLD's to the root in and of itself is a non-issue, but the specific issue of variants a wrong approach there could cause stability issues for the root zone.

Next IPV 6 records, they've been added at a slow steady rate. The conversation inside of SSAC is that the impact of adding more IPV 6 records into the root zone is very small. It is just business as usual and there is no reason to really interrupt future requests for IPV 6 records even if you add DNS SEC and new TLD's and IDN's.

Finally on the next slide, a new consideration we're looking at is the location of the (54:08 – inaudible) servers. Now there is a possibility that a remote location of a (inaudible) instance of the root might inhibit growth of the root zone itself. The RSST study actually points to that and SSAC is looking into what that impact might be. And root server operators haven't spoken clearly about this. Inside SSAC we have some dialogue with root server operators and some of them say this may not be a problem at all. There are others who worry this may become a real operational issue.

So what is needed here is some direct and straightforward discussion with the root operators before SSAC can come to a reasonable and logical conclusion that this is or is not a problem going forward.

So in summary, the RSST report and the TNO report, from the study of SSAC and RSAC along with the staff commissioned, what is clear is that the 2 of these are not sufficient to conclude the root scaling study itself. There are still gaps that exist, there are still issues that may potentially impact the scaling of the root as you saw a new one that came up was the placement of (55:30 – inaudible) instances but we worry there may be other issues that are not yet identified.

We're also looking at should communication between ICANN and the root server operators should that or could that be improved from where it is right now? So some of the discussions inside of SSAC lead to and these are not yet final conclusions, just underline that, but our thinking is it's possible that we don't need for the work for the studies from SSAC and/or RSAC to start new TLD delegations. But it could be required to continue new TLD delegations. So that is where it seems to be converging to. This might change based on the discussions going on. There is very vigorous debate inside of SSAC and if you listened into these calls and debates, it is striking the amount of energy that the volunteer members of the SSAC are putting into this. There is a lot of care and passion about it. But there is not yet complete convergence on coming to final recommendations.

We're hoping that next quarter we'll be able to issue recommendations based on the RSST and TNO reports, having those as input into our thinking. We also are targeting next quarter to initiate a second version, the next version if you will of the root scaling study to look at the pieces that have been left out or not completed in the first study.

One of the things, when we began the root scaling study effort last year, one of the things that SSAC and RSAC but SSAC specifically in this presentation what we looked at and we bookmarked was we don't know, no one has done a study as to what the scaling of the root, what the end user impact might be. We bookmarked that and said that's something that has to be studied. It is not immediately urgent for all these other issues for signing the root, etc. but it's still important to be done. So that important work we hope to initiate that work in the 3rd quarter.

So that hopefully gives you a clear picture of what are our thought processes and what we plan to do. I'll open for questions and hand it back to Janis.

Janis:

Thank you Rom for this presentation. I have immediately 3 hands Sweden, European Commission and Italy.

Maria:

I would like to say at the discussion yesterday at the planner session about the new TLD process there was a request from the floor talking about how to handle it if you see smoke on the edges of the DNS system. I think there was someone in the panel talking about then you have to slow down the core. Slowing down a core you need a tool, so my question is actually do you have the tool? If so, what kind of tool you have to slow down? That is something that I think is very important because also in this presentation you talked about 3 different issues. If so, how many and when? How will we know? But I would like to add a 4th and it's how to be able to slow down the core? Do you have the tool or clue what that tool could be?

Steve:

Let me speak with 2 hats on at the same time as both Chair of SSAC and as a member of the ICANN Board. First, with a purely technical hat on, the notion of early warning system of detecting smoke at the edge of the car if you will is a very compelling and appealing idea. However, I have to say that as appealing as that notion is in the abstract, matching that up to the specifics of what we're talking about in the DNS remains an open question.

One of the things that the RSST report talked about was an early warning system. We know from the notion of an early warning system comes from the early missile warning systems where we know 2 things, we know what the result is going to be namely a missile is going to arrive and cause some serious damage and we also know what to look for that is going to tell us if there is namely something that indicates a launch and gives us some number of minutes of advanced warning.

We don't have the corresponding specifics of what it is that would be going wrong, we don't have the corresponding specifics of what you would look for. Again, with my engineering and technical hat on, I would be absolutely interested in understanding what those things are.

Second, and also I must say we're talking about an extremely slow moving system. It takes a very, very, very long time from the time somebody request some information be put into the root to get it through the entire process and into the root. Never mind the application process for GLTD's, never mind the regular all the growth process, today it takes from the perspective of a competent TLD operator who is making a planned change, if you go and ask how long in advance do you plan to make this change because it takes so long to get information into the root the answer is 6 weeks. Now that's not the advertised amount of time. IANA says it only takes us a couple of days and only takes 12 hours to propagate it out from VeriSign to the root server operators. But if you actually ask from the outside what does the system look like to the users? It is an extraordinarily slow process totally inconsistent with operating on the internet time.

Now let me go back with my Board hat on and answer your question about do we have the tools to slow things down. The answer is absolutely. Nothing goes into the root without getting through a multiple approval process; particularly new applications have to be approved. There is

an authorization process through the Department of Commerce but even before it goes to the Department of Commerce there is considerable processes within ICANN.

The Board has a responsibility to make sure that there is stability and security in the process. If appropriate alarms were raised it would be the Board's responsibility as a last resort if not managements to slow that process down and do whatever is necessary to protect the process. So I think that part is actually the easier part and it's the lack of clarity about what do we mean by smoke, that is actually creating, if you will, more smoke than real content here.

European Commission:

Now I'm a little comforted in comparison with Seoul. What was the situation in Seoul? We had some guys who had done something very quickly, 2 months or so. Saying when we were questioning them, well we didn't have enough data and our model is not really perfect. This was kind of reiterated when I saw the comments coming from your corner saying listen this is not enough.

Now since then there has been a couple of months gone by and I have the feeling if you don't have more data that you're comfortable even without additional data with what you presented. So your comfort is not based on some further modeling of other data but you have, my impression is you have said the crucial issue is DNS SEC that is the thing that really challenges the system, the rest is more marginal. And if we come through with DNS SEC we're all right.

The other conclusion I sense is okay this will be maybe in July but it won't really impact the speed of the other things. We shouldn't say we have to wait 6 months more until we tackle more things like GTLD's or IDNs. That is something new for me in this session is you say well there are some issues we haven't really looked at and then IDN variants, it's not IDN as such but it's IDN variants and I would like to say that that's new and something that runs in parallel and I would like to know exactly what you mean by that?

Elizabeth:

I'm sorry if I'm coming back on something you mentioned but I just wanted to make sure I properly understood it. When you said that the variant is something which is identical, you refer to the fact that the string is visually identical. So if we have, for example, AAA Latin the AAA would be visually identical. But you didn't refer to something which is like confusing the similar.

Rom:

Let me address that, variants themselves depending on who you ask you get a somewhat different definition of it. I think really what we're talking about here is when a GTLD or a CCTLD comes in and says here are 2 or more strings and we declare that these strings are the same thing or mean the same thing. that is how they define it, and we want all of these strings, 2

or more of these strings to actually work in the root and they may make 1 or more representations and some might say we will take measures to ensure that each of the strings that goes into the root will somehow be tied together so that if you are a Registrant and you get one, you get all the others somehow even though in the root they're considered individual entries.

Others might make a representation that says even though they mean the same or look the same or we represent they are the same let's say but we may want them to work in slightly different ways in terms of where they point to on the DNS. The question that SSAC is looking into is (a) what is the expected behavior? Should variants that come into the root, should they point to the same place? If they should point to the same place, then how do you make sure they point to the same place? Is there an appropriate way either technically or in other ways to ensure this happens? Keeping in mind that once you delegate a string to an operator from that level further down below ICANN directly doesn't have authority or control over how that string gets used.

So if the goal is a DNS system that converges and if you are allowing variants to be delegated into the root that might cause divergence, then you have potentially a stability issue. So we have not defined specifically what is a variant. Is it visually similar? Does it mean the same? Does it look the same? That in many ways is dependent upon the representations of the applicant for the TLD.

Certainly SSAC what it is looking at is if such a representation is made and if there is a request for these different strings to somehow be tied together and treated as the same, then is it feasible? If it's feasible what are the risks associated with it? I hope that clarifies it and perhaps we can talk offline about that.

To the earlier set of questions, I don't think there is yet a sense of the SSAC as a whole that there is comfort with all these different pieces. The difference from Seoul to here is that the DNS SEC addition into the root and all the exercises associated with the tests so far seem to be going well. so there is, I would characterize the mood as cautiously optimistic but come June or July if there is a serious problem with or if we find something that happens in the root as a result of the root being signed, then you can certainly anticipate SSAC to step in and say this is a problem and we should slow things down until we figure out what to do about this problem.

But I think in general your sense is right and there is more optimism about where things might go but there is still not enough, no new facts or data from other than the studies except for the fact there is a DNS SEC addition to the root. Those tests seem to be going well.

Janis:

Thank you Rom. Italy and then Egypt.

Italy:

Having participated through this working group in the SSAC I can testify there is an enormous amount of competence and of operational skill. But as the study goes on, as we understand from the conclusions here more analysis and more data have to be acquired. This is why the SSAC study didn't give the numbers, especially concerning the new GTLD's. This was smoothing that connected to the new GTLD's, the community and maybe also the ICANN Board is expecting.

But it was very, very important this confrontation about the elements that increased the size of the root zone. One could conclude and say then the DNS SEC and new GTLD's are in competition. One of the conclusions that Rom didn't show is the time schedule, DNS now is in an accelerated phase and has not to be stopped at all, it has to go ahead, while the insertion of new GTLD's there is a phase connected to the time of implementation decided by ICANN.

But in the end, certainly we learned that the root serve operators I would not say are a problem but in part are a problem in the sense that they have to say how much new GLTD's per year they are confident to manage without operational problems. We know the root servers have no specific contract for doing this job. So we are confronted with some weakness of the system let's say. And this justifies even more the studies of the new initiative on security and stability that were announced before by the staff.

This is my evaluation from being in the group. The only criticism that could be moved to the SSAC is why these studies weren't done before the announcement in Paris of the unlimited additional new GTLD's?

Steve:

Let me sidestep the Paris question. Let me note that with respect to engaging directly with the root server operators, we have the benefit of having a real live root server operator in our midst here. Bill Manning, 2 who is the other one? Curtis where is Curtis? Oh you're hiding. We have 2 so maybe we'll get 3 answers, root server operators. Janis with your permission may I ask if either or both would like to speak?

Bill:

My name is Bill Manning and I work with the University of Southern California and we operate the B root name server. I was also a member of the study team that did the root scaling study. The question about rate of change is somewhat similar to asking the question, do you drink water? The answer is yes. How much water do you drink? A liter a day, a thousand liters a day, a quarter million liters a day, how much water can you drink? We did not know.

So we engaged with and continue to engage with ICANN to come to a realization of what the expected rate is. And within that construct I think we actually have this ongoing dialogue that says that we're able to handle the kinds of rates of change that are being suggested, so the scalability is there.

Now as to future studies, certainly we need them. There are several of them that were pointed out in the RSST report and there are others that have come forward and Greg talked about some of them. So there continues to be a dialogue. There also continues to be discussions about how to regularize the communication between root operators and ICANN. Thank you.

Steve:

Curtis do you want to jump in here?

Curtis:

I'm Curtis Lindquist from the I Root Server in Stockholm. I think I share what Bill said. I just want to say we've also published the letter to ICANN saying we'll take a root server and we acknowledge this. There is a discussion between the root server operators and ICANN of what expected change rate is and the expected size of the zone and that will give us some idea of to tell you whether we can handle it or not.

But we are in dialogue with this and I think as Bill said we as well as other root server operators participated in the root scaling study and I think we all support that study and the data that is in the report.

Egypt:

I think good part of my question was asked by Elizabeth and it is again related to the variants. I want to make sure I understand right, so currently you are not looking into what is the definition of the variants. I mean you're expecting that whenever there is a definition and we agree this should be pointing at the same place then you are trying to find the mechanism, right? Because I think when we say variants this could be confusingly similar, could be identical, I'm not sure whether this extends to translations of the same word. And if we leave it up to the applicant might even extend to defensive registrations.

And again, the same things written in different scripts, I mean it is a very wide range of…thank you.

Rom:

You're right our focus is not on defining the variants. We're simply saying we expect as a matter of course that applicants will come in to the process and say here are variants, here is the string and here are variants, please delegate all of them or some of them and please make sure they work and have them point to the same place.

Our focus is what happens from that point onwards? Are there stability types of issues? We're not nearly as focused on whether it is identical or translation, similarities, at least that are not where we're thinking of going. We're much more concerned about expected behavior of the

DNS post delegation and ensuring that a predictable outcome will remain predictable once variants get, if variants get delegated. So that is really where our focus is.

Janis:

Thank you, Egypt do you want a follow up question?

Egypt:

I was just going to a quick remark that again I know it's not the focus now of the group but I don't think it's a good idea to leave it totally up to the applicant. I mean there should be a criteria or definition for what is a variant and then the applicant should commit that those strings falls within the criteria. We cannot just leave it totally to that.

Steve:

I think you're raising some extremely valid points but we're not the right people to be responding to that. There is a whole other set of people. so the relationship is that when the choices are made about variants, then there is a technical issue about how best to support that and so that's the element that intersects with the work we've been doing.

Janis:

Thank you Steve. United Kingdom.

UK:

Thank you to everybody who has been contributing to this discussion, which has been very informative. I hear there is a lot of dialogue going on and that's very necessary. I feel very uncomfortable going back to my Minister and saying there is dialogue going on. We really need a clear sense of how these issues are going to be fully bottomed out and key decisions then made. If I can say to my Minister there is going to be a convening of experts on a certain date and the ICANN Board is going to take a decision that's going to please the Minister.

I think my message here is if we could be through the Chair if we could be informed as soon as the experts here and who they are engaging within ICANN and externally do reach a point of firm understanding of whether it's a trigger point or cut off point between one GTLD application round, a cutoff point between that round and a decision needing to be made on whether successive rounds should be undertaken, which I understood was one of the points that was made earlier that no further work needs to be done now. But with new TLD rounds then maybe further studies would be required, if I understood that point earlier on that you made or maybe I need correcting on that.

Likewise, on this 5th component on this whole debate, the remote locations, as I understood it there is no clear determination yet of whether this is a serious operational issue. If we in the

GAC could be informed of when that point of determination is made I would requests that through the Chair that the experts come back to us and then I can report back to the Ministers on whether to discount that or add it to the list.

I just wanted to underline that this is very informative but we have to go back and advise our Ministers and just to say there is a hell of a lot of discussions and exchanges and dialogue going on is a very weak thing when you go to the Minister's office and he wants to know what the risk is. I guess that was my point, thanks.

Steve:

I appreciate very much the awkwardness of the position you feel. There is a subtlety that I want to try and disentangle here related to your question. When we started this study, we felt a great sense of urgency and set a very thick timeline to get it done. The result of that work which is embodied in the RSST and TNO reports did in fact meet the schedule but didn't in many of our opinions cover the ground adequately in a coherent and documented way.

As a result, the advice out of that we felt unable to support fully and just forward it and say there it is. With a certain amount of chagrin we have seen the error of our ways and changed the priority to trying to get it right rather than try to get it now. So that leaves us in the complimentary awkward position of well we can't tell you when we're going to finish this exactly but we do nonetheless continue to feel that urgency.

And as Rom showed in the slides, we have a schedule for moving this along. In parallel, you have the GTLD introduction process plan that you hear about from other parts of ICANN that we're not responsible for and that talks about setting up a round and then taking a breath between rounds, etc. Irrespective of anything we do or any of the issues that are raised, it would be very natural to just as a normal business process that when you start something you would then make some adjustments as you learn through that.

So I think what you're hearing are 2 learning processes that are proceeding quasi independently and somewhat in parallel. One is on the business side of we'll do a round and then we'll learn from that and then on the security and stability study side that we are probing these issues as rapidly and as thoroughly as we can. Some of them are resolving just because the passage of time is providing some clarification.

Then finally with respect to your last point about the placement of these (1:26:13 inaudible) service, my guess is at the end of the day that will get taken off the table. I'm just speaking personally. However, it was put on the table in a implicit form by having it raised in the discussion with the root server operators and it would be inappropriate to ignore that and say well as long as you raised that then let's go find out if that is actually a driving force or not. I think we'll have that discussion and the root server operators will come to some statement about that and we'll move forward.

Many of the root server operators take the position you tell us what to put in the root and we'll make sure it gets served and that's been a very positive posture on that. and I think again I'll take the risk of just speaking personally and take off all my hats, I think at the end of the day that's roughly where it will go and if there are some adjustment to that then it will be worth teasing that out and making sure it gets full airing.

Janis:

Thank you Steve. I have 2 further requests for the floor, one from the League of Arab States our new observer here for the first time and then France.

League of Arab States:

I just want to point out that probably to some applicants maybe variants, they need to point our variants not to delegate all of them but rather to protect other variants. They need to allocate 1 or 2 but protect the other variants from abuse. Thank you.

Rom:

Yes I understand what you're saying. I think our focus is less on the allocation. In the ICANN process, an applicant may be allocated several strings but where we worry about potential security and stability issues is when more than one string is delegated and there is somehow supposed to be tied to each other and go to the same place. There is more work that needs to be done and that's where we worry about the security and stability issues. But we're not thinking about or have problems with allocation of multiple variants. That is a separate process all together.

Bertrand:

One element Steve was describing the sort of parallel track between the study and the root scaling which is basically what Bill Manning was saying about how quickly can you drink water. The other element which is basically the new GTLD introduction process, the EOI discussion which is basically how much water is piling up in the dam before we open the gates?

The problem I have at the moment is because of the uncertainty of a potential of a second round, the likelihood that people will over subscribe or over apply in order to make sure they are in this small window whenever it comes is growing. So we are having a stupid Catch-22 race whereby on the one hand it would be absolutely no problem to have successive rounds very near one to another, having a first round of 50 and then a round of 150 and another round of 200. But at this time because we're trying to solve all the problems and before anything opens, we basically will end up having maybe 500 or 600 applications that will have to be processed.

However, the staff is saying they will have to do batches because the processing of the applications taking time, the time and delays for introducing all of this is going to be extending

progressively. So my question is, even if through an opening of the round there were 500 or 600 applications, provided that they would be progressively introduced suddenly not in one year, do you think that this is a completely valid and non-threatening type of rate? Let's say you have 500 or even this is enormous even 100 or 200 that gets into 3 years in the root, is this something that is completely within the zone of comfort?

Janis:

Steve I will add a little bit to this question. When Maria was speaking about the car and smoke, as process is designed now the evaluation will take place outside ICANN by the evaluation teams. Each evaluation team will see each application. But the team will not see everything; let's say the whole picture which will come only to IANA people and ICANN Board.

So assuming that all the evaluators say yes, yes, yes everything is fine we go ahead and then suddenly the whole picture shows that we need to slow down for technical reasons. But there has been already process engaged, money involved, which potentially would create a lot of legal difficulties to ICANN.

Again, this is the question of whether we can allow the start of the round without being absolutely sure how much we can handle. Not putting ICANN in potentially say uncomfortable position which may cost a lot of money and trouble, where the technical and policy side come together.

Steve:

So the quality of this kind of discussion is different if there are numbers on the table versus there are not. We now have some numbers on the table in the form of delegation rates paper that was recently released.

There are 2 kinds of numbers associated there or presented there. One is the expectations, how many are likely to come and so forth and it's measured in the small numbers of hundreds for the first round. I think it would not be too risky to say that if those are the numbers that actually show up, there is no issue whatsoever. They get processed, get put in the root and the root server operators have no problem.

The more interesting question for this discussion is what happens if there are truly large numbers? The model presented there is there would be a maximum capacity of the evaluation teams and therefore a round would be divided up into batches and each batch would move through. And if you take those numbers, its 4 months to start a new batch, so you would have a new batch every 4 months of about 400 I believe. So that leads to 1,200 per year coming through and an estimated success rate of 77%. I won't challenge where that number comes from. That leads to a maximum of 924 per year. But it takes a year to a year and half to ramp up to all that.

So that is kind of the maximum size of nozzle that is spewing stuff out. But you get to see this well in advance.

So one of the questions which can now be asked in very crisp and sharp terms is in 1 ½ years can you handle, the address to the root server operators, can you handle an increase of 924 per year every year? And we don't have a formal answer back but now that there is a number that narrows the conversation down and we're no longer talking about millions or hundreds of thousands.

So I don't anticipate that some of the more extreme kinds of scenarios that it's easy to imagine without concrete information are quite as relevant. So I'm not losing any sleep over this for what that's worth.

Janis:

Bertrand.

Bertrand:

Yeah as a matter of fact thank you very much for the answer. I have 2 quick follow ups, the first thing is following those numbers and the idea of batches, I have trouble understanding and this is not directed to your study but more general comment regarding the process we're in. I have trouble understanding why it is perfectly normal, transparent and accountable to have the staff defining batches versus having the community defining a set number for first round and set number for second round. This is beyond my understanding.

The thing is in the current mechanism there are many ways for the community as a whole, for the Board, for all the different entities to come together and say we all have collectively an interest, not only to solve the legal problems regarding the process but also to have as quickly as possible a small well designed round and then as quickly as possible afterwards another little bit larger round. Can we design rules for that?

For instance, something that has been floating during those first days is if there were an objective to have a relatively limited first round that would be fair knowing that there is not an unlimited number of actors who are completely aware and so on. Why not establish a limit for the first application, the number of applications one single entity can apply for in the first round? Is that completely unrealistic?

Janis:

I think this is a question we can raise during the debate with the Board today. But if you want to answer Steve?

Steve:

I think that is the right place for that question. The questions we focus on are divorced from that question of how you manage that business process. That is really a business position and I was thinking so if you limit it to 50 or 100 who is going to make that decision? The answer is oh I know who I would get; Bertrand will volunteer for the selection process of who should be in the first 50. I like that idea.

Bertrand:

I actually do.

Janis:

Thank you. Rom?

Rom:

I just want to respond to one of the clarifications a colleague from the UK was asking about the first round versus the second round. That wasn't the intent. What we were really trying to say was to open up the process of getting applications and processing applications in this new TLD round, it seems at least the feeling inside of SSAC is we may not need more studies. However, once you begin the process and start adding TLD's into the zone it's possible that some of these other factors that are still yet to be studies may infringe upon the rate of introduction even from this first round.

So we're not trying to say anything about future rounds, we're just focused on this current round.

Janis:

Thank you.

Steve:

Let me also add our colleague Suzanne Wolf has been very actively involved in this. She regrets she couldn't come physically to Nairobi but she's been actively watching and listening and participating in this. She's been very helpful in facilitating the interactions with the root server operators.

Janis:

Thank you and do we have other questions? I don't see any requests for the floor. Steve and Rom thank you very much for your presentation and for this useful exchange. Personally, I am more comfortable than I was after the Seoul discussion. All questions aren't answered but there is the level of comfort has certainly increased.

I will see whether GAC feels as a result of this discussion that we need to meet again in Brussels or we will meet again the next time in Latin America. That is a function of our debate tomorrow and thank you very much.

Steve:

Thank you and as I said at the opening it's a pleasure and privilege. I actually look forward to these and so you may have understood now that we have a very specific strategy of providing just enough of an answer so that we get a positive response but not so much so that you don't invite us back for more the next time.

Janis:

Thank you. The remaining thing in the GAC, we need to identify volunteers who would draft a proposal for the communiqué. I'm looking around for the hands. I see Italy and the European Commission is volunteering thank you.

Our next session starts at 2:00.